ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

P.G DIPLOMA IN CYBER SECURITY

CSP-016
WHITE HAT HACKING

Block

1 INTRODUCTION TO HACKING

Unit – 1
Overview of Hacking

Unit – 2
Footprinting & Reconnaissance

Unit – 3
System Hacking

Unit – 4
Sniffers

EXPERT COMMITTEE

Dr. P.K Behera **(Chairman)**
Reader in Computer Science
Utkal University
Bhubaneswar, Odisha

Dr.J.RMohanty **(Member)**
Professor and HOD
KIIT University
Bhubaneswar, Odisha

Sri PabitranandaPattnaik **(Member)**
Scientist-E, NIC
Bhubaneswar, Odisha

Sri Malaya Kumar Das **(Member)**
Scientist-E, NIC
Bhubaneswar, Odisha

Dr. Bhagirathi Nayak **(Member)**
Professor and Head (IT & System)
Sri Sri University, Bhubaneswar,Odisha

Dr.Manoranjan Pradhan **(Member)**
Professor and Head (IT & System)
G.I.T.A
Bhubaneswar, Odisha

Sri Chandrakant Mallick **(Convener)**
Consultant (Academic)
School of Computer and Information Science
Odisha State Open University
Sambalpur, Odisha

P.G. DIPLOMA IN CYBER SECURITY

Course Writers
Bijay Kumar Paikaray
Centurion University of Technology and Management, Odisha
Editor
Chandrakant Mallick
College of Engineering, Bhubaneswar

UNIT-1 Overview of Hacking

Unit Structure

1.0 Introduction

In a cyber security world, the person who is able to discover weakness in a system and manages to exploit it to accomplish his goal referred as a Hacker, and the process is referred as Hacking.

Now a day, people started thinking that hacking is only hijacking Facebook accounts or defacing websites. Yes, it is also part of hacking field but it doesn't mean that it is the main part of hacking.

So what is exactly hacking, what should we do to become a hacker? You need not worry; you will learn it from this unit. The main thing you need to become a hacker is to have self-interest. You should always ready to learn something and learn to create something new.

The term "white hat hacker" in Internet slang refers to an ethical computer hacker, or a computer security expert, who specializes in penetration and in other testing methodologies to ensure the security of an organization's information systems. Hacking is a term coined by IBM meant to imply a broader category than just penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively.

1.1 Learning Objective

After learning this unit you should be able to

- Know about hacking and hacker.
- Know about who is a hacker and how to attack?
- Identify different types of hackers.
- Learn more about different types of cybercrimes.
- Revisit the concepts of security threats and its types.
- Identify the programming languages that are useful to hackers.
- Learn more about the concept of Ethical Hacking.
- Explain the Phases of Ethical Hacking
- Differentiate between Hackers and Crackers
- Know the advantages and disadvantages of Ethical Hacking.

1.2 What is Hacking?

" Hacking is art of exploring the hidden things that are being hidden from general usage and finding loop holes in the security and use them to benefit the others"

In another way we can tell Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access.

Example of Hacking: Using password cracking algorithm to gain access to a system.

Computers have become mandatory to run a successful business. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. The term "Hacking" means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

1.3 What is a Hacker?

Everyone here thinks that hacking is just stealing of data and information illegally but this perception is absolutely wrong.

"Hacking is unauthorized use of computer and network resources. (The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)"

Hacking is not always unauthorized. Hacking also includes exploring the Things that are being hidden from the general usage. So exploring things i.e being Hidden from general User is also hacking.

1.3.1 Who is a Hacker?

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

1.3.2 Who is attacking you?

When talking about attackers and hacking it often happens that we ask people working at customer's sites "who is scaring you?" Most of the time the answer we hear is not "Well, you know that we are scared by script kids, playing with those couple of un-patched machines we have," nor is it "We really scared about industrial spies." Rather, 98% of the time the answer is "We don't know."

These answers possibly mean that the company, feeling as a potential target, has not developed a proper IT Security Risk Analysis, while trying to figure

out who may want to attack its IT infrastructure and gain access to its information.

This mistake probably happens because every time people hear "hackers profiling," the word "profiling" automatically makes them think about something that has already happened, rather than something that may happen.

The hacking world has changed dramatically in the last thirty years, and the somehow "romantic" figure of the hacker of the '80s is far from today's.

1.3.3 Types of Hackers

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Symbol	Description
	**Ethical Hacker (White hat):** A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration testing and vulnerability assessments.
	**Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

	**Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
	**Script kiddies:** A non-skilled person who gains access to computer systems using already made tools.
	**Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
	**Phreaker:** A hacker who identifies and exploits weaknesses in telephones instead of computers.

1.4 What is a Cybercrime?

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using mobile phones via SMS and online chatting applications.

1.4.1 Type of Cybercrime

- The following list presents the common types of cybercrimes:
- **Computer Fraud:** Intentional deception for personal gain via the use of computer systems.
- **Privacy violation:** Exposing personal information such as email addresses, phone number, and account details, etc. on social media, websites, etc.
- **Identity Theft:** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information:** This involves distributing copyright protected files such as eBooks and computer programs etc.
- **Electronic funds transfer:** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering:** This involves the use of the computer to launder money.
- **ATM Fraud:** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of Service Attacks:** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam:** Sending unauthorized emails. These emails usually contain advertisements.

1.5 What is a Security Threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-

physical such as a virus attack. In these tutorial series, we will define a threat as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

1.5.1 What are Physical Threats?

A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.

The following list classifies the physical threats into three (3) main categories;

- **Internal**: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External**: These threats include Lightning, floods, earthquakes, etc.
- **Human**: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures.

The following list shows some of the possible measures that can be taken:

- **Internal**: Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented by the use of voltage controllers. An air conditioner can be used to control the humidity in the computer room.
- **External**: Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage. Housing computer systems in high lands are one of the possible ways of protecting systems against floods.
- **Humans**: Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

1.5.2 What are Non-physical threats?

A non-physical threat is a potential cause of an incident that may result in;

- Loss or corruption of system data
- Disrupt business operations that rely on computer systems
- Loss of sensitive information
- Illegal monitoring of activities on computer systems
- Cyber Security Breaches
- Others

The non-physical threats are also known as logical threats. The following list is the common types of non-physical threats;

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

To protect computer systems from the above-mentioned threats, an organization must have logical security measures in place. The following list shows some of the possible measures that can be taken to protect cyber security threats

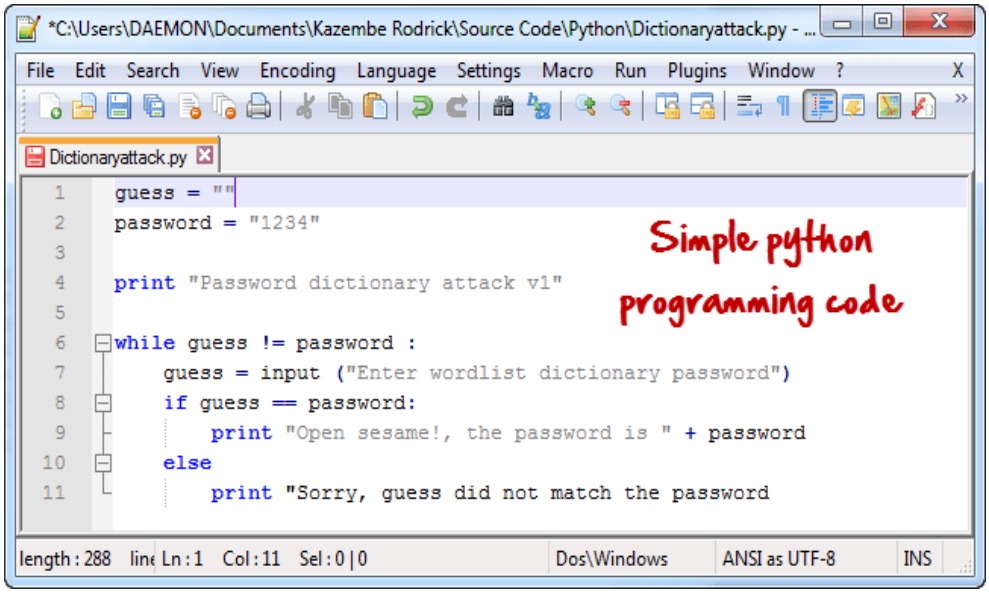
To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software. In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user's computer.

Unauthorized access to computer system resources can be prevented by the use of authentication methods. The authentication methods can be, in the form of user ids and strong passwords, smart cards or biometric, etc.

Intrusion-detection/prevention systems can be used to protect against denial of service attacks. There are other measures too that can be put in place to avoid denial of service attacks.

1.6 What is a Programming Language?

A programming language is a language that is used to develop computer programs. The programs developed can range from operating systems; data based applications through to networking solutions.



1.6.1 Why should you learn how to program?

- Hackers are the problem solver and tool builders, learning how to program will help you implement solutions to problems. It also differentiates you from script kiddies.
- Writing programs as a hacker will help you to automate many tasks which would usually take lots of time to complete.
- Writing programs can also help you identify and exploit programming errors in applications that you will be targeting.
- You don't have to reinvent the wheel all the time, and there are a number of open source programs that are readily usable. You can customize the already existing applications and add your methods to suit your needs.

1.6.2 What Languages should we learn?

The answer to this question depends on your target computer systems and platforms. Some programming languages are used to develop for only specific platforms. As an example, Visual Basic Classic (3, 4, 5, and 6.0) is used to write applications that run on Windows operating system. It would, therefore, be illogical for you to learn how to program in Visual Basic 6.0 when your target is hacking Linux based systems.

1.6.3 Programming languages that are useful to hackers

Sr no.	Computer languages	Description	Platform	Purpose
1	**HTML**	Language used to write web pages.	*Cross platform	**Web hacking** Login forms and other data entry methods on the web use HTML forms to get data. Been able to write and interpret HTML, makes it easy for you to identify and exploit weaknesses in the code.
2	**JavaScript**	Client side scripting language	*Cross platform	**Web Hacking** JavaScript code is executed on the client browse. You can use it to read saved cookies and perform cross site scripting etc.
3	**PHP**	Server side scripting language	*Cross platform	**Web Hacking** PHP is one of the most used web programming languages. It is used to process HTML forms and performs other custom tasks. You could write a custom application in PHP that modifies settings on a web server and makes the server vulnerable to attacks.

4	**SQL**	Language used to communicate with database	*Cross platform	**Web Hacking** Using SQL injection, to by-pass web application login algorithms that are weak, delete data from the database, etc.
5	**Python** **Ruby** **Bash** **Perl**	High level programming languages	*Cross platform	**Building tools & scripts** They come in handy when you need to develop automation tools and scripts. The knowledge gained can also be used in understand and customization the already available tools.
6	**C & C++**	High level programming	*Cross platform	**Writing exploits, shell codes, etc.** They come in handy when you need to write your own shell codes, exploits, root kits or understanding and expanding on existing ones.
7	**Java** **CSharp** **Visual Basic** **VBScript**	Other languages	Java &CSharp are *cross platform. Visual Basic is specific to Windows	**Other uses** The usefulness of these languages depends on your scenario.

* Cross platform means programs developed using the particular language can be deployed on different operating systems such as Windows, Linux based, MAC etc.

1.6.4 Other skills

In addition to programming skills, a good hacker should also have the following skills:

- Know how to use the internet and search engines effectively to gather information.
- Get a Linux-based operating system and know the basics commands that every Linux user should know.
- Practice makes perfect, a good hacker should be hard working and positively contribute to the hacker community. He/she can contribute by developing open source programs, answering questions in hacking forums, etc.

1.7 What is Ethical Hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

1.7.1 Why Ethical Hacking?

- Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's image and save an organization a lot of money.
- Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

1.7.2 Legality of Ethical Hacking

Ethical Hacking is legal if the hacker abides by the rules stipulated in the above section on the definition of ethical hacking. The International Council of E-Commerce Consultants (EC-Council) provides a certification program

that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

1.7.3 The Concept of Ethical Hacking

The following are the basic concepts of ethical hacking:

1. Phase of Pen testing

Pen Test, like forensics, is almost as much an art as it is a science – you can only be taught so far, technical techniques and tools are all very well, but you really need a mind that can think sideways and approach a task from as many angles as possible.

2. Foot printing

Tools and tricks to get the information about the computer, IP and mac address, related user and system.

3. Scanning

Before starting the pen testing, pen tester must have some information about network and system. So pen tester scans the entire network with some tool like Nmap, Zenmap, ping and hping etc.

4. Enumeration

During the enumeration phase, possible entry points into the tested systems are identified. The information collected during the reconnaissance phase is put to use.

5. System Hacking

System hacking is login to system without credentials not only by pass the credentials but also you can work in system as root user by privilege escalation.

6. Trojans

It is a generally non-self-replicating type of malware program containing malicious code. A Trojan often acts as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. While Trojans and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage.

7. Viruses and Worms

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

8. Sniffing Traffic

It is a program that monitors and analyzes network traffic, detecting and finding problems. Various technique and tool is used for sniffing like kali linux MITM attack, tshark, urlsnarf etc.

9. Social engineering

In this technique, ethical hacker creates the phishing page of website to obtain credential of users.

10. Denial of service

A DoS attack generally consists of efforts to temporarily interrupt or suspend or down the services of a host connected to the Internet.

