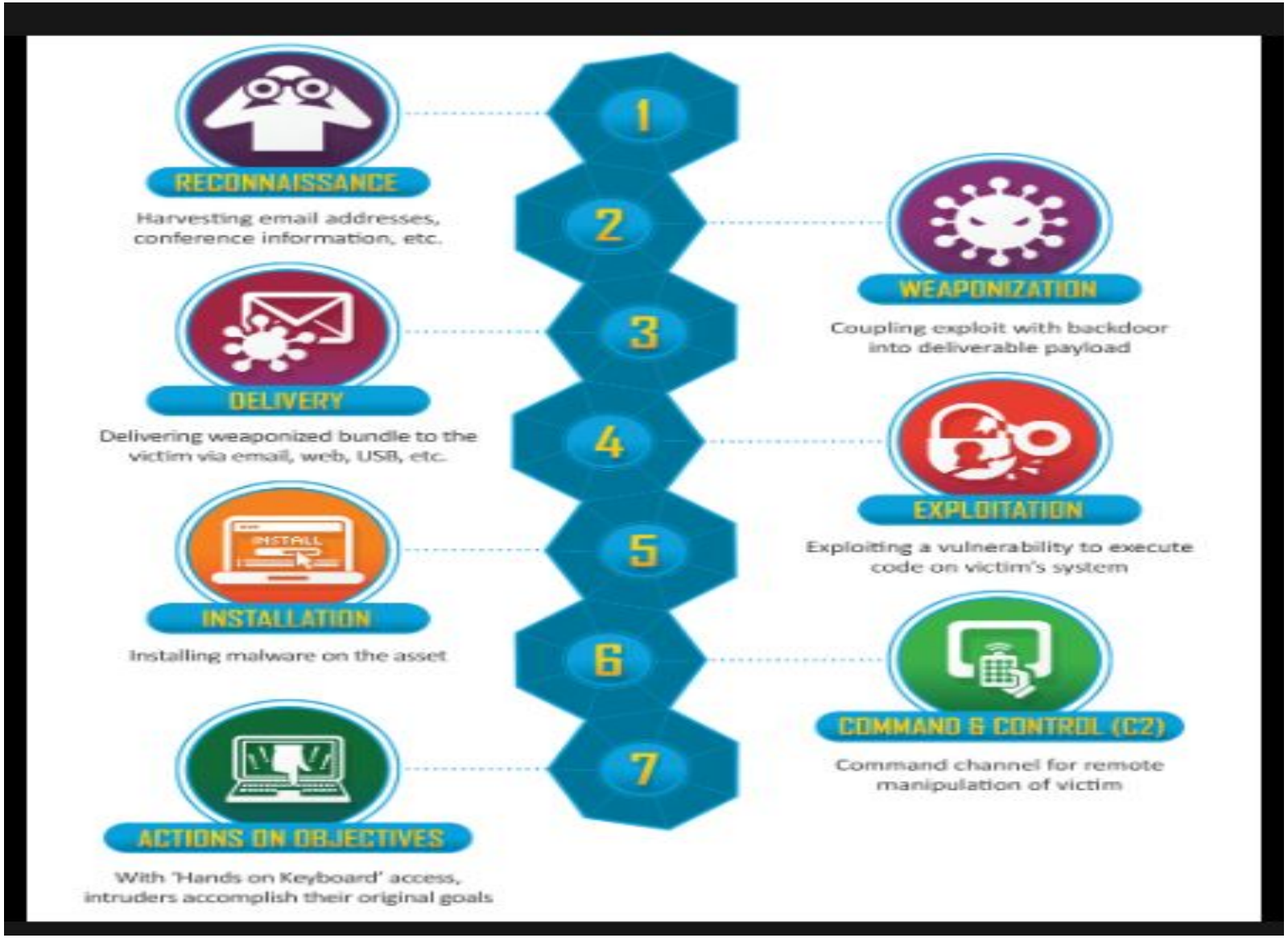
Unit 2: Understanding Cyber Security Kill Chain

The cyber kill chain is intended to defend against sophisticated cyberattacks, also known as advanced persistent threats (APTs), wherein adversaries spend significant time surveilling and planning an attack. Most commonly these attacks involve a combination of malware, ransomware, Trojans, spoofing and social engineering techniques to carry out their plan.