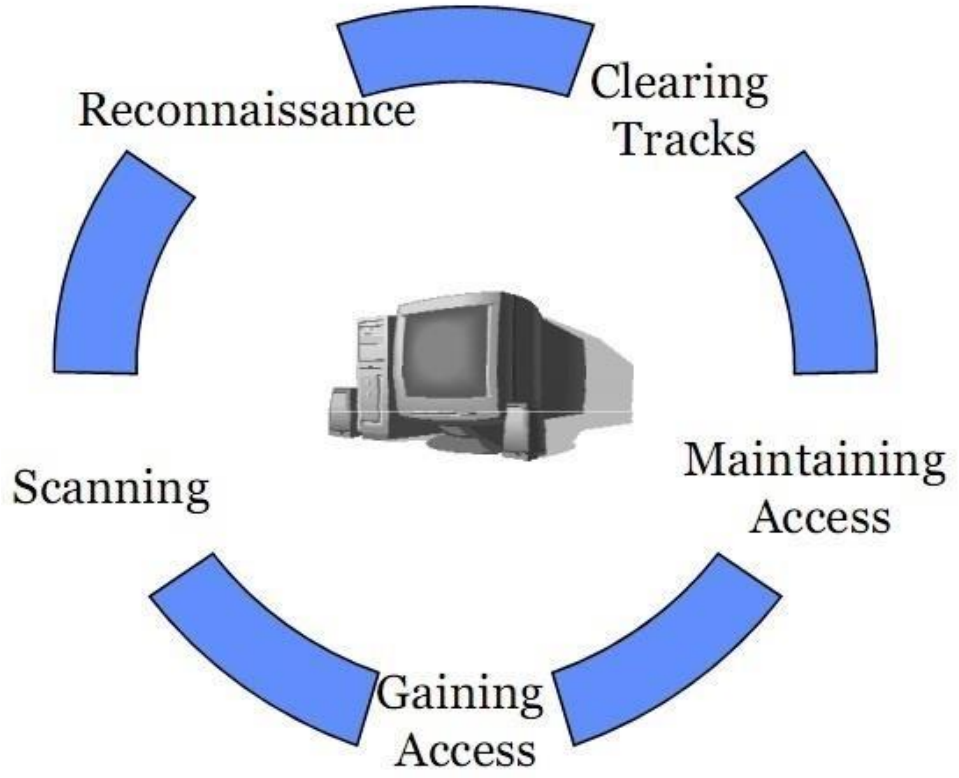
1.7.4 Potential Security Threats to Your Computer Systems

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify computer security threats is the first step in protecting computer systems. The threats could be intentional, accidental or caused by natural disasters.

1.8 Phases involved in hacking

The five phases of Hacking are as follow:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks



1.8.1 The Five Phases of Hacking

Reconnaissance: - This is the primary phase where the Hacker tries to collect as much information as possible about the target. It includes identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc.

Scanning: - It involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase can include diallers, port scanners, network mappers, sweepers, and vulnerability scanners. Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts.

Gaining Access:- After scanning, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. Examples include stack based buffer overflows, denial of service (DoS), and session hijacking.

Maintaining Access: - Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system.

Covering Tracks: - Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include steganography, the use of tunnelling protocols, and altering log files.

1.8.2 Role of Ethical Hacker

As serious security professionals, we almost give “similar security talk” to other business teams in other organization regarding anti-virus definitions, VPNs, encryption, mobile security, social media security, hacking, and so on. But when these security measures are not taken seriously, they fall apart.

This is when vulnerabilities set in and malicious elements seize the opportunity to penetrate the system.

Now comes the “certified ethical hacker”, whose primary job is to attack his own organization’s system to weed out vulnerabilities before “real hackers” do. The adrenaline rush of being an ethical hacker is unparalleled. Though an ethical hacker's role is similar to that of a “penetration tester”, it involves broader duties. "The term ethical hacking is said to have been coined by IBM” (White hat (computer security).

1.8.3 Common Hacking Methodologies

The most common methods used by intruders to gain control of home computers are briefly described below.

1. Trojan horse programs

Trojan horse programs are a common way for intruders to trick you (sometimes referred to as "social engineering") into installing "back door" programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus.

2. Back door and remote administration programs

On Windows computers, three tools commonly used by intruders to gain remote access to your computer are BackOrifice, Netbus, and SubSeven. These back door or remote administration programs, once installed, allow other people to access and control your computer.

3. Denial of service

Another form of attack is called a denial-of-service (DoS) attack. This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

4. Being an intermediary for another attack

Intruders will frequently use compromised computers as launching pads for attacking other systems. An example of this is how distributed denial-of-service (DDoS) tools are used. The intruders install an "agent" (frequently through a Trojan horse program) that runs on the compromised computer awaiting further instructions. Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch a denial-of-service attack on another system. Thus, the end target of the attack is not your own computer, but someone else's - your computer is just a convenient tool in a larger attack.

5. Unprotected Windows shares

Unprotected Windows networking shares can be exploited by intruders in an automated way to place tools on large numbers of Windows-based computers attached to the Internet. Because site security on the Internet is interdependent, a compromised computer not only creates problems for the computer's owner, but it is also a threat to other sites on the Internet. The greater immediate risk to the Internet community is the potentially large number of computers attached to the Internet with unprotected Windows networking shares combined with distributed attack tools.
Another threat includes malicious and destructive code, such as viruses or worms, which leverage unprotected Windows networking shares to propagate.
There is great potential for the emergence of other intruder tools that leverage unprotected Windows networking shares on a widespread basis.

6. Mobile code (Java/JavaScript/ActiveX)

There have been reports of problems with "mobile code" (e.g. Java, JavaScript, and ActiveX). These are programming languages that let web developers write code that is executed by your web browser. Although the

code is generally useful, it can be used by intruders to gather information (such as which web sites you visit) or to run malicious code on your computer. It is possible to disable Java, JavaScript, and ActiveX in your web browser.

7. Cross-site scripting

A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.
You can potentially expose your web browser to malicious scripts by following links in web pages, email messages, or newsgroup postings without knowing what they link to using interactive forms on an untrustworthy site
viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags.

8. Packet sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require administrator-level access.
Relative to DSL and traditional dial-up users, cable modem users have a higher risk of exposure to packet sniffers since entire neighbourhoods of cable modem users are effectively part of the same LAN. A packet sniffer installed on any cable modem user's computer in a neighbourhood may be able to capture data transmitted by any other cable modem in the same neighbourhood.

1.9 What is a Profile?

According to Rogers (2000d), “hackers are not a homogeneous group” In addition, “there is no generic profile of a hacker.”Voiskounsky et al. (2000) claimed that hackers derive from the heterogeneity of the population of the hacker community in Russia. Many researchers tried to categorize hackers into several subgroups depending on diverse characteristics (see Rogers, 2000b).

Landreth (1985) defined the hacker community as novice, students, tourists, crasher, and thief based on the activities hackers were involved in. The novice is thought to be the least experienced and the person who makes petty mischief. The student group is considered those who easily get bored and are

unchallenged at school and who try to explore others' computer systems at home.

Hollinger (1988) claimed that people involved in hacking activities should fit into three categories: pirates, browsers, and crackers. The pirates have a low level of hacking techniques. They are limited to pirate computer software. The browsers have middle level of technical ability and are able to access to individuals' personal files. They usually 9 don't destroy files. The crackers have the best hacking techniques and are considered the most serious abusers.

Goodell (1996) maintained that hackers can be divided into three groups: hackers, crackers, and phreakers. Hackers are involved in hacking to obtain knowledge and satisfy intellectual curiosity. Crackers usually commit destruction, vandalism, and defacement on web pages. Phreakers are mainly interested in manipulating and attacking the telephone system.

Chandler (1996) categorized hackers into four different generations. The first generation of hackers was smart and techno-oriented students, programmers, and computer scientists from MIT. They were interested in hacking for academic and professional curiosities. The second generation of hackers was more likely to be technological radicals. They made "blue boxes" that allowed a person to get long distance telephone service without charge.

Chantler (1996) categorized hacker groups into three sub-groups: elite, neophytes, and losers (lamers) based on hackers' attributes such as hackers' activities, their prowess at hacking, their knowledge, motivation, and how long they had been hacking. The elite group has a high level of hacking techniques and desires to achieve self-discovery and enjoys the excitement and challenge. The neophytes have moderate level of hacking skill and still learn more knowledge about hacking. The losers (lamers) don't have intellectual 10 knowledge and mainly use hacking skill for a desire for profit, revenge, theft, and espionage.

Power (1998) indicated that hackers can be categorized into sport intruders, competitive intelligence, and foreign intelligence. The sport intruders break into computer servers, deface web pages, and damage files. The competitive intelligence tries to avoid illegal hacking and unethical activities and mainly fall into the realm of competitive espionage (Rogers, 2000b). The foreign intelligence is involved in hacking activities for the purpose of a nation's security or economic interests.

Parker (1998) subdivided hackers into seven profiles of cybercriminals: pranksters, hackersters, malicious hackers, personal problem solvers, career criminals, extreme advocates, and malcontents, addicts, and irrational and

incompetent people. Pranksters are referred to people who perpetrate tricks on others. They seldom inflict harm on others.

Adamiski (1999) noted that hacker community has a loose hierarchy, and this is composed of the elite, ordinary, and darksiders. The elite have a high level technique so that they can make software and attack tools. The ordinary hacker group is similar to crackers. They are involved in breaking into computer systems and attacking telephone 11 company computer switches. The darksiders are engaging in financial gain through hacking.

Rogers (2000b) classified the hacking community in seven distinct categories: newbie/tool kit (NT), cyber-punks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC), and cyber-terrorists (CT) depending upon level of technical ability. The NT has limited computer skills and use tool kits2 to conduct attack. The CP category is made up of hackers who usually have better computer skills. They can make basic levels of their own software; they also intentionally engage in defacing web pages or send "Spam" mails.

1.10 The Hacking Mindset

The idea that looking for magic shortcuts, and "hacks" might be related to the belief that one is special or doesn't need to put in long hours of demanding work in order to achieve something.

I'd like to expand on this idea a bit and explain why we think the "hacking" mentality (in language learning or even "life" itself) may actually be a sign of a fixed mindset. If you have a fixed mindset, you don't like being told that things require hard work and sustained effort. After all, you're special. You should be able to achieve success without effort, because you inherently deserve it.

1.10.1 The Hacker Mindset

The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music. Actually, you can find it at the highest levels of any science or art. Software hackers recognize these kindred spirits elsewhere and may call them hackers too and some claim that the hacker nature is really independent of the particular medium the hacker works in.

1.11 The Basic Difference between Hackers and Crackers

Hacker: A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

Cracker: A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data; deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.

1.12 Skills Required Becoming an Ethical Hacker

Skills allow you to achieve your desired goals within the available time and resources. As a hacker, you will need to develop skills that will help you get the job done. These skills include learning how to program, use the internet, good at solving problems, and taking advantage of existing security tools.

1.13 Ethical Hacking- Advantages and Disadvantages

Advantages of Ethical Hacking

Most of the benefits of ethical hacking are obvious, but many are overlooked. The benefits range from simply preventing malicious hacking to preventing national security breaches. The benefits include:

- Fighting against terrorism and national security breaches
- Having a computer system that prevents malicious hackers from gaining access
- Having adequate preventative measures in place to prevent security breaches

Disadvantages of Ethical Hacking

As with all types of activities which have a darker side, there will be dishonest people presenting drawbacks. The possible drawbacks of ethical hacking include:

- The ethical hacker using the knowledge they gain to do malicious hacking activities
- Allowing the company's financial and banking details to be seen
- The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system
- Massive security breach

1.14 Let us Sum up

Hacking is identifying and exploiting weaknesses in computer systems and/or computer networks. Cybercrime is committing a crime with the aid of computers and information technology infrastructure. Ethical Hacking is about improving the security of computer systems and/or computer networks. A threat is any activity that can lead to data loss/corruption through to disruption of normal business operations. There are physical and non-physical threats Physical threats cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters. Non-physical threats target the software and data on the computer systems. Finally we have learnt that Programming skills and Networking skills are essential to becoming an effective hacker. Hacking tools are programs that simplify the process of identifying and exploiting weaknesses in computer systems.

1.15 Self Assessment Questions

1. What is hacking?

……
……
……
……
……

……
……
……
……
……

2. Explain difference between hackers and crackers.

……
……
……
……
……
……
……
……
……
……

3. What is cybercrime?

……
……
……
……
……
……
……
……
……
……

4. What is security threat?

……
……
……
……
……
……
……
……
……
……

5. What is ethical hacking?

……
……
……
……
……

……
……
……
……
……

1.16 Model Questions

1. Explain about deference types of hacker.
2. What is the legality in ethical hacking?
3. Explain about the concept of ethical hacking.
4. Write about the role of ethical hacking.
5. Write about Basic Difference between Hackers and Crackers.
6. Write about Advantages and Disadvantages Ethical Hacking.

1.17 References & Further Readings

1. http://www.guru99.com/learn-everything-about-ethical-hacking-tools-and-skills.html
2. http://cdn.ttgtmedia.com/searchNetworking/downloads/hacking_for_dummies.pdf
3. http://picateshackz.com/2015/04/understand-hacker-mindset-to-become-real-hacker.html#G2EfK2R3iPelK6Hx.99
4. The hacker mentality: exploring the relationship between psychological variables and hacking activities by hyung-jin woo (under the direction of joseph r. Dominick).

UNIT-2 Footprinting & Reconnaissance

Unit Structure

2.0 Introduction

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Footprinting where we collect public information and building a map of the server or domain objective, without interacting direct with it.Footprinting where there is active target identification through and techniques such as port scanning, and different identifications of services, operating systems and server banners. Footprinting is one of the most important techniques security auditing, since allows them gather information about the target we are analyzing.