Phases of Kill Chain

Reconnaissance

During the Reconnaissance phase, a malicious actor identifies a target and explores vulnerabilities and weaknesses that can be exploited within the network.

- External Reconnaissance
- Internal Reconnaissance

External Reconnaissance

External reconnaissance is done outside of the organization's network and systems. It is normally targeted by exploiting the carelessness of users of an organization.

- An attacker is simply looking for a vulnerable target to attack.
- The motive is to harvest as much information as possible from outside the target's network and systems.
- This may be information about the target's supply chain, obsolete device disposal, and employee social media activities.
- This will enable the attacker to decide on the exploitation techniques that are suitable for each vulnerability identified about a particular target.

External Reconnaissance methods

1. Dumpster diving:-

- Organizations dispose of obsolete devices in a number of ways, such as through bidding, sending to recyclers, or dumping them in storage.

Google:-

- Google is one of the companies that are thorough in the way they dispose of devices that may have contained user data.
- The company destroys its old hard drives from its data centers to prevent the data that they contained from being accessed by malicious people.
- The hard drives are put into a crusher that pushes steel pistons up the center of the disks, rendering them unreadable. This process continues until the machine spits out tiny pieces of the hard drive, which are then sent to a recycling center.

- Most organizations are not thorough enough when handling old external storage devices or obsolete computers. Some do not even bother to delete the contained data. Since these obsolete devices may be disposed of by sometimes careless means, attackers are able to easily obtain them from their points of disposal.

External Reconnaissance methods

2. Social Media:-

- Hackers have found social media to be the best place to mine data concerning specific targets, as people are likely to share information on such platforms**.**
- Hackers exploit social media users is by going through their account posts to obtain information that can be used in passwords or as answers to secret questions used to reset some accounts.
- This is information such as a user's date of birth, their parent's maiden name, names of the street that they grew up in, pet names, school names, and other types of random information.
- The recent incident involving a Russian hacker and a Pentagon official showed how sophisticated hackers have become.
- Another danger looming in social media is identity theft. It is surprisingly easy to create a fake account bearing the identity of another person.
- Hackers track information about organizations' users and their bosses. They can then create accounts with the names and details of the bosses. This will allow them to get favors or issue orders to oblivious users, even through the likes of social media.

External Reconnaissance methods

3. Social Engineering:-

- A company can shield itself from many types of attack with security tools, but it cannot completely protect itself from this type of threat. Social engineering has been perfectly developed to exploit human nature—something beyond the protection of security tools.
- Humans are sympathetic, trusting of friends, show-offs, and obedient to higher authorities; they are easy to convince provided that one can bring them around to a certain way of thinking.

Social Engineers uses six levers to make the victims fall into the trap.

- Reciprocation
- Scarcity
- Consistency
- Liking
- Authority
- Social Audience

Types of Social Engineering Attacks

Pretexting: This is a method of indirectly putting pressure on targets to get them to divulge some information or perform unusual actions. It involves the construction of an elaborate lie that as been well-researched so as to appear legitimate to the target.

Diversion Theft: This is a con game, whereby attackers persuade delivery and transport companies that their deliveries and services are requested elsewhere. There are some advantages of getting the consignments of a certain company—the attackers can physically dress as the legitimate delivery agent and proceed to deliver already-flawed products. They might have installed rootkits or some spying hardware that will go undetected in the delivered products.

Types of Social Engineering Attacks

- **Phishing**

A link leading to a malicious or fraudulent website is also attached and the users are advised to use it to access a certain legitimate website. The attackers will have made a replica website, complete with logos and usual content, as well as a form to fill in with sensitive information. The idea is to capture the details of a target that will enable the attacker to commit a bigger crime.

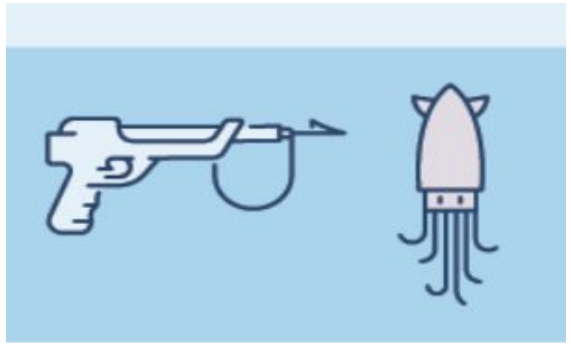
Types of Social Engineering Attacks

- **Phishing**

Phone Phishing(Vishing): This is a unique type of phishing where the attacker uses phone calls instead of emails. It is an advanced level of a phishing attack whereby the attacker will use an illegitimate interactive voice response system that sounds exactly like the ones used by banks, service providers, and so on.

Spear Phishing:-

Spear phishing is specifically targeted to obtain information from particular end users in an organization. Spear phishing is more strenuous since it requires the attackers to perform a number of background checks on targets in order to identify a victim that they can pursue. Attackers will then carefully craft an email that addresses something of interest to the target, coercing him or her to open it



Types of Social Engineering Attacks

Water Holing: This is a social engineering attack that takes advantage of the amount of trust that users give to websites they regularly visit, such as interactive chat forums and exchange boards. Users on these websites are more likely to act in abnormally careless manners. Users will not hesitate to click on links provided on these types of website. These websites are referred to as watering holes because hackers trap their victims.

An example of water holing is the exploitation of vulnerabilities in a site such as StackOverflow.com, which is often frequented by IT personnel. If the site is bugged, a hacker could inject malware into the computers of the visiting IT staff.

Baiting:- An attacker will leave a malware-infected external storage device in a place where other people can easily find it. It could be in the washroom of an organization, in the elevator, at the reception desk, on the pavement, or even in the parking lot. Greedy or curious users in an organization will then retrieve the object and hurriedly plug it into their machines.

Quid quo pro:- These attackers do not have any advanced tools at their disposal and do not do research about the targets. These attackers will keep calling random numbers claiming to be from technical support, and will offer some sort of assistance

Types of Social Engineering Attacks

Tailgating: Most organizational premises have electronic access control and users normally require biometric or RFID cards to be allowed in. An attacker will walk behind an employee that has legitimate access and enter behind them. At times, the attacker may ask an employee to borrow their RFID card, or may gain entry by using a fake card under the guise of accessibility problems.

Internal Reconnaissance

Internal reconnaissance is done on-site. This means that the attacks are carried out within an organization's network, systems, and premises. Mostly, this process is aided by software tools. An attacker interacts with the actual target systems in order to find out information about its vulnerabilities.

External reconnaissance is done without interacting with the system, but by instead finding entry points through humans that work in the organization. That is why most external reconnaissance attempts involve hackers trying to reach users through social media, emails, and phone calls. Internal reconnaissance is still a passive attack since the aim is to find information that can be used in future for an even more serious attack

Sniffing

- Sniffing tools are designed to capture the packets being transmitted over a network and to perform analysis on them, which is then presented in a human-readable format.

- Packet Sniffing is the process of expanding monitors checks every packet that passes through any network.

- Packet Sniffers will give network administrators the to monitor their networks and get insights into that. Thus, you can detect the root cause of network issues, troubleshoot the networking issues, traffic analyzing, the bandwidth of management, and network security and compliance to deal with it.