2.1 Learning Objective

After learning this unit you should be able to

- Know about what is Footprinting.
- Learn about footprinting terminologies
- Know about the different type of footprinting.
- Study about tricks and techniques of footprinting.
- Identify the footprinting threats.
- Understand the process of Information Gathering.
- List the advantages and some weaknesses of information gathering.
- Learn about the basic concepts Hacker Methodology.
- Know the Ethical Tools used for the reconnaissance phase.

2.2 What is Footprinting?

Footprinting is basically the first step of the hacking which is used by Hackers and penetration testers for gathering information about a server where a website is hosted, A hacker does footprinting in-order to find weakness and security holes of the server through which it can be rooted (Hacked) and same is the Job of penetration tester but often hackers do this for bad purpose but a penetration tester is hired to do this in order to increase security. The purpose of footprinting to learn as much as you can about a system of the server, it's remote access capabilities, its ports and services which are running behind it, Registrar queries, DNS queries, and the aspects of its security. All kinds of Hacking Must start with footprinting if you are

targeting a specific server and system. This is the start of a successful attack on a system, and you can get much information depending upon your skills.

2.3 Footprinting Terminologies

Footprinting is the process of using various tools and technologies to understand and learn the best way to attack a target. Attackers find out as much as possible without actually giving themselves away. They find public information or appear as normal users. The attacker/hacker does a 'whois' lookup to find as much information as possible about the network along with the domain name. They might stroll through your DNS tables using nslookup, dig, or other utilities to do domain transfers to find the names of machines. The hacker/attacker browses other public information looking for the public web site and anonymous FTP sites. Specifically, hackers/attackers look for domain names, network blocks, particular IP addresses, networking protocols in use, internal domain names, IDSs (Intrusion Detection Systems), telephone numbers, ACLs (Access Control Lists), etc. Footprinting is necessary to identify the above listed items. Hackers use this information to attack. Security personnel can use it to strengthen their security stance.

2.3.1 Uses of Footprinting

Footprinting is a necessary evil. What does that mean? Successful hackers are building their information database about your company's security weaknesses. Wouldn't be nice to know these weaknesses in advance to take proper action? Yes, it would be nice. Therefore, security personnel need to add footprinting to their already long task list. One has to remember that an organization's security is a process, not a technology. A good security system provides multiple layers of security. The system would be defined as "a collection of things or elements which, working together, produce a result not achievable by the things alone."

It allows a hacker to gain information about the target system. This information can be used to carry out further attacks on the system. That is the reason by which it may be named a Pre-Attack, since all the information is reviewed in order to get a complete and successful resolution of the attack.

2.3.2Crawling

Crawling is the process of surfing the internet to get the required information about the target. The sites surfed can include the target's website, blogs and social networks. The information obtained by this method will be helpful in other methods too.

2.4 Types of Footprinting and their Explanation

Below are types of footprinting and their sub-branches:-

2.4.1 Open Source Footprinting

It is a type of safest footprinting as it is in legal limits and you can do it without any fear that if you are doing any kind an illegal task. It includes finding basic information which is majorly present for public use too, Like finding out the phone numbers, Emails Addresses, performing who is request for the domain name, searching through DNS tables, and scanning certain ip addresses through automated tools (I,ll post them later with detailed info, of usage), and searching out some common means of finding information about the server system and owner.

Many of the companies post a large amount of information about them self at the their own website without realizing the fact that it can be useful for a hacker too, also sometimes in HTML and coding comments are present which themselves give hackers a lot of information about coding. As comments are present their to tell a coder about the function of some specific code.

2.4.2 Network Enumeration

Network enumerating is a computing activity in which user names and info on groups, shares and services of networked computers are retrieved. It should not be confused with Network mapping which only retrieves information about which servers are connected to a specific network and what operating system is run on them. It includes identifying the domain name and also searching for the registrar information since companies domains are listed with registrar information. The hacker simply needs to know which registrar the company is listed with. There are five types of queries listed under.

Registrar Queries:

Registrar Queries or WHOIS (pronounced as the phrase who is) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.

Organizational Queries:

This is searching a specific registrar to obtain all instances of the target's name. The results show many different domains associated with the company as it may use a large number of domains with its dedicated server or system you can say.

Domain Query:

A domain query is based off of results found in an organizational query. Using a domain query, you could find the company's address; domain name, administrator and his/her phone number, and the system's domain servers as while registering a domain this is included in registration forum. The administrative contact could be very useful to a hacker as it provides a purpose of how to do social engineering. So this is where social engineering comes into play. Many administrators now post false phone numbers to protect themselves from this so that they may not be fooled so easily.

POC Query:

This query finds the many IP addresses a machine may have which are majorly public and are associated with machine.

DNS Interrogation:

After gathering the information needed using the above techniques, a hacker would begin to query the DNS using tools. A common problem with system administrators is allowing untrusted, or worse, unknown users, to perform a DNS Zone Transfer. Many freeware tools can be found on the internet and can be used to perform DNS interrogation. Tools such as nslookup, for PC, and AGnet Tools, for Mac, also in Linux flavor many open source applications are present for this purpose.

2.5 Similar Common Tricks And Techniques Regarding Footprinting

2.5.1 OS Identification

This involves sending illegal ICMP (Internet Control Message Protocol) or (TCPTransmission Control Protocol) packets to a machine for identifying Operating system used on server or machine in simple words.

2.5.2 Ping Sweep

Try Pinging Different IP addresses found by you during Footprinting:-

Try Pinging Different IP addresses found by you so that you may figure out that which IP is alive in-order to scan for open ports later.

2.5.3 Performing TCP Scans

Scan ports on machines to see which services are offered by system. TCP scanscan be performed by scanning a single port on a range of IPs (Many IPs But checking one port on them), or by scanning a range of ports on a single IP (Many Ports but on a single IP). Both techniques will produce helpful information for hacker and you.

2.5.4 Performing UDP Scans

Send garbage UDP packets to a desired port. Well normally don't perform

UDP scans a whole lot because most machines show and reply with an ICMP 'port unreachable' message. Meaning that no service is available, most of the advanced machines and servers show this behavior.

2.6 Footprinting Threats

Attackers gathers valuable system-level information such as account details, OS and other software versions, server names, and db schema details from footprinting techniques.

Threats include:

- Business loss
- Corporate espionage
- Privacy loss
- Social engineering
- System and network attacks
- Information leakage

2.7 Information Gathering

2.7.1 What is Information Gathering?

Information gathering helps the individual and the organization to undertake complicated tasks that would otherwise be extremely hard to accomplish if not out rightly impossible without the benefit of gathered information. As defined in the dictionary, information gathering is the act of collecting information from various sources through various means.

In the literal sense, information gathering is a basic human skill necessary for undertaking basic human activities such as eating, sleeping, working etc. For

in order to eat, one must know if the food is edible or not; and in order to sleep, one must know if the sleeping place is comfortable or not.

As applied in the fields of business and other specialized organizations (scientific, military, academic) however, information gathering is an advanced skill which requires the training and education of personnel in the procedures and methods of gathering information from sources that are of higher level than ordinary sources. In the case of interviewing personalities for example, a researcher usually gets to interview authorities and proper officials, and thus, he must know the proper ways to address distinguished personalities of the community and the society in general.

In general practice, information gathering is the collection of data for dealing with the individual's or the organization's current situation. More data means more and better ways of dealing with the current situation. More data broadens the minds of those who will use the data to solve current organizational problems. New ideas come more easily if there are lots of facts to be used as bases.

There are two main types of sources in the field of information gathering, namely:

- **Existing sources –** existing sources are those sources of information that can be found in the printed, in video, in audio and other materials that are available to the public or upon request to proper bureaucracy.

- **Natural sources –** natural sources are first hand sources such as those who have tried products, services and methods, and expressing their experience and opinions to the researcher.

2.7.2 Who undertakes information gathering and why

Information gathering is an assignment of the research specialist within the organization's intelligence department. They are the personnel properly trained and equipped to carry out the research tasks in the most efficient manner. The proper handling of data requires methods and procedures unique to the field of information gathering. Research personnel do this task unequivocally thru skills like data sifting, intelligent questioning, and other research skills. Other company personnel can also do their own information gathering on the personal level to improve their job performances and as a self-help tool. Researchers undertake information gathering in order to:

- Broaden the scope of knowledge of the organization
- For the development of particular skills
- To reduce the apprehension caused by the unknown
- For a higher level of understanding of special subjects

- And obviously, for solving problems

Additionally, on the non-professional aspect of the research undertaking, information can also give inspiration and entertainment.

2.7.3 How to Undertake Information Gathering

In order to implement a good information gathering design, a step-by-step approach is advisable for any researcher to follow:

- **Analyzing the problem –** The researcher needs to identify the purpose and the process of the research he is doing. For whom is he doing it and why? These questions and more needs to be answered right at the start of the research.

- **Identifying the sections of the information gathering –** Before going through with the process of information gathering, a sectioning of the general outline of the task can be helpful. Sections such as those classifying the recipients of the data, the detailing of the specific questions that needs to be answered, and also the setting of the knowledge levels of the team members involved facilitates an easier to follow research program.

- **After the outline of the research task-** The researcher may then set the actual plan of activities needed to carry out the information gathering tasks. Questions such as: Where to go to for the research? What materials need to be invested in? What skills are needed to be implemented? And the details of the research materials like the availability, languages, location and accessibility needs some suasion.

- **The gathering methods and tools –** The tools that are involved in information gathering such as data storage devices and publications have their own set of required skills that the researcher must readily possess or is capable of having. Languages contained in publications could pose a problem and data storage devices could have proprietary names. And names, as we all know in the computer industry means lots of adjustments.

- **Begin the gathering –** During the gathering of the data, the researcher encounters various amounts of information that may or may not be relevant to the present subject of the research. He must sift through all of these carefully.

- **Review and record the data obtained –** a recording that includes everything from the start to the end of the gathering process must be

set in writing to provide all the information that the organization needs.

2.7.4 Advantages and Some Weaknesses of Information Gathering

Information gathering, per se, delivers a great deal of advantage to the organization undertaking it. Due to its enlightening nature for example, the researcher and his organization catches a better glimpse of other people's situations. They are able to empathize with other people if they knew better. Better alternatives in problem solving are also in the offing upon learning of mistakes already committed by other parties.

On the down side, with the proliferation of massive amounts of data in the Internet, any researcher who took up gathering of information in the Internet can suffer from information overload. There's just no absolute lead with information gathering in the Internet and pursued leads might lead to the doldrums in information gathering.

2.7.5 Best ways of information gathering

An organization reduces the stress on itself if it has an efficient means of information gathering. And for that efficiency to take place, some key points in the practice of information gathering needs to be stressed:

- A Staff needs to be organized and distributed to take on specific assignments.
- They also must be trained in the different approaches to inquiring.
- Everyone involved must be constantly updated in the ongoing research project
- With interviews, the information gathering staff should have good questioning skills
- Creativity, inventiveness and adaptability are key qualities that bring progress to the gathering of information.

2.7.6 Team reporter facilitates information gathering

Team reporter is a web based email application that updates everyone on the team especially remote working teams about project status and the progress the team is making on it. Each member of the remote working team submits a report on his expertise via email that Team reporter automatically sends to

each member. Members can gather information about the whole project and the team with Team reporter. All these Team reporter undertakes by means of the following procedures:

- Creating questions that the team members will answer.
- Tailoring the questions to be asked to fit project needs
- Scheduling the sending out of email queries.
- Team members replying with their status reports.
- Upon receiving individual team member reports, scheduling of overall status updates to every team member.
- Adopting preset business scenarios.
- Prompting team members who forget their reports.
- Arranging an archive of team status reports

Team reporter has the following advantages:

- Ready in 5 minutes
- Free start-up
- Accessible even to novice users and managers
- No IT software or hardware requirements
- Only email login required for Team members

2.8 Finding information in a Company's URL

There are three ways to get a great URL. The first is with magical inspiration: that perfect and available name comes to you in the shower. The second is with a ton of money, by buying an existing domain. The third (if inspiration and money are lacking) is with the process outlined below, which may yield a workable name. These days, you start with the URL and then check that some variation of the company name is available (for registration purposes). That part is relatively easy.

2.8.1 Relax (But Avoid Really Horrible Ones)

URLs matter a lot less than it would seem when you are starting out. One can think of plenty of terrible names that did great and vice versa. We are now moving away from destination sites. Search engines and browser capabilities, such as Firefox's awesome bar, will help people find you.

If you are relying on a great name to build traffic doesn't. Unless you have a lot of money to buy an existing domain and that is probably not a good use of your cash there are cheaper ways to build traffic.

So then, “okay” is good enough. Don’t obsess over the URL. Save your obsessing for usability design. But avoid the real stinkers, the names that make people laugh at you and then ignore you. We live in a global world, too, so do check that your great URL does not mean “Your mother is a mangy dog” in Chinese, French, or whatever.

2.8.2 Process for Getting a Great URL

Here is the three-step process:

1. Go for a run (or whatever exercise you enjoy doing).
2. Have a double espresso.
3. Do something totally relaxing, like petting your cat, to clear your mind and let inspiration set in.

Did that do the trick? No? Try the longer process:

1. Choose some “themes” that relate to your biz.
2. Brainstorm with some pals to come up with a really long list of words that vaguely relate to those themes.
3. Use bulk registration to test a lot of them. Make a shorter list of what is available with .com.
4. Check that shorter list against:
   - a trademark search on uspto.gov,
   - some people who will give you an honest response,
   - a few major languages for the “mangy dog” test.
5. If that cut leaves you short, go back to some of the names you like and try them out with .net. In some cases .net is okay, particularly if the .com name is owned by someone small and non-competitive whom you can buy out later.
6. Still coming up short? Try country extensions. For example, if you want rabbit.com, try rabbit (Italy). This is risky. It sounds clever and occasionally works, but mostly confuses people.
7. Once you get a viable list of three that check out, buy all three and then test, test, test. And test with as broad a community as you can get. Use Twitter, your blog, whatever connects you to your network quickly. And go outside your network.
8. If all three fall short of this last hurdle, start from the top: go for a run, double espresso, etc. Allow time for this. The best ideas come at the oddest times and usually when you are thinking of something else.
9. When you find your chosen one:
   - Register the trademark at uspto.gov.
   - Protect major country extensions, .net, .info, and other extensions that a squatter or competitor may try to take if they see you get traction.

- Create a logo that works.
- Ensure the company name is available. In the worst case, CoolSite.com could be run by Boring Company LLC doing business as (DBA) CoolSite.com.

10. Go, End, go!

2.9 The Hacker Methodology

Many newbie hackers seem to be confused regarding the process or methodology to employ a successful hack. Most want to simply go straight to the exploit without doing the due diligence to make certain that the hack will work and you won't get caught.

Here, I want to lay out for you the proper methodology, with example tools and techniques for a hack, from start to finish.

Step 1: Performing Reconnaissance

Good reconnaissance is critical to great hacking. In general, a good hacker wills recon for about 2 to 3 times longer than he/she would performing the actual hack. It's not unusual to spend weeks or months gathering information before even beginning to attempt an exploit.

Most exploits are dependent on operating systems, applications, ports, and services, so you need to gather this information before you start hacking. If you don't, you will likely fail, get caught, or both. I can't emphasize this enough. Newbie hackers are always so anxious to get to the exploit that they often ignore this phase of the attack.

Recon can be broken into at least two categories, passive and active.

Passive Reconnaissance

Passive reconnaissance can be defined as gathering information about the target without actually "touching" the target, or in a way that looks like normal traffic.

It is use Netcraft to gather info about websites, such as the web server, operating system, last reboot, and other technologies. All of this information is critical before starting the hack.

In addition, passive reconnaissance can include DNS and SNMP mining, dumpster diving, social engineering, using social media such as Facebook and LinkedIn, and of course, Google hacking, among other techniques.

Active Reconnaissance

Active reconnaissance is information gathered about the target by actually sending packets to the target and evaluating the response. The results of active recon are much more specific and reliable, but also much riskier. Anytime we send a packet to a site, our IP address is left behind.

Nmap, Hping, Netdiscover, P0f, and Xprobe2 are among the many tools we can use to gather info on remote targets that can be useful in revealing open ports, running services, and operating systems.

Active recon can also include enumeration of the network. Techniques such as banner grabbing and the use of vulnerability assessment tools such as Nessus, Nikto, and Retina are also often a part of this phase.

Step 2: Gaining Access (Exploitation)

Exploitation can take many, many forms, and the successful hacker will use their imagination to come up with multiple attack vectors. Metasploit is an excellent tool for exploitation, but don't fall in love with it. As soon as Metasploit develops new exploits, the AV software manufacturers immediately begin developing a new signature for it.

Once you have done thorough recon and know all the ports, services and apps, try looking into the vulnerability databases such as SecurityFocus, TechNet, and others for known vulnerabilities and exploits.

Be creative and think about all of the protocols that the system or network uses and how they might be abused. Always consider the possibility of a man-in-the middle attack and never overlook the good social engineering attack.

Step 3: Privilege Escalation

Very often, we can get access to the system or network, but only with the privileges of an ordinary user. This happens often when we use a client-side attack, where we are attacking an ordinary user's vulnerable applications, such as the web browser, Adobe Flash, Adobe Reader, etc.

Ultimately, we want root or sysadmin privileges that will give us unfettered access to the entire network. This is where we need to escalate privileges. Furthermore, if we have a legitimate account on a website or LAN, we may be able to escalate its privileges to gain root or sysadmin.

In some cases, if we have been able to compromise one system with user privileges on the network, we can pivot from that single system to compromise another system with system privileges.

If you can get the Metasploit Meterpreter on the system, the meterpreter has a command "getsystem" that iterates through 15 known privilege escalation methods to gain system admin privileges.

Once again, do not downplay or ignore the possibility of using social engineering techniques to gain system admin privileges by, in many cases, asking for the password under the proper context.

Step 4: Leaving Behind a Backdoor or Listener

Once we have successfully exploited the system and then escalated our privileges to sysadmin or root, it will be necessary to leave behind a listener or rootkit. This listener, ideally, will persist beyond when the system is rebooted and will be there when we want to come back to the system and continue to use/exploit/extract.

This listener can take many forms, such as Netcat, a command shell, VNC, Meterpreter, etc.

Step 5: Extracting Data

Ultimately, the primary reason for exploiting/hacking a machine is to gain access and extract or exfiltrate data. This can be credit card data, personally identifiable information (PII), intellectual property, or other valuable information.

To do so, we need a way to remove the data in a way that is not readily noticeable by the sysadmin, and ideally, encrypted. Recub and Cryptcat are two tools that can remove data stealthily.

Metasploit'sMeterpreter also has an upload and downloads command for uploading malicious software and downloading critical and valuable data.

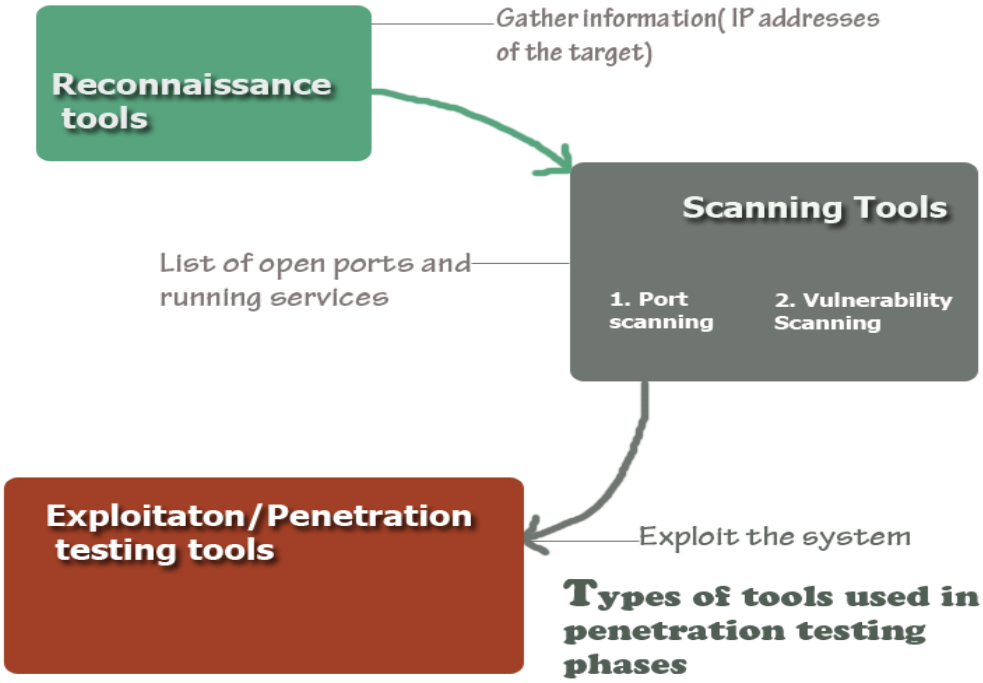
Step 6: Covering Your Tracks

To make certain that our exploits don't lead back to us, we need to cover our tracks. This can take many forms such clearing log files, removing any software we uploaded, removing our command history, etc. Metasploit'sMeterpreter has a killav script to disable antivirus software, as well as a cleared command that removes the event logs on Windows systems.

2.10 Tools Used For The Reconnaissance Phase

In footprinting or reconnaissance phase, a penetration tester collects as much information as possible about the target machine. The primary purpose of this phase is to gather intelligence so as you can conduct an effective penetration

test. At the end of his phase, you are expected to have a list of IP of your target machine that you can scan later on.



2.10.1 Reconnaissance /Footprinting Tools

Reconnaissance can be either active or passive. In active reconnaissance you send traffic to the target machine while a passive reconnaissance uses Internet to gather information. When you use active reconnaissance, you need to remember that the target machine may notice that you are planning a penetration test. In the case of passive test, target machine has no clue about who is gather intelligence and planning an attack. The following are the tools you can use:

1. **Google:** use advanced Google search to gather information about the target's website, webservers and vulnerable information. Sometimes, jobs posted in the companies' websites reveal valuable information about the type of information technologies used in the target company.

2. **The harvester:** you can use it to catalogue email address and subdomains. It works with all the major search engines including Bing and Google. This is a build in tool of Kali Linux.

3. **WHOIS:** to get information about domains, IP address, DNS you can run whois command from your Linux machine. Just type whois followed by the domain name:

Whois yourdomain.com

Alternatively, you can visit whois.net and type the domain name of your target.

4. **Netcraft:** they have a free online tool to gather information about webservers including both the client and server side technologies. Visit http://toolbar.netcraft.com/site_report/ and type the domain name.

5. **Nslookup:** you can use it to query DNS server in order to extract valuable information about the host machine. You can use this tool both in Linux and Windows. From your windows machine, open the command prompt and the type 'nslookup' followed by the domain name.

6. **Dig:** another useful DNS lookup tool used in Linux machine. Type dig followed by the domain name.

7. **MetaGoofil**: it's a Meta data collection tool. Meta data means data about data. For instance, when you create word document in Microsoft word, some additional information are added to this word file such as file size, date of creation, the user name of the creator etc.-all these additional information is called meta data. MetaGoogle scours the Internet for metadata of your target. You can use it with both Linux (built in Kali Linux) and Windows.

8. **Threatagent drone:** it is a web based tool. You need to sign up at https://www.threatagent.com/ and type the domain name that you want to reconnaissance. Once the drone extracts all the information about your target, it will create a complete report about the target, which will include the IP address range, email address, point of contacts etc.

9. **Social engineering**: it is perhaps the easiest way to gather information about an organization. You can find lots of free information about social engineering in the Internet. Depending on the types of information you need about your target organization, you need to choose the appropriate technique. But remember that this technique needs time to master and you need to plan it very carefully, otherwise your activity can easily trigger an alert.

   After gathering solid information about the target, the next step is to start scanning the target system.

Scanning Tools

A pen tester scans the target machine in order to find the weakness in the systems. The two major activities of the scanning phase are port scanning and vulnerability scanning.

Port scanning helps to identify a list of opened ports in the target and based on the list of ports you can determine what types of services are running in the system.

The second step in scanning is to run a vulnerability scan to identify specific weakness in the software and services running in the servers.
At the end of port scan you will have the following information:

- Number and type of opened ports
- Type of services running in the servers
- Vulnerabilities of the services and software

10. Nmap: If you have doubt about which tool to use for scanning, use Nmap. This tool creates a complete list of opened ports in your target. You can use is both in Windows and Linux environment. The graphical interface for Windows is called Zenmap, which you can run without learning any command. But, for greater control and granularity for the output, you need to learn the commands.

11. Nessus: Once you find the list of open ports, the next step is start looking for vulnerability in the servers. One of the efficient tools to vulnerability scan is Nessus. Remember that Nessus is not a free tool.

12. Nexpose: if you are looking for a free vulnerability scanner, you can use nexpose community edition from rapid7.

Penetration testing/exploitation

This is the most important phase of a penetration test, which is also known as exploitation because a pen tester makes real attempts to gain access to the target system at this phase.

13. MEDUSA: you can use it to gain to the authentication services in the target machine. Medusa can authenticates with a number of popular services such as FTP, HTTP, IMAP, MS SQL, MySQL, PCAnywhere, POP3, RLOGIN, SMTPM, Telnet, SSH, VNC etc. before using Medusa you need to have several information in your hand such as username, target IP address, a password file(a dictionary file containing a list of popular and widely used passwords).

14. Hydra: this is another useful tool like Medusa used to break authentication system.

15. Metasploit: it can be considered one of the finest open source exploit in the world. The best thing about Metasploit is that it is free. If you are planning to become an open tester and what to learn exploitation, you can start using metasploit without any hesitation. On the other hand, an exploitation tool like Metasploit is a real exploit. When an exploitation tool discovers any vulnerability, it exploits it immediately, which may cause severe damage to the system or can cause network disruption. So, take extra care when playing with any such tools.

2.11 Let us Sum Up

According to Christine Orshesky, there is an increasing need for corporations to protect themselves from computer viruses and other things that bump around the on-line community. Denial of Service attacks and widespread virus infections have raised the issue of 'due care'. No longer is it reasonable to rely solely on the installation of antivirus products to protect the on-line environment. A holistic approach that provides the corporation with an integrated and layered security posture is necessary to achieve protection – including policy, procedures, awareness, and technology. There are many devices available to the hacker to footprint any company's network. Use these tools to find the weaknesses before they do. Therefore, you can prepare an organized approach to your layered security. Never try to use the above mentioned tools in a network or system without authorization from the proper authority. The intention of the post is to help the IT professional who also wants to learn and develop a career in penetration testing.