Sniffing Tools

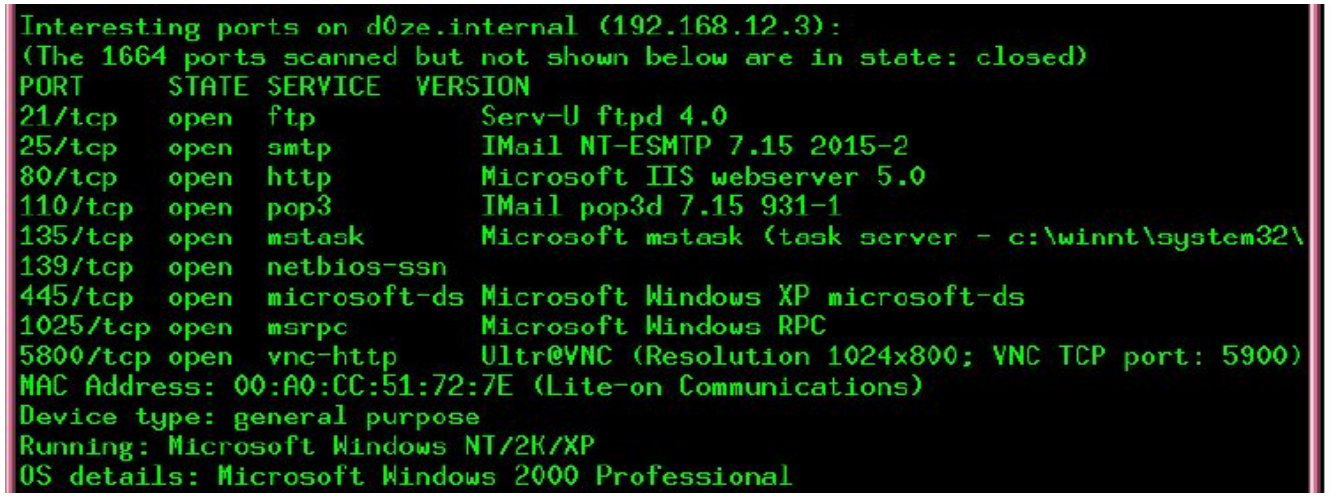
TcpDump: This is an open-source sniffing tool that is used for packet capture and analysis. Tcpdump runs using a command line interface. Tcpdump has also been custom-designed for packet capturing as it does not have a GUI that enables the analysis and display of data. It is a tool with one of the most powerful packet-filtering capabilities and can even selectively capture packets.

Wireshark:- The tool is so powerful that it can steal authentication details from the traffic sent out of a network. Wireshark features include capturing packets,importing pcap files, displaying protocol information about packets, exporting captured packets in multiple formats, colorizing packets based on filters, giving statistics about a network, and the ability to search through captured packets.

Scanning

In this subphase of reconnaissance, an attacker will critically examine weak points identified in the reconnaissance phase. It involves the use of various scanning tools to find loopholes that can be exploited to stage an attack. Attackers take a considerable amount of time in this stage as they know that it determines a significant percentage of their success.

Nmap Tool



Scanning Tools

1. Nmap

- Nmap is a free and open source network mapping tool that is available for Windows, Linux, and macOS.
- Nmap can do an inventory of the devices connected to a target network, identify the open ports that could be exploited, and monitor the uptime of hosts in the network.
- This tool is also able to tell the services running on a network's hosts to fingerprint the operating systems used by the hosts and to identify the firewall rules being enforced in the network.
- User interface tool called Zenmap. Zenmap is a tool for beginners that comes with all the functionalities of Nmap.

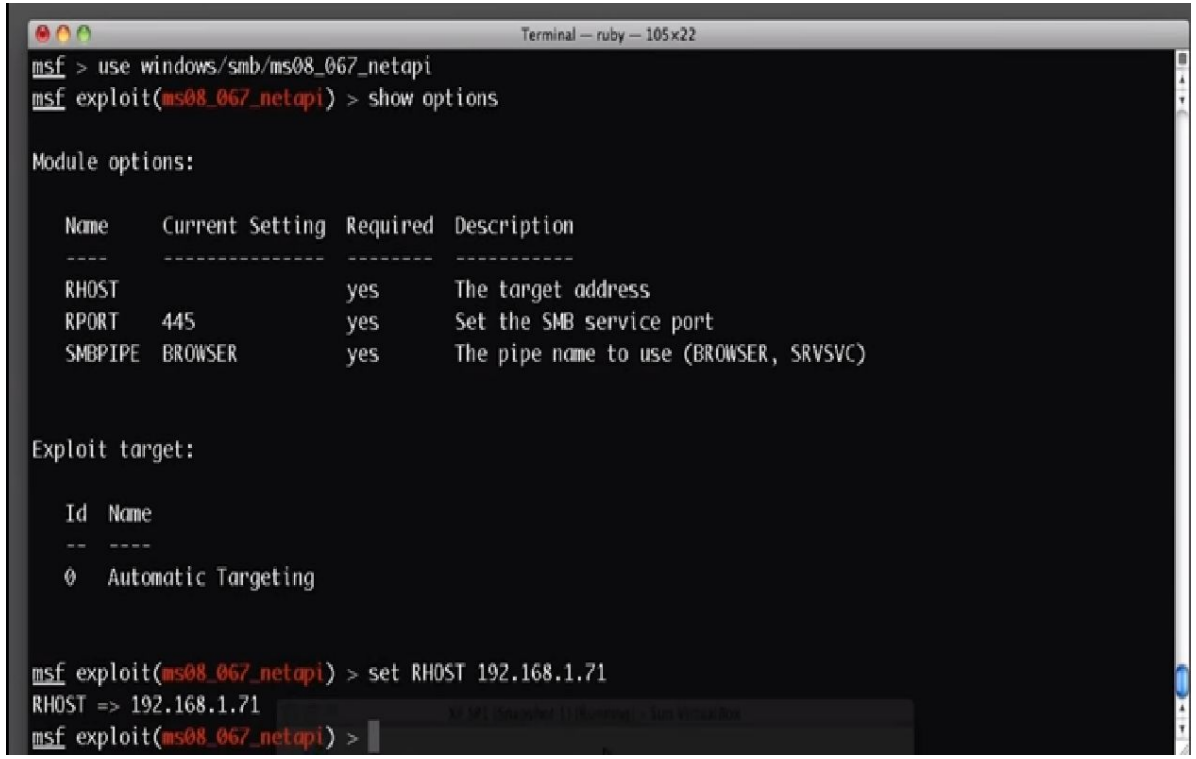
#nmap www.targetsite.com
#nmap 255.250.123.189