2.12 Self Assessment Questions

1. What is footprinting in hacking?

……
……
……
……
……

2. What are the footprinting threats?

……
……

……
……
……

3. Explain about Open Source Footprinting.

……
……
……
……
……

4. Write about sort note Information Gathering.

……
……
……
……
……

5. How to undertake information gathering?

……
……
……
……
……..……

2.13 Model Questions

4. Explain about Advantages and Disadvantages of information gathering.
5. Explain about TCP Scans.
6. Explain different Types of footprinting.
7. Write about Tools used for the reconnaissance phase.
8. What are the Hacker Methodology explain it.

2.14 References & Further Readings

1. http://www.teamreporterapp.com/information-gathering/
2. https://null-byte.wonderhowto.com/how-to/hack-like-pro-hacker-methodology-0155167/
3. https://hackertarget.com/brute-forcing-passwords-with-ncrack-hydra-and-medusa/
4. http://resources.infosecinstitute.com/penetration-testing-intelligence-gathering/#gref

UNIT-3 System Hacking

Unit Structure

3.0 Introduction

Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. Computer hacking is the practice of modifying computer hardware and software to accomplish a goal outside of the creator's original purpose is most common among teenagers and young adults. System Hacking actually involves gaining access and changing the integrity of the system. In this unit, you'll learn the basics of gaining access to a system, how authentication works, and how & when to use that to your advantage.

3.1 Learning Objective

After learning this unit you should be able to

- Know about System hacking.
- Know about different type of System hacking.
- Learn different types of tools used by hackers.
- Study about hacking process.
- Differentiate between hacking and cracking.
- Differentiate Legal Hacking and illegal hacking.
- Know about various methods for password cracking.
- Learn about keystroke logger.

3.2 What is System Hacking

System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. This unit explains the main methods of system hacking password cracking; privilege escalation, spyware installation, and keylogging and the countermeasures IT security professionals can take to fight these attacks. Security expert Lisa Bock also covers Steganography, spyware on a cell phone, and tactics for hiding tools.

3.3 Types of System Hacking

There are of four types of password attack

1. Passive online attack
2. Active online attack
3. Offline attack
4. Non-technical attack

1. Passive Online Attack

In passive online attacks an attacker don’t contact with authorizing party for stealing password, in other words he attempts password hacking but without communicating with victim or victim account. Types of passive online attacks include wire sniffing, Man in the middle attack and reply attack.

2. Active Online Attack

This type of attack can be directly termed as password guessing. An attacker tries number of passwords one by one against victim to crack his/her password.

3. Offline Attack

Offline password attacks are performed from a location other than the actual computer where the password reside or were used. Offline attacks requires physical access to the computer which stores password file, the attacker copies the password file and then tries to break passwords in his own system. Offline attacks include, dictionary attacks, hybrid attacks, brute force attack, pre-computed hash attacks, syllable attacks, rule based attacks and rainbow attacks.

4. Non Technical Attack

This type of attacks does not require any technical knowledge hence termed as non-technical attacks. This kind of attacks may include, social engineering, shoulder surfing, keyboard sniffing and dumpster diving.

3.4 What is Rootkits?

A rootkit is a type of malicious software that is activated each times your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals, network connections, and the keyboard.

Root kit helps hackers to maintain hidden access to the system using virus , Trojan horse, spyware etc.

3.5 Steganography

The art and science of hiding information by embedding messages within other, seemingly harmless messages is called Steganography. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

Steganography sometimes is used when encryption is not permitted. Or, more commonly, Steganography is used to supplement encryption. An encrypted file may still hide information using Steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

3.6 Hacker Tools

There now are more than 100,000 known viruses with more appearing virtually daily. The myriad of hackers and their nefarious deeds can affect any computer owner whether an occasional home user, e-mailer, student, blogger, or a network administrator on site or on the internet. No matter your level of computer use, you must protect your computer, business, or even your identity. The best way to know how to protect your computer is to understand the hacker's tools and recognize their damage.

3.6.1 Hacking Tools

1. Lophtcrack

LophtCrack is a recovery and password auditing tool originally created by Mudge. It tries to crack Windows passwords from obtained hashes from stand-alone Windows workstation, primary domain controllers, networked servers or Active Directory. It can sometimes sniff hashes off the wire. These tools also have several methods of generating password guesses.

Is Lophtcrack Free?

No, 3 versions of LophtCrack: Professional, Administrator and Consultant are available for purchase.

Does LophtCrack Work on all Operating Systems?

No, it only works for Microsoft Windows.

What are the Typical Uses for L0phtCrack?

L0phtCrack is used to recover lost Microsoft Windows passwords or to test someone's password strength. It uses brute force, rainbow tables, and hybrid and dictionary attacks. Even if this one of the tools of choice, crackers' use old versions because of its high availability and low price.

Download from: http://1337x.org/torrent/42867/0/ (use torrent client to download)

2. LCP

Main purpose of LCP program is user account passwords auditing and recovery in

Windows NT/2000/XP/2003. Accounts information import, Passwords recovery, Brute force session distribution, Hashes computing.

A good free alternative to Lophtcrack.

LCP was briefly mentioned in our well read Rainbow Tables and Rainbow Crack article.

Download from:http://www.lcpsoft.com/english/download.htm

3. Hacking windows administrator password of xp/vista/7

This hack will show you how to reset Windows administrator password (for Win 2000, XP, Vista and Win 7) at times when you forget it or when you want to gain access to a computer for which you do not know the password.

Most of us have experienced a situation where in we need to gain access to a computer which is password protected or at times we may forget the administrator password without which it becomes impossible to login to the computer. So here is an excellent hack using which you can reset the password or make the password empty (remove the password) so that you can gain administrator access to the computer. You can do this with a small tool called Offline NT Password & Registry Editor. This utility works offline, that means you need to shut down your computer and boot off your using a floppy disk, CD or USB device (such as pen drive). The tool has the following features.

You do not need to know the old password to set a new one

You will detect and offer to unlock locked or disabled out user accounts!

There is also a registry editor and other registry utilities that works under Linux/Unix, and can be used for other things than password editing.

How it works?

Most Windows operating systems stores the login passwords and other encrypted passwords in a file called same (Security Accounts Manager). This file can be usually found in \windows\system32\config. This file is a part of Windows registry and remains inaccessible as long as the OS is active. Hence it is necessary that you need to boot off your computer and access this same file via boot. This tool intelligently gains access to this file and will reset/remove the password associated with administrator or any other account.

Offline NT Password &Reg Editor Download

It is recommended that you download the CD version of the tool since floppy drive is outdated and doesn't exist in today's computer. Once you download you'll get a bootable image which you need to burn it onto your CD. Now boot your computer from this CD and follow the screen instructions to reset the password.

Another simple way to reset non-administrator account passwords

Here is another simple way through which you can reset the password of any non-administrator accounts. The only requirement for this is that you need to have administrator privileges. Here is a step-by-step instruction to accomplish this task.

1. Open the command prompt (Start->Run->type cmd->Enter)

2. Now type net user and hit Enter

3. Now the system will show you a list of user accounts on the computer. Say for example you need to reset the password of the account by name eldho, and then do as follows

4. Type net user eldho * and hit Enter. Now the system will ask you to enter the new password for the account. That's it. Now you've successfully reset the password for John without knowing his old password.

4. Key-Logger

Keyloggers capture and store all the keystokes which we typed in the system; modern keyloggers can capture system events&activities, screen shotes and clipboard.

Some of them can act as spy too, all the datas will be sending to your mail id.

Download from: http://1337x.org/torrent/47798/0/ (use torrent client to download)

5. USB Keylogger

It capture all the keystrokes by using a USB drive which contain the usbkeylogger software

Download from:http://www.keyghost.com/USB-Keylogger.htm (paided s/w :( )

6. Keyloggerfor Mobile

A Keylogger is program or file that has been executed to record all of the keystrokes a computer. This can be utilized for monitoring all the activities that takes place on a computer and the details will be stored in the software.

Keylogger for S60v3 is used to monitor the keystroke that occurs on your Symbian device when the application is running. The software is written is python language and it requiring its runtime environment for proper working.

7. Spyware

It will capture all the events,activities, website visited, keystroke, and screenshots, from a remote machine to our machine through mail

Download from: http://1337x.org/torrent/47798/0/(use torrent client to download)

8. Openpuff (Stenography Tool)

OpenPuff is a advanced watermarking and Steganography, or data hiding, program capable of storing up to 256MB of encrypted data using an invisible copyright mark in pictures, video, audio, and flash files. OpenPuff supports many carrier formats: images (BMP, JPG, PCX, PNG, TGA), audio support (AIFF, MP3, NEXT/SUN, WAV), video support (3GP, MP4, MPG, VOB) and flash-Adobe support (FLV, SWF, PDF).

Download from: http://embeddedsw.net/zip/OpenPuffv340.zip

3.6.2 Viruses, Exploits, Worms, and More

The term computer "virus" originated to describe machine code command inserted into a computer's memory that, on execution, copies itself into other programs and files on the computer. Depending on the hacker's intent, the design of a virus can merely be an inconvenience or have very serious consequences up to a potential catastrophe.

Generally, a virus is a piece of software, a series of data, or a command sequence that exploits a bug, glitch, or vulnerability. Each example is appropriately termed an "exploit." An exploit causes unintended or unanticipated behavior to occur in a computer's operating system or applications while propagating itself within the computer.

An exploit and operates through a network security vulnerability or "hole" without previous access to the vulnerable system is a "remote" exploit. An exploit that needs prior access to a system is termed a "local" exploit. These are usually intended to increase the hacker's access privileges beyond those granted by a system administrator.

Worms are simply viruses that send copies over network connections. A bomb resides silently in a computer's memory until set off by a date or action. A Trojan horse is a malicious program that cannot reproduce itself, but is distributed by CD or e-mail.

3.7 Avoid Computer Holes/Vulnerabilities

Install only trusted software and delete unknown emails. If you have any doubt about a piece of software's function, do not install it. If you receive e-mails from random people's names, resist your curiosity and do not open it, just delete it.

Under no conditions download or open attachments from anyone that you do not know and even then be cautious. Banks and most companies that create online personal accounts will not send you attachments. If they do, it is probably best to go to the company site and request the download or at least see if it is legitimate. Avoid adult web sites, a hacker's paradise.

Whether in your e-mail or online, do not click on ads. If the ad is of interest, find the site. Be careful with what you physically put into your computer. This is especially true for shared R/W CDs, USB hard disks, or flash drives. This is an easy path for a virus to follow from computer to computer.

3.7.1 Protection: Install Anti-Virus Software

Anti-virus software searches for evidence of the presence of viral programs, worm, bombs, and Trojan horses by checking for the characteristic appearances or behaviours that is typical of these programs. When found the program logs its discovery, its type, often its name or an identifier, and it potential for damage. The anti-virus software then eliminates or isolates/quarantines the infected files. For the individual, commercial software is relatively inexpensive; however, there are free anti-virus programs available.

Since new viruses appear almost daily with new code it is imperative that you update you antivirus program often to keep up with these threats; therefore, make sure to set your program to update automatically. To avoid the annoyance of computer slowdown schedule full scale scans late at night.

The same is true for your Windows Operating System. Very often, your OS is where hackers discover the holes to exploit. Of course, in an ever-continuing battle, this software is continuously updated with security patches.

Finally, secure your wireless network with a router that has a built in firewall. Almost all wireless routers are set to no security when first installed. Log into the router and at least set it to basic security with a strong password to replace the factory setting that any hacker knows. A firewall or router that is not configured properly or non-existent allows hackers to scan passwords, e-mails, or files that cross your network connection.

3.8 System Hacking Scenario

Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain, users often fail to take advantage of this. Therefore, passwords are one of the weakest links in the information-security chain. Passwords rely on secrecy for their security. After a password is compromised, its original owner isn’t the only person who can access the system with it. As you'll learn, hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This unit demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exit in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems.

3.8.1 Is Computer Hacking a Crime?

The term "hacking" is often used as if it's synonymous with illegal computer access. Hacking isn't necessarily a criminal activity, however. A computer hacker can simply be someone who knows how to circumvent the limitations of a device or a piece of software. Ethical hackers often break into computer systems with permission to find vulnerabilities and improve security. Hacking is a crime when the perpetrators access systems without the owner's permission.

3.8.2 Hacking Process

The term "hacking" is a very broad one. Hacking a device or system can refer to altering or improving it, without any suggestion of illicit access. An example of such a "hack" might be turning off the Wi-Fi adapter on your laptop to save the battery. More commonly, hacking, means circumventing the security measures of a computer or networked computer system. It can be done legally and ethically; non-maliciously but illegally; or illegally and with intent to do harm, in which case the term "cracking" may apply.

3.8.3 Laws and Regulations

The laws relating to computer hacking vary from region to region. Broadly speaking, it's typically illegal to access a private computer system unless you have the express permission of the individual or organization the system belongs to. Penalties are usually more severe if malicious damage is involved. Hacking into government systems, even without any malicious intent, often carries a particularly high penalty, as this can have national security implications.

3.8.4 Hacking Versus Cracking

The hacker community is strongly opposed to what they see as the widespread misuse of the term "hacking" to designate malicious intrusions and deliberate damage of computer systems. Many self-described hackers regard this kind of behaviour as unacceptable and prefer the term "cracking" to describe it, with the perpetrators being described as "crackers." Ethical hacking is sometimes referred to as "white hat hacking" to distinguish it from cracking, which is also termed "black hat hacking." "Gray hat hacking" describes activity that's somewhere between the two, existing in a legal and ethical gray area.