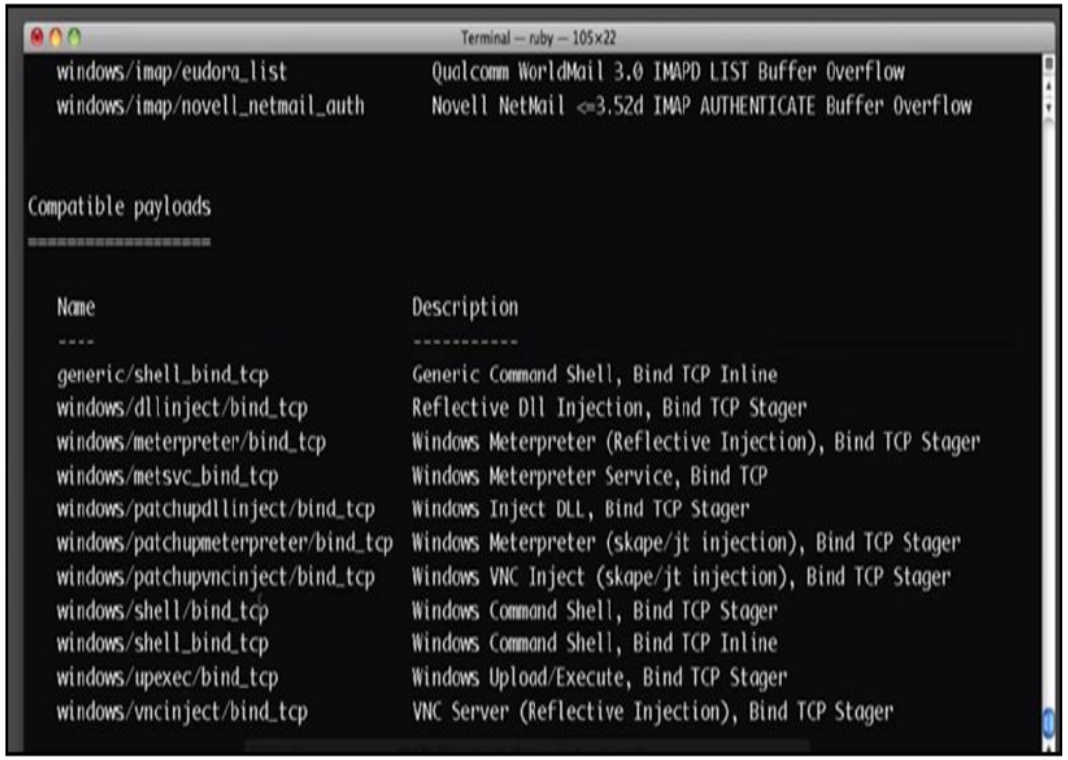
2. Metaspoilt

- This is a Linux-based hacking framework that has been used countless times by hackers. This is because Metasploit is made up of numerous hacking tools and frameworks that have been made to effect different types of attacks on a target.