3.8.5 Illegal Hacking

Illegal hacking involves computer-related activity that breaks the law. Motivations include simple curiosity, where a person has no intention of damaging a system or causing problems, and is solely interested in obtaining information. If done without permission, this kind of hacking is still illegal. Some incursions are motivated by prankishness and involve annoying but ultimately fairly benign conduct. More serious acts of cracking or black hat hacking include vandalizing websites, deleting information, stealing private information such as lists of client names and details, or placing malware on computer systems.

3.8.6 Legal Hacking

Legal hacking is very narrowly defined, so it's up to hackers to familiarize themselves with local and national laws regarding hacking, and to work within them. Generally speaking, hacking may be legal if you are working on your own computer system or if you have explicit and detailed written permission for anything you do to someone else's system.

3.8.7 Uses of Legal Hacking

Legal hacking is often used by organizations who want to ensure the safety of their computer systems. To this end, hackers may volunteer or be recruited to attempt to break into a system or device as if they were criminals, in order to pinpoint security flaws. Some companies issue public challenges to hackers to break into their systems, offering a reward; more typically, security consultants are contracted to attempt a hack.

3.9 Remote Password Guessing

As an organization's IT security practices mature, it gets better at protecting its network perimeter systems: the patches get applied more regularly, the firewall rules become more restrictive, the OS gets locked-down more rigorously. Even at such companies, authentication systems often lag behind. If the employees, partners, customers, vendors need to remotely access an application with logon screen that requires a password, two things will often hold true:

1. The application will assist the user in remembering the password.

This may involve emailing the password to the user's email address. If you're an attacker, you will try gaining access to that inbox to retrieve the password.

The application may also present the user with a "secret question" picked by him or her in advance. Unfortunately, such questions often have easy-to-guess answers. Favourite colour: Blue. Favourite month: March. It doesn't take many tries to go through likely answers to such questions. Even if it doesn't work for a particular user, it may work over a large population of targeted users. In many cases, answering such questions may not trigger the account lock-out mechanism.

Finally, the application may provide a different response to a valid username than to an invalid username. For instance, if the username and password are both incorrect, it might say "Access denied." But if the username is correct, it might say "Password incorrect."

Make sure your users recognize the importance of protecting access to their email boxes. Help them by protecting the email servers. Also, consider implementing complexity requirements for answers to secret questions or give users a few secret questions to chose from, but omit common questions such as those about colour. Finally, don't provide too much information in response to a failure to logon successfully.

2. The user will select an easy to remember and easy-to-guess password.

There are too many passwords to remember. Of course, users will try to select those that are easy for them to remember. Much has been said about encouraging users to select hard-to-guess passwords, so I won't repeat the discussion here. Once concern to keep in mind is that if your selection requirements are too strict, or if the users need to change the password too often, they will still find a way to beat the system. They may write the passwords down or use the same password across multiple systems/sites/organizations.

Also, the use of default passwords plagues many environments. If possible, require that your users change the pre-assigned password after first logging on to the system, and make sure the default passwords you assign are difficult to guess.

Automatically locking an account after several failed logon attempts will address many of these concerns, but sometimes it's not a feasible option. We may be concerned about denying service to our customers or executives. Or we may not have the staff to deal with unlock-my-account requests. A nice compromise is often a mechanism that locks the account for a few minutes, then automatically unlocks it. This can slow down the attacker's guessing tactics, yet allow the legitimate user to login after a brief waiting period. Implementing CAPCHA to discern between human and non-human users of your site can be effective as well to discourage automated password guessing.

3.9.1 Include Remote Password Guessing in Your Assessment

If your security assessment procedures do not already include remote password guessing, consider adding this task. The steps that come to mind include:

Identify publicly-accessible services/applications that request username/password credentials and attempt by passing them via manual guessing. Keep an eye out for account lock-out mechanisms.

Query Google and examine your public website to identify possible usernames. (The Backtrack CD has some nice tools for that.)

Compile a list of possible passwords the users might use, accounting for your organization's location, name, and industry-specific terminology. Add common names and words like "password" to the list. I find that having a short, but intelligently-crafted list is more effective than using a 100KB dictionary file (the long file often takes too long to cycle through remotely).

After trying the manual route, make use of an automated password guessing tool to see whether it can guess logon credentials using the short password list you put together. Hydra is an excellent tool for this task. It's free, fast, and effective, even though it's poorly documented. (Anyone feels like writing a comprehensive guide to using Hydra, or pointing us to one that already exists?) Hydra is included on the above-mentioned Backtrack CD, and supports most of the protocols you're likely to encounter in the field.

3.10 Eavesdropping

Eavesdropping is as an electronic attack where digital communications are intercepted by an individual whom they are not intended.

This is done in two main ways: Directly listening to digital or analog voice communication or the interception or sniffing of data relating to any form of communication.

Eavesdropping is the act of intercepting communications between two points.

In the digital world, eavesdropping takes the form of sniffing for data in what is called network eavesdropping. A specialized program is used to sniff and record packets of data communications from a network and then subsequently listened to or read using cryptographic tools for analysis and decryption.

For example, Voice over IP (VoIP) calls made using IP-based communication can be picked up and recorded using protocol analyzers and then converted to audio files using other specialized software.

Data sniffing is easily done on a local network that uses a HUB since all communications are sent to all the ports (non-recipients just drop the data) and a sniffer will simply accept all of the incoming data.

This goes the same for wireless networking where data is broadcast so even non-recipients can receive the data if they have the proper tools.

Actual eavesdropping, that is the simple act of listening to other people talk without them knowing it, can be done using current technology such as hidden microphones and recorders.

Hacking into devices such as IP phones is also done in order to eavesdrop on the owner of the phone by remotely activating the speaker phone function.

Devices with microphones including laptops and cellphones also can be hacked to remotely activate their microphones and discretely senddata to the attacker.

3.11 Various methods of password cracking

Most people understand that good password security is the first and most effective strategy for protecting sensitive systems and data, yet systems are regularly compromised via breached user accounts.

It is fairly common knowledge that one should use strong passwords that are not easily "guessed" - such as by employing passwords that are 12 to 16 characters in length that use both upper and lower case letters, and which include non-alphanumeric characters.

But sophisticated hackers are not always simply attempting to "guess" passwords based on information lifted from social networks and the like, but instead are using various methods to undermine what most would think to be a secure password choice.

PC Pro's Davey Winder posted a nice little write-up on the top ten methods hackers use to crack passwords

Winder's top ten and a brief excerpt of the technique are as follows:

1. Dictionary attack

This uses a simple file containing words that can, surprise, be found in a dictionary. In other words, if you will excuse the pun, this attack uses exactly the kind of words that many people use as their password.

2. Brute force attack

This method is similar to the dictionary attack but with the added bonus, for the hacker, of being able to detect non-dictionary words by working through all possible alpha-numeric combinations from aaa1 to zzz10.

3. Rainbow table attack

A rainbow table is a list of pre-computed hashes - the numerical value of an encrypted password, used by most systems today - and that’s the hashes of all possible password combinations for any given hashing algorithm mind. The time it takes to crack a password using a rainbow table is reduced to the time it takes to look it up in the list.

4. Phishing

There's an easy way to hack: ask the user for his or her password. A phishing email leads the unsuspecting reader to a faked online banking, payment or other site in order to login and put right some terrible problem with their security.

5. Social engineering

A favorite of the social engineer is to telephone an office posing as an IT security tech guy and simply ask for the network access password. You’d be amazed how often this works.

6. Malware

A key logger or screen scraper can be installed by malware which records everything you type or takes screen shots during a login process, and then forwards a copy of this file to hacker central.

7. Offline cracking

Often the target in question has been compromised via an hack on a third party, which then provides access to the system servers and those all-important user password hash files. The password cracker can then take as long as they need to try and crack the code without alerting the target system or individual user.

8. Shoulder surfing

The service personnel 'uniform' provides a kind of free pass to wander around unhindered, and make note of passwords being entered by genuine members of staff. It also provides an excellent opportunity to eyeball all those post-it notes stuck to the front of LCD screens with logins scribbled upon them.

9. Spidering

Savvy hackers have realized that many corporate passwords are made up of words that are connected to the business itself. Studying corporate literature, website sales material and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack.

10. Guess

The password crackers best friend, of course, is the predictability of the user. Unless a truly random password has been created using software dedicated to the task, a user generated 'random' password is unlikely to be anything of the sort.

3.12 Keystroke Logger

No doubt everyone wants to know who and how is using their PC. Especially when it comes to situations when the owner is away from PC and cannot physically control its usage. Here is when using keystroke logger can be a perfect solution for you as it will keep you informed of everything what was typed on your PC.

Keystroke logger Software allows tracking everything what was typed on your PC. With keystroke recorder you can easily get access to all keystrokes,

messages typed in Instant messengers, texts of emails which were typed, passwords, texts typed in different documents and so on. In other words keystroke logger tracks any keyboard activity including system keys and controls on multimedia keyboards.

Keystroke loggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data. Keystroke logger recorders may also be used by employers to observe employees' computer activities, parents to supervise their children's internet usage, users to track possible unauthorized activity on their devices or law enforcement agencies to analyze incidents involving computer use. These uses are considered ethical or appropriate in varying degrees.

3.12.1 Types of Keystroke Logger

A hardware-based Keystroke logger is a small device that serves as a connector between the computer keyboard and the computer. The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adaptor, making it relatively easy for someone who wants to monitor a user's behavior to hide such a device.

Most workstation keyboards also plug into the back of the computer, keeping the connections out of the user's line of sight. A hardware Keystroke logger may also come in the form of a module that is installed inside the keyboard itself. When the user types on the keyboard, the Keystroke logger collects each keystroke and saves it as text in its own miniature hard drive, which may have a memory capacity of up to several gigabytes. The person who installed the Keystroke logger must later return and physically remove the device in order to access the information that has been gathered. There are also wireless Keystroke logger sniffers that can intercept and decrypt data packets being transferred between a wireless keyboard and its receiver.

Screenshot of data captured from Keystroke logger software

A key logging software program Bottom of Form does not require physical access to the user's computer for installation. It can be downloaded on purpose by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly and executed as part of a rootkit or remote administration Trojan (RAT). The rootkit can launch and operate stealthily in order to evade manual detection or antivirus scans.

A common Keystroke logger program typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file that does all the recording and an executable file that installs the DLL file and triggers it to work. The Keystroke logger program records each keystroke the user types and uploads the information over the internet periodically to whoever installed the program. There are many other ways that key logging software can be designed to monitor keystrokes, including hooking keyboard APIs to another application, malicious script injection or memory injection.

Some key logging programs may include functionality for recording user data besides keystrokes, such as capturing anything that has been copied to the clipboard and taking screenshots of the user's screen or a single application.

3.12.2 Detection, Prevention and Removal

As there are various types of Keystroke logger that use different techniques, no single detection or removal method is considered the most effective.

Antikeylogger software is designed specifically to scan for software-based Keystroke loggers, by comparing the files on a computer against a Keystroke logger signature base or a checklist of common Keystroke logger attributes. Using an antikeylogger can be more effective than using an antivirus or antispyware program, as the latter may identify a Keystroke logger as a legitimate program instead of spyware.

3.13 Let us Sum-up

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in computer hacking activities are typically referred to as “hackers.”

Computer programmers as a subculture of the general engineering and scientific community have their own set of heroes with aspects based on the

values that programmers respect. These heroic figures, called hackers, are not at all like the popular press version of the computer hacker. Legendary hackers are both real and fictional, but tend to share certain common features: extraordinary programming skill, cleverness in the face of difficulty, an ability to suspend all other activities while producing a solution to a problem, an appreciation for a clever solution to a seemingly insignificant problem, weakness in some other aspect to balance their skill as a hacker, and adherence to some form of the Hacker Ethic.

3.14 Self Assessment Questions

1. What is System Hacking?

……
……
……
……
……

2. Types of System Hacking

……
……
……
……
……

3. What Is Rootkits?

……
……
……
……
……

4. What is Steganography?

……
……
……
……
……

5. Why need uses of legal hacking?

……
……
……

……
……..……

3.15 Model Questions

1. What is Eavesdropping and explain its?
2. Explain about different type of hacker tools.
3. Write the different between hacker tools and hacking tools.
4. Write the sort notes about legal hacking and illegal hacking.
5. Write the various methods of password cracking.

3.16 References & Further Readings

1. http://itstillworks.com/computer-hacking-crime-1387.html
2. https://isc.sans.edu/forums/diary/Remote+Password+Guessing+Concerns+Observations+Recommendations/3212/
3. http://kyrion.in/blog/2017/06/22/computer-hacking-crime/
4. https://www.gohacking.com/hack-windows-administrator-password/

UNIT-4 Sniffer

Unit Structure

4.0 Introduction

Some of the more "legitimate" uses for a sniffer fall towards the roles of the network administrators. They can be used to probe the network for bandwidth usage, helping pinpoint which individual machines may be running malware or simply have wrong network settings. Sniffers are often used as a practical defense against finding intrusion attempts by detecting inappropriate traffic. If you're ever going to be in a role where you need to ensure your network is protected, you would do well to learn how to use a sniffer. I recommend Wireshark (formerly known as Ethereal), it's free (as in beer) and well supported with great documentation. Other alternatives are NAI Sniffer (commercial), TCPDump (*nix), WinDump (Win32), Cain & Abel, Dsniff, and Ettercap (the last three are more specialized for password extraction but can still be used to test your applications or network protocols).

Sniffers can also be used to bypass security. Many application protocols pass credentials in plain text or use weak encryption that is easy for a sniffer to decode. Common examples of insecure protocols are FTP, Telnet, POP3, SMTP, and HTTP Basic Authentication. Instead, secured/encrypted protocols should be used, SFTP, SSH, HTTPS (SSL).

4.1 Learning Objective

After learning this unit you should be able to

- Know about what a sniffer is and what is sniffing.
- Classify different types of sniffers and its use.
- Identify different types of hackers.
- Study about how sniffer attacks takes place.
- Know about ARP and how ARP works and its use.
- Study about ARP spooling and spooling attack.
- Know aboutDNS, DNS work and DNS spooling.
- Understand DNS Spoofing Techniques and poisoning.
- Know about the MAC, MAC spooling and MAC spooling attack.
- Know the Countermeasure of sniffing attacks.

4.2 What is a Sniffer

A sniffer, which can also be referred to as a network analyzer, is a piece of software that analyzes network traffic, decodes it, and gives it back packet information so that a network administrator can use it to help diagnose problems on the network. But because these tools can be so powerful, they can also help give leverage to those of the black hat world by allowing them to pull plain text information off the network as well (usernames, passwords, unencrypted emails, instant message chat, etc.).

4.3 What is Sniffing

Sniffing is one of the most effective techniques in attacking a wireless network whether it is mapping the network to gain information, to grab information, or to capture encrypted data. Sniffers usually act as network probes or snoops; examine network traffic but not intercepting or altering it.

A sniffer sometimes referred to as a network monitor or network analyzer, can be used by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the sniffer an administrator can identify erroneous packets and use the data pinpoint bottlenecks and help maintain efficient network data transmission.

Sniffer simply captured all data packets pass through a given network interface.

By placing a sniffer on a network in promiscuous mode a malicious intruder can capture and analyze all of the network traffic. Within a given network, user name and password information is generally transmitted in clear text which means that information is generally transmitted in clear text which means that the information would be viewable by analyzing the packets being transmitted.

A sniffer can only capture packet information within a given subnet so it is not possible for a malicious attacker to place a packet sniffer on their home ISP network and capture network traffic from inside your corporate network.

However if one machine on the internal networks becomes compromised through a Trojan or other security breach, the introducer could run sniffer from that machine and use the captured user name and password information to compromise other machine on the network.

4.3.1 Types of Sniffing

Sniffing is of two types:

1. Active Sniffing
2. Passive sniffing

The terms active and passive sniffing has also been used to describe wireless network sniffing. They have analogous meaning. Passive wireless sniffing involves sending no packets, and monitoring the packets send by other. Active sniffing involves sending out multiple networks to identify APs.

4.3.1.1 Active Sniffing

When sniffing is performed on a switched network, it is known as active sniffing.

Active sniffing relies on injecting packets into the network that cause traffic. Active sniffing is required to bypass the segmentation that switches provided. Switch maintain their own Arp cache special type of memory known as content addressable Memory (CAM),keeping track of which host is connected to which port.

Sniffers are operated at the Data Link Layer of OSI model. This means that they do not have to play by the same rules as application and services that resides further up stack. Sniffer can grab whatever they see on the wire and record it for later review. They allow the user to see all the data contained in packet, even information that should remain hidden.

4.3.1.2 Passive Sniffing

Hubs see all the traffic in that particular collision domain. Sniffing performed on a hub is known as passive sniffing.

Passive sniffing is performed when the use is on a hub. Because the user is on a hub, all traffic is sent to all ports. All the Attacker must do is to start the sniffer and just wait for someone on the same collision domain to start sending or receiving data. Collision domain is a logical area of the same collision domain to start sending or receiving data. Collision domain is a logical area of the network in which one or more data packets can collide with each other.

Compatibility of Passive Sniffing

Passive sniffing worked well during the days that hubs were used. The problem is that there are few of these devices left.Nowdays most of the network are working on switches where active sniffing is useful.

4.4 Understanding Packet Sniffers

Network traffic is one of most resource laden stream which contains everything we talk about on internet. If you can get data from it, you can know what is my password or even Google's Password, in technical words it's called as Network Sniffing and software which are used to sniff data are called as Packet Sniffers. SO if you place a sniffer on a router (router is a hardware which sends data to right destination) you can see all the data and record it. Imagine the power of it now!!!

4.4.1 What is A Packet Sniffer?

A packet sniffer is a program which runs silently and monitors data on a network stream. It's called as passive as it does not send any information to you but just collects and stores it somewhere. If you run such a sniffer on your system, it can tell you your own IP address and IP addresses of other sites which you visit.

4.4.2 How Packet Sniffers Work?

Sniffers are basically small programs with one goal, interception of data. They can watch all unencrypted data that travels from your computer or when on router it can see all the data travelling through network. Now the question is how they are allowed to read data. It's possible because of the architecture itself. Which means, if you send some data I will read it but I will accept it only when the data is addressed to me.But now think, we have 4-5 computers in a network? You send a message to Computer A which is not having any sniffer. But Computer B is having one. If you send some information to computer A, the message is send to everybody with IP address of Computer A, so all the computers except A should reject it, but I have one sniffer on Computer B. So though computer itself rejects it but the sniffer accepts the data.

Thus if you are sending unencrypted data on a network, there is a high chance of your data being stolen.

4.4.3 What Are The Types Of Packet Sniffers?

- **Commercial Sniffers** which are used by network administrator to control the type and see the bottle neck data.
- **Underground Sniffers** which are used to steal data, so as to gain access of data stored which can be used for bad.

4.4.4 What are the uses of packet sniffers?

Packet Sniffers was never made to hack or stole information. They had a different goal, to make things secure. But then everything has a dark side. Here are few uses:-

- Network Analysis to find the traffic and its problem around the network.
- Detect Attackers if some resource is used high and traffic is coming from same ip again and again.
- Searching unencrypted text like password.
- To convert data into human readable format, mostly used in war to get hold of enemies.

Sniffers are very hard to detect due to its passiveness but there is always a way.

4.5 Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

4.5.1 How ARP Works

When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

Since protocol details differ for each type of local area network, there are separate ARP Requests for Comments (RFC) for Ethernet, ATM, Fiber Distributed-Data Interface, HIPPI, and other protocols.

4.5.2 What Is ARP Spoofing?

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

4.5.3 ARP Spoofing Attacks

The effects of ARP spoofing attacks can have serious implications for enterprises. In their most basic application, ARP spoofing attacks are used to steal sensitive information. Beyond this, ARP spoofing attacks are often used to facilitate other attacks such as:

- **Denial-of-service attacks:** DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.

- **Session hijacking:** Session hijacking attacks can use ARP spoofing to steal session IDs, granting attacker's access to private systems and data.

- **Man-in-the-middle attacks:** MITM attacks can rely on ARP spoofing to intercept and modify traffic between victims.

4.5.4 ARP Spoofing Detection, Prevention and Protection

The following methods are recommended measures for detecting, preventing and protecting against ARP spoofing attacks:

- Packet filtering: Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in ARP spoofing prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from

outside the network that show source addresses from inside the network and vice-versa).

- Avoid trust relationships: Organizations should develop protocols that rely on trust relationships as little as possible. Trust relationships rely only on IP addresses for authentication, making it significantly easier for attackers to run ARP spoofing attacks when they are in place.

- Use ARP spoofing detection software: There are many programs available that help organizations detect ARP spoofing attacks. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.

- Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster ARP spoofing attack prevention by encrypting data prior to transmission and authenticating data when it is received.

4.6 ARP Poisoning

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.

The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa, so his or her target's MAC is now associated with the attacker's IP address). Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination. Because ARP Poisoning attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. Besides Man-in-the-Middle Attacks, ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets.

4.6.1 ARP Poisoning (MITM) Attack

A Man-In-The-Middle (MITM) attack is achieved when an attacker poisons the ARP cache of two devices with the (48-bit) MAC address of their Ethernet NIC (Network Interface Card). Once the ARP cache has been successfully poisoned, each of the victim devices sends all their packets to the attacker when communicating to the other device. This puts the attacker in the middle of the communications path between the two victim devices; hence the name Man-In-The-Middle (MITM) attacks. It allows an attacker to easily monitor all communication between victim devices.

4.7 Domain Name System (DNS)

The domain name system (DNS) is the way that internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types TechTarget.com into a web browser, a server behind the scenes will map that name to the IP address 206.19.49.149.

Web browsing and most other internet activity rely on DNS to quickly provide the information necessary to connect users to remote hosts. DNS mapping is distributed throughout the internet in a hierarchy of authority. Access providers and enterprises, as well as governments, universities and other organizations, typically have their own assigned ranges of IP addresses and an assigned domain name; they also typically run DNS servers to manage the mapping of those names to those addresses. Most URLs are built around the domain name of the web server that takes client requests.

4.7.1 How does DNS work?

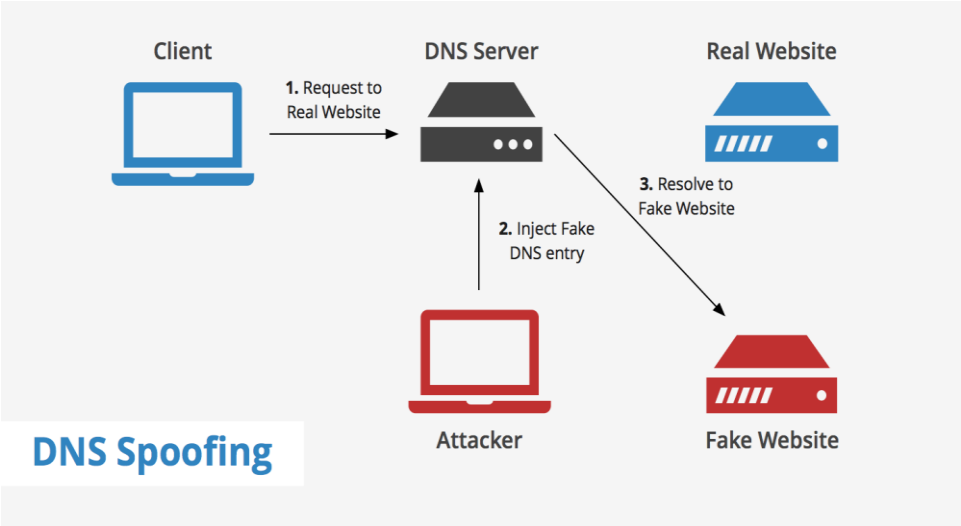
DNS servers answer questions from both inside and outside their own domains. When a server receives a request from outside the domain for information about a name or address inside the domain, it provides the authoritative answer. When a server receives a request from inside its own domain for information about a name or address outside that domain, it passes the request out to another server usually one managed by its internet service provider. If that server does not know the answer or the authoritative source for the answer, it will reach out to the DNS servers for the top-level domain e.g., for all of .com or .edu. Then, it will pass the request down to the authoritative server for the specific domain e.g., techtarget.com or stkate.edu; the answer flows back along the same path.

4.7.2 How does DNS increase web performance?

To promote efficiency, servers can cache the answers they receive for a set amount of time. This allows them to respond more quickly the next time a request for the same lookup comes in. For example, if everyone in an office needs to access the same training video on a particular website on the same day, the local DNS server will ordinarily only has to resolve the name once, and then it can serve all the other requests out of its cache. The length of time the record is held the time to live is configurable; longer values decrease the load on servers, shorter values ensure the most accurate responses.

4.7.3 What Is DNS Spoofing?

DNS spoofing occurs when a particular DNS server's records of "spoofed" or altered maliciously to redirect traffic to the attacker. This redirection of traffic allows the attacker to spread malware, steal data, etc. For example, if a DNS record is spoofed, then the attacker can manage to redirect all the traffic that relied on the correct DNS record to visit a fake website that the attacker has created to resemble the real site or a different site completely.



4.7.4 How Does Normal DNS Communication Work?

A DNS server is used for the purpose of resolving a domain name (such as keycdn.com) into the associated IP address that it maps to. Once the DNS server finds the appropriate IP address, data transfer can begin between the client and website's server. The visualization below shows a how this process takes place at a high level.

Once the DNS server finds the domain-to-IP translation, it will cache it so that upon subsequent requests for that domain, the DNS lookup will happen much faster. However, this is where DNS spoofing can become a real

problem since a false DNS lookup can be injected into the DNS server's cache thus altering the visitors' destination.

4.7.5 How Does DNS Spoofing Work?

DNS spoofing is an overarching term and can be carried out using various methods such as:

- DNS cache poisoning
- Compromising a DNS server
- Implementing a Man in the Middle Attack

However, an attacker's end goal is usually the same no matter which method they use. Either they want to steal information, re-route you to a website that benefits them, or spread malware. The most discussed method to perform DNS spoofing is using cache poisoning which we'll explain next.

4.7.6 How to Prevent DNS Spoofing

As a website visitor, there's not much you can do to prevent DNS spoofing. Rather, this falls more in the hands of the actual DNS provider that is handling a website's DNS lookups as well as the website owner. Therefore, a few tips for site owners and DNS providers include:

Implement DNS spoofing detection mechanisms – it's important to implement DNS spoofing detection software. Products such as XArp help product against ARP cache poisoning by inspecting the data that comes through before transmitting it.

Use encrypted data transfer protocols – Using end-to-end encryption via SSL/TLS will help decrease the chance that a website / its visitors are compromised by DNS spoofing. This type of encryption allows the users to verify whether the server's digital certificate is valid and belongs to the website's expected owner.

Use DNSSEC – DNSSEC, or Domain Name System Security Extensions, uses digitally signed DNS records to help determine data authenticity. DNSSEC is still a work in progress as far as deployment goes, however implement in the Internet root was level in 2010. An example of a DNS service that fully supports DNSSEC is Google's Public DNS.