Scanning Tools

- The Metasploit is run from a Linux terminal, which gives a command-line interface console from which exploits can be launched. The framework will tell the user the number of exploits and payloads that can be used. The user has to search for an exploit to use based on the target or what is to be scanned on a target's network.





Scanning Tools

Wardriving:- This is an internal reconnaissance technique used specifically for surveying wireless networks and is commonly done from an automobile. It is targeted mostly at unsecured Wi- Fi networks.

Network stumbler: Windows-based and it records SSIDs of unsecured wireless networks before using GPS satellites to record the exact location of the wireless network

Mini stumbler: Mini stumbler is a related tool, but has been designed to run on tablets and smartphones.

Aircrack-ing Aircrack-ng is a dangerous suite of tools that is used for wireless hacking, It is important to note that Aircrack-ng relies on other tools to first get some information about its targets. Mostly, these programs discover the potential targets
that can be hacked.

Scan rand

Cabin and Abel

Internal Reconnaissance: Scanning/Sniffing Tools

tcpdump:-

It is a command line-based packet sniffer. It covers all layers, you can capture the packets. It comes pre-installed in kali linux.

- tcpdump --help
- tcpdump -i eth0 -v (it can capture wide variety of data)
- tcpdump -i eth0 -v host 192.168.62.129(in the kali linux browser open 192.168.62.129 go to mutillidae and start clicking on some other tabs..)
- tcpdump -i eth0 -v src 192.168.62.128(start browsing in kali linux machine)
- tcpdump -i eth0 -v dst 192.168.62.129(in the kali linux browser open 192.168.62.129 go to mutillidae)
- tcpdump -i eth0 -v dst 192.168.62.129 and src 192.168.62.128
- tcpdump -i eth0 -v net 192.168.62.0/24
- tcpdump -i eth0 -v tcp and net 192.168.62.0/24
- tcpdump -i eth0 -v src port 80 and dst 192.168.62.129
- tcpdump -w /home/kali/traffic.pcap -i eth0 -v tcp and net 192.168.62.0/24

Nikto:

Ensure both kali linux and metaspoiltable 2 vm are up and running

Open 192.168.62.129 in kali linux browser.

- nikto -host http://192.168.62.129/phpAdmin/
- nikto -host 192.168.62.129
- nikto –help
- nikto -h http://192.168.62.129/phpAdmin/ -o out.txt
- cat out.txt
- nikto -h http://192.168.62.129/phpAdmin/ -Cgidirs -C
- nikto -h http://192.168.62.129/phpAdmin/ -f csv -o 1.csv
- cat 1.csv

Scanning/Sniffing Tools

Nessus Vulnerability Scanner:-

Nessus provides a range of services, including vulnerability assessments, network scans, web scans, asset discovery, and more, to aid security professionals, penetration testers, and other cybersecurity enthusiasts in proactively identifying and mitigating vulnerabilities in their networks.

Nessus tool for vulnerability scanner

- https://www.tenable.com/products/nessus/nessus-essentials
- Installing Nessus on kali linux
- Download the Nessus package for Debian on the Nessus website and make sure you set the Platform to Linux-Debian-amd64.
- When it's finished downloading, open your Linux terminal and navigate to the location you downloaded the Nessus file to.
- Install Nessus using this command:
- sudo dpkg -i Nessus-10.4.1-debian9_amd64.deb
- Start the Nessus service with this command:

Scanning/Sniffing Tools

- sudo systemctl start nessusd.service
- On your browser, go to https://kali:8834/. It would show a warning page.
- Click on Advanced. Then, click on Accept Risk and Continue.
- Choose the Nessus Product you prefer. If you want the free version of Nessus, click on Nessus Essentials.
- Enter your name and email address to receive an activation code by email. Paste the activation code into the space provided and choose a username and password.
- Allow Nessus to download the necessary plugins.
- Once the plugin downloads have completed, you can start using the Nessus service.