4.7.7Understand DNS Spoofing Techniques

DNS Spoofing (or DNS Poisoning) this is a technique that tricks a DNS server into believing it has received authentic information when in reality it hasn't. Once the DNS server has been poisoned, the information is generally

cached for a while, spreading the effect of the attack to the users of the server. When a user requests a certain website URL, the address is looked up on a DNS server to find the corresponding IP address. If the DNS server has been compromised, the user is redirected to a website other than the one that was requested, such as a fake website.

To perform a DNS attack, the attacker exploits a flaw in the DNS server software that can make it accept incorrect information. If the server doesn't correctly validate DNS responses to ensure that they come from an authoritative source, the server ends up caching the incorrect entries locally and serving them to users that make subsequent requests. This technique can be used to replace arbitrary content for a set of victims with content of an attacker's choosing. For example, an attacker poisons the IP addresses DNS entries for a target website on a given DNS server, replacing them with the IP address of a server the hacker controls. The hacker then creates fake entries for files on this server with names matching those on the target server. These files may contain malicious content, such as a worm or a virus. A user whose computer has referenced the poisoned DNS server is tricked into thinking the content comes from the target server and unknowingly downloads malicious content.

The types of DNS spoofing techniques are as follows:
Intranet Spoofing Acting as a device on the same internal network
Internet Spoofing Acting as a device on the Internet
Proxy Server DNS Poisoning Modifying the DNS entries on a proxy server so the user is redirected to a different host system
DNS Cache Poisoning Modifying the DNS entries on any system so the user is redirected to a different host.

4.8 DNS Cache Poisoning

Since DNS servers cache the DNS translation for faster, more efficient browsing, attackers can take advantage of this to perform DNS spoofing. If an attacker is able to inject a forged DNS entry into the DNS server, all users will now be using that forged DNS entry until the cache expires. Once the cache expires, the DNS entry will return to normal as the DNS server will go through the complete DNS lookup process again. However, if the DNS server's software still hasn't been updated, then the attacker can replicate this error and continue funnelling visitors to their website.

DNS cache poisoning can also sometimes be quite difficult to spot. If the malicious website is very similar to the website it is trying to impersonate, some users may not even notice the difference. Additionally, if the attacker is using DNS cache poisoning to compromise one company's DNS records in

order to have access to their emails for example, then this may also be difficult to detect.

4.9 What is MAC Flooding?

The MAC Flooding is an attacking method intended to compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located. As we've already seen, the hubs broadcast the data to the entire network allowing the data to reach all hosts on the network but switches send the data to the specific machine(s) which the data is intended to be sent. This goal is achieved by the use of MAC tables the aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So, considerable number of incoming frames will be flooded at all ports.

MAC Address Table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like broadcasting. Let's see, what are the benefits of the attackers with the MAC Flooding attacks.

4.9.1 What is MAC Flooding Attack?

In computer network jargon, MAC flooding is a technique employed in order to compromise the security of the network switches.

Switches maintain a list (called a CAM Table) that maps individual MAC addresses on the network to the physical ports on the switch.

This enables it to only send data out of the physical port where the recipient computer is located, instead of indiscriminately broadcasting the data out of all ports like a hub.

The advantage of this method is that data is only routed to the network segment containing the computer that the data is specifically destined for.

In a typical MAC flooding attack, a switch is flooded with packets, each containing different source MAC addresses. The intention is to consume the limited memory set aside in the switch to store the MAC address-to-physical port translation table.

The result of this attack causes the switch to enter a state called "fail open mode", in which all incoming packets are broadcast out on all ports (as with a hub), instead of just down the correct port as per normal operation.

A malicious user could then use a packet sniffer (such as Wire shark) running in promiscuous mode to capture sensitive data from other computers (such as unencrypted passwords, e-mail and instant messaging conversations), which would not be accessible were the switch operating normally.

Some more advanced switches, such as those from Nortel, Cisco or Allied Telesis gives you an opportunity to set up protection against this attack with limiting and/or hardwiring some MAC addresses to a dedicated port.

You can also set the policy that if a port gets too many MAC addresses, the default is to shut the port down, and generate a log message.

4.9.2 How to prevent the MAC Flooding Attack?

We can prevent the MAC Flooding attack with various methods. The following are some of these methods.

1) Port Security
2) Authentication with AAA server
3) Security measures to prevent ARP Spoofing or IP Spoofing
4) Implement IEEE 802.1X suites

Port Security

The port security is often used as a counter measure for MAC Flooding attack. The switches are configured to limit the number of MAC addresses that can be learned on ports connected to the end stations. Also a small table of ‘secure’ MAC addresses is maintained with the traditional MAC address table. This table also acts as a subset of the MAC address table. Cisco switches are available with in-built port security system.

Authentication with AAA server

In this method, the discovered MAC addresses are authenticated against an authentication, authorization and accounting server (AAA Server) and these addresses are subsequently filtered

Security measures to prevent ARP spoofing or IP Spoofing.

Security measures to prevent ARP Spoofing or IP Spoofing in some cases may also perform additional MAC address filtering on uncast packets.

Implement IEEE 802.1X suites

Implementing IEEE 802.1X suites will allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address.

These are the methods often used to prevent the MAC Flooding attack.

4.10 Countermeasure

In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

There are several stages involved in combating denial of service attacks. The first is recognizing that you are undergoing an attack. The second is determining what kind of attack is being executed. For example is it a single source attack or are there multiple sources being used? The final stage involves counteracting the attack. Different methods are utilized to combat different types of attacks and knowledge of how the attack is being performed can help in choosing the best solution. Different techniques can also be used depending on whether or not the network has mobile components in it. We will illustrate some techniques that have been suggested to determine the type of attack and some of the countermeasures that can be instigated in response.

4.11 Let us Sum-up

“Sniffer for the detection of lost Mobile phones” paves a way by means of which the lost mobile phones can be recovered. But the process of detection is yet to be developed through the software. There are certain boundary conditions or criteria that have to be qualified for the identification of the lost mobile like the power of the mobile should be good enough, the mobile phone should not be in the shadow region etc., but however this method can be improved by using modern technologies and devices.

In common industry usage, a sniffer (with lower case "s") is a program that monitors and analyzes network traffic, detecting bottlenecks and problems.

Using this information, a network manager can keep traffic flowing efficiently. Sniffer (with a capital "S") is a trademark owned by Network General. The generic term may have originated from Sniffer, which is said to be the first packet capture and decode software that was offered for the purpose of network analysis and troubleshooting.

4.12 Self Assessment Questions

1. What is a Sniffer?

……
……
……
……
……

2. Discuss about different types of Sniffing.

……
……
……
……
……

3. What is ARP Spoofing?

……
……
……
……
……

4. What is ARP poisoning?

……
……
……
……
……

5. Explain how does DNS work?

……
……
……
……
……

4.13 Model Questions

1. Write the sort note about packet sniffer?
2. What is ARP and how its work?
3. Discuss about the ARP Spoofing detection, prevention and protection.
4. What is MAC Flooding?
5. What is MAC flooding attack?
6. What is the different between sniffer and sniffing?

4.14 References & Further Readings

1. http://www.colasoft.com/resources/sniffer.php
2. https://en.wikipedia.org/wiki/Packet_analyzer
3. https://www.keycdn.com/support/dns-spoofing/
4. http://www.infosecisland.com/blogview/3684-How-to-Detect-a-Mac-Flooding-Attack.html

Answer of Self Assessment Questions (Unit-1)

1. What is hacking?

Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system. In another way we can tell Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access**.** Example of Hacking: Using password cracking algorithm to gain access to a system

2. Explain difference between hackers and crackers.

A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data; deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.

3. What is cybercrime?

Cybercrime, also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone. The Department of Justice divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack; and crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally-obtained data.

4. What is security threat?

Security Threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack. In these tutorial series, we will define a threat

as a potential attack from a hacker that can allow them to gain unauthorized access to a computer system.

5. What is ethical hacking?

Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming with countermeasures that protect the weaknesses. Ethical hackers must abide by the following rules.

- Get written permission from the owner of the computer system and/or computer network before hacking.
- Protect the privacy of the organization been hacked.
- Transparently report all the identified weaknesses in the computer system to the organization.
- Inform hardware and software vendors of the identified weaknesses.

Answer of Self Assessment Questions (Unit-2)

1. What is footprinting in hacking?

Footprinting is the first and most convenient way that hackers use to gather information about computer systems and the companies they belong to. The purpose of footprinting is to learn as much as you can about a system, its remote access capabilities, its ports and. services, and the aspects of its security.

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

2. What are the footprinting threats?

Footprinting threats is the attackers gathers valuable system-level information such as account details, OS and other software versions, server names, and db schema details from footprinting techniques.

Threats include:

- Business loss
- Corporate espionage
- Privacy loss
- Social engineering
- System and network attacks
- Information leakage

3. Explain about Open Source Footprinting.

Open Source Footprinting is the easiest and safest way to go about finding information about a company. Information that is available to the public, such as phone numbers, addresses, etc.

Performing who is requests, searching through DNS tables, and scanning certain IP addresses for open ports, are other forms of open source footprinting. Most of this information is fairly easy to get, and getting it is legal, legal is always good.

4. Write about sort note Information Gathering.

Preparation is crucial to any social engineering engagement. Information gathering is the most time-consuming and laborious phase of the attack cycle but is often a major determinant of the success or failure of the engagement. The professional social engineer must be aware of: information-gathering tools freely available online, the many accessible locations online that house valuable pieces of data, the software which can be used to aid in finding and collating the data, and the value or use of seemly insignificant data which can be collected online, over the phone, or in-person.

5. How to undertake information gathering?

Information gathering is an assignment of the research specialist within the organization's intelligence department. They are the personnel properly trained and equipped to carry out the research tasks in the most efficient manner. The proper handling of data requires methods and procedures unique to the field of information gathering. Research personnel do this task unequivocally thru skills like data sifting, intelligent questioning, and other research skills. Other company personnel can also do their own information gathering on the personal level to improve their job performances and as a self-help tool. Researchers undertake information gathering in order to:

- Broaden the scope of knowledge of the organization
- For the development of particular skills
- To reduce the apprehension caused by the unknown
- For a higher level of understanding of special subjects
- And obviously, for solving problems

Additionally, on the non-professional aspect of the research undertaking, information can also give inspiration and entertainment.

Answer of Self Assessment Questions (Unit-3)

1. What is System Hacking

System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. This unit explains the main methods of system hacking—password cracking; privilege escalation, spyware installation, and key logging—and the countermeasures IT security professionals can take to fight these attacks. Security expert Lisa Bock also covers Steganography, spyware on a cell phone, and tactics for hiding files and tools.

2. Types of System Hacking

There are of four types of password attack
1. Passive online attack
2. Active online attack
3. Offline attack
4. Non technical attack

Passive Online Attack

In passive online attacks an attacker don't contact with authorizing party for stealing password, in other words he attempts password hacking but without communicating with victim or victim account. Types of passive online attacks include wire sniffing, Man in the middle attack and reply attack.

Active Online Attack

This type of attack can be directly termed as password guessing. An attacker tries number of passwords one by one against victim to crack his/her password.

Offline Attack

Offline password attacks are performed from a location other than the actual computer where the password reside or were used. Offline attacks requires physical access to the computer which stores password file, the attacker copies the password file and then tries to break passwords in his own system. Offline attacks include, dictionary attacks, hybrid attacks, brute force attack, pre-computed hash attacks, syllable attacks, rule based attacks and rainbow attacks.

Non Technical Attack

This type of attacks does not require any technical knowledge hence termed as non-technical attacks. This kind of attacks may include, social engineering, shoulder surfing, keyboard sniffing and dumpster diving.

3. What Is Rootkits?

A rootkit is a type of malicious software that is activated each times your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals, network connections, and the keyboard.

Root kit helps hackers to maintain hidden access to the system using virus , Trojan horse, spyware ect.

4. What is Steganography?

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

Steganography techniques can be applied to images, a video file or an audio file. Typically, however, Steganography is written in characters including hash marking, but its usage within images is also common. At any rate, Steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

5. Why need uses of legal hacking?

Legal hacking is often used by organizations who want to ensure the safety of their computer systems. To this end, hackers may volunteer or be recruited to attempt to break into a system or device as if they were criminals, in order to pinpoint security flaws. Some companies issue public challenges to hackers to break into their systems, offering a reward; more typically, security consultants are contracted to attempt a hack.

Answer of Self Assessment Questions (Unit-4)

1. **What Is Sniffer?**

   A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks, where they sniff packets, they're often called packet sniffers.

2. **Discuss about different types of Sniffing.**

   Sniffing can be either Active or passive in nature.

   Passive Sniffing

   In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

   Active Sniffing

   In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port.

3. **What is ARP Spoofing?**

   ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker’s MAC address with the IP address of a legitimate computer or server on the network. Once the attacker’s MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

4. **What is ARP poisoning?**

   Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user.

5. **Explain how does DNS work?**

   The Domain Name System (DNS) is a central part of the Internet, providing a way to match names (a website that you are looking for) to numbers (the address for the website). Anything connected to the Internet - laptops, tablets, mobile phones, and websites - has an Internet Protocol (IP) address made up of numbers. Your favorite website might have an IP address like 64.202.189.170, but this is obviously not easy to remember. However a domain name such as bestdomainnameever.com is something people can recognize and remember. DNS syncs up domain names with IP addresses enabling humans to use memorable domain names while computers on the Internet can use IP addresses.