Scanning/Sniffing Tools

Wireshark:

- Ensure both the Kali Linux and Metasploitable2 virtual machines are up and running.
- Open Kali Linux and navigate to Applications -> Snipping & Spoofing -> Wireshark.
- Select the interface (eth0) to capture network traffic.
- Access the browser on Kali Linux and enter the IP address of the Metasploitable2 VM (e.g., 192.168.62.129) to open the Mutillidae website.
- Navigate to Damn Vulnerable Web Application (DVWA) and proceed to the login page.
- Enter random credentials (e.g., username: admin, password: 12345) and attempt to log in, resulting in a login failure message.
- Switch to Wireshark, where traffic interception has begun.
- In the filter bar, type "http" and select the http with post stream contains login.php page.
- Right-click on HTTP traffic, choose "Follow," then "HTTP stream" to open a new window.
- The new window displays intercepted traffic containing the username and password entered on the DVWA login page, showcasing successful traffic interception using Wireshark

John the Ripper

A popular offline password cracker is John the Ripper. This tool enables security practitioners to crack passwords, regardless of encrypted or hashed passwords, message authentication codes (MACs) and hash-based MACs (HMACs), or other artifacts of the authentication process.

adduser admin

provider the password.

cat /etc/shadow
cp /etc/shadow ./pass.txt

In pass.txt, have only recent added details to be cracked.

john -format=crypt pass.txt

john --show pass.txt

Access and Privilege Escalation

This phase comes after an attacker has already identified a target, and scanned and exploited its vulnerabilities using the previously discussed tools and scanning tools. The main focus of the attacker in this phase is to maintain access and move around in the network while remaining undetected.

Privilege escalation can be done in two ways: vertical, and horizontal:

Vertical privilege escalation	Horizontal privilege escalation
Attacker moves from one account to another that has a higher level of authority	Attacker uses the same account, but elevates its privileges
Tools used to escalate privileges	User account used to escalate privileges

Table 1: A comparison of horizontal and vertical privilege escalation

Vertical Privilege Escalation

- Vertical privilege escalation is where the attacker has to grant the higher privileges to himself/herself.
- It is a complex procedure since the user has to perform some kernel-level operations to elevate their access rights.
- Once the operations are done, the attacker is left with access rights and privileges that allows them to run any unauthorized code.
- The rights acquired using this method are those of a super user that has higher rights than an administrator.
- Due to these privileges, an attacker can perform various harmful actions that not even an administrator can stop.
- In Windows, vertical escalation is used to cause buffer overflows that attackers use to execute arbitrary code.

Horizontal Privilege Escalation

- Horizontal privilege escalation, on the other hand, is simpler since it allows a user to use the same privileges gained from the initial access.
- A good example is where an attacker has been able to steal the login credentials of an administrator of a network. The administrator account already has high privileges that the attacker assumes immediately after accessing it.
- Horizontal privilege also occurs when an attacker is able to access protected resources using a normal user account.

Exfiltration

- This is the phase where the main attack starts. Once an attack has reached this phase, it is considered successful.
- The attacker normally has unobstructed freedom to move around a victim's network and access all its systems and sensitive data.
- The attacker will start extracting sensitive data from an organization. This could include trade secrets, usernames, passwords, personally identifiable data, top-secret documents, and other types of data.
- Attackers normally steal huge chunks of data in this stage. This data can either be sold off to willing buyers or leaked to the public.

Sustainment

- Sustainment happens when the attackers are already freely roaming in the network and copying all data that they think is valuable.
- They enter this stage when they want to remain undetected. There is an option to end the attack in the previous stage when data has already been stolen and can either be publicized or sold.
- Highly motivated attackers that want to completely finish off a target choose to continue with the attack, though. Attackers install malware, such as rootkit viruses, that assure them of access to the victim's computers and systems whenever they want.
- The main aim of entering this stage is to buy time to perform another and even more harmful attack than exfiltration. The attacker is motivated to move past data and software and attack the hardware of an organization.

Assault

- Assault is the most feared stage of any cyber-attack.
- It is where the attacker does damage exceeding the data and software. An attacker might disable or alter the functioning of the victim's hardware permanently.
- The attacker focuses on destroying hardware controlled by the compromised systems and computing devices.

Example:

- A good example of an attack that got to this phase is the Stuxnet attack on Iran's nuclear station.
- It was the first recorded digital weapon to be used to wreak havoc on physical resources.
- Initially, Stuxnet is used to manipulate valves in the nuclear facility, causing the pressure to build up and damage a few devices in the plant. The malware was then modified to attack a larger target, the centrifuges.
- The malware was transmitted to the target computers through USB thumb drives, since they were not connected to the internet. Once it infected one of the target computers, the malware replicated itself and spread to the other computers.
- The Stuxnet malware shows the heights that this phase can reach. The Iranian nuclear facility stood no chance of protecting itself as the attackers had already gained access, escalated their privileges, and stayed out of sight from security tools.

Obfuscation

- This is the last stage of the attack which some attackers may choose to ignore.
- The main aim here is for the attackers to cover their tracks for various reasons.
- If the attackers do not want to be known, they use various techniques to confuse, deter, or divert the forensic investigation process that follows a cyber-attack.

Obfuscation is done in many ways.

- One of the ways that attackers prevent their adversaries from catching up with them is by obfuscating their origins.

Example: Hackers at times attack outdated servers in small businesses and then laterally move to attack other servers or targets.

This type of obfuscation was recently witnessed in a university where the IoT lights were hacked into and used to attack the university's servers.

- Another origin obfuscation technique is the use of public school servers. Hackers have repeatedly used this technique where they hack into vulnerable web applications of public schools and move laterally into the schools' networks, installing backdoors and rootkit viruses to the servers.
- Hackers commonly use is the stripping out of metadata. Metadata can be used by law enforcement agencies to catch up with perpetrators of some crimes.

Obfuscation

- It is also common for hackers to cover their trails using dynamic code obfuscation. This involves the generation of different malicious codes to attack targets, but prevents detection from signature-based antivirus and firewall programs.

- The pieces of code can be generated using randomizing functions or by changing some function parameters. Therefore, hackers make it significantly harder for any signature based security tool to protect systems against their malicious codes. This also makes it difficult for forensic investigators to identify the attacker as most of the hacking is done by random code.

Threat Life Cycle Management

- An investment in threat life cycle management can enable an organization to stop attacks just as they happen.
- Cybercrimes are increasing because there are more motivated threat actors. Cybercrime has become a low-risk, high-return business for some people. Despite the increase in the number of breaches, there has been a very low conviction rate, which shows that very few cyber criminals get caught.
- Cyber criminals are today able to access numerous exploits and malware that are for sale, provided that they can pay commensurate amounts of money.
- Cybercrime has become a business that has sufficient suppliers and willing buyers.
- There is expansion of attack surfaces by organizations. New technologies have been adopted, bringing new vulnerabilities and therefore widening the surface area that cybercriminals can attack.
- IOT (Internet of Things) caused number of companies to be hacked.

Threat Life Cycle Management

- The best investment that they can make now is in threat life cycle management to allow them to respond appropriately to attacks based on the phase that they are in.

Phases of threat life cycle management.

- Forensic Data Collection
  --Organizations should collect security event and alarm data.
  -- Collect of log and machine data.
  --Forensic sensor data
- Discovery Phase
  --Search Analytics-IT employees carry out software aided analytics
  -Identify known or reported exceptions from network and antivirus security tools.
  --Machine Analytics-The software normally has machine learning capabilities ,artificial intelligence, enabling them to autonomously scan large amounts of data and give brief and simplified results to people to further analyze

- Qualification Phase

Threat Life Cycle Management

- Investigation Phase
  - In the investigation phase, threats are categorized as true positives are fully investigated to determine whether or not they have caused a security Incident.
  - This phase requires continuous access to forensic data and intelligence about many threats.
  - This phase also looks at any potential damage a threat might have done in organization before it was identified by security tools.

- Neutralization Phase
  - Here mitigation techniques are applied to eliminate or reduce the impact of an identified threat to an organization
  - Organizations strive to get to this stage as quickly as possible since threat involving ransomware might do reversible damage in short period of time.

- Recovery
  - This phase comes once the organization is sure that its identified threats have been neutralized.
  - The aim here is to restore the organization data in less time.
  - Recovery is less time critical and it is highly depends on the type of software or services being made available again.