CYBER SECURITY AND NETWORKING

What is Ethical hacking

Ethical hacking, also known as "white hat" hacking, is the practice of using hacking techniques and tools to identify security vulnerabilities in computer systems, networks, and applications. The primary goal of ethical hacking is to help organizations identify and fix potential security weaknesses before malicious attackers can exploit them.

It's important to note that ethical hacking is legal and is done with the consent of the organization being tested. Ethical hackers are bound by strict ethical guidelines and codes of conduct, and they must operate within the law and respect the privacy of individuals and the organizations they are testing.

Hacker Process : Reconnaissance - Scanning – gaining access – maintaining access – erasing clues

Ethical hacker : Reconnaissance - Scanning – gaining access –writing report – presenting reports

- ✓ Ethical Hacking: Also known as "white hat" hacking, ethical hacking involves using hacking techniques to identify and report security vulnerabilities in computer systems, networks, and applications. This type of hacking is done with the permission of the organization being tested, and the goal is to improve their security.

- ✓ Black Hat Hacking: Black hat hackers use hacking techniques to gain unauthorized access to computer systems and networks for malicious purposes, such as stealing data or causing damage. This type of hacking is illegal and can result in severe consequences for the hacker if caught.

- ✓ Grey Hat Hacking: Grey hat hackers are a mix of ethical and black hat hackers. They may identify security vulnerabilities in computer systems without permission but will report the vulnerabilities to the organization instead of exploiting them for malicious purposes.

- ✓ Hacktivism: Hacktivists use hacking techniques to promote a political or social agenda. They may deface websites or leak sensitive information to expose wrongdoing or bring attention to an issue.

- ✓ Script Kiddies: Script kiddies are individuals who use pre-made hacking tools and scripts to launch attacks on computer systems without understanding the underlying principles or techniques.

Type of Hacking

Black box hacking is a type of penetration testing or ethical hacking technique in which the tester has no prior knowledge or access to the internal workings or architecture of the system being tested. This technique simulates an attack from an external threat actor with no insider knowledge. In black box testing, the tester is given no information about the target system other than its external interface, such as a website or an API. The goal is to identify vulnerabilities and potential attack vectors that could be exploited by a malicious actor. Black box testing requires the tester to use a combination of manual and automated techniques to identify weaknesses in the system. The tester may use tools such as port scanners, vulnerability scanners, and password cracking software to identify potential attack vectors. One of the advantages of black box testing is that it provides a realistic simulation of a real-world attack scenario. However, it can also be time-consuming and may not identify all possible vulnerabilities in the system

White box hacking is a type of penetration testing or ethical hacking technique in which the tester has full access to the internal workings or architecture of the system being tested. This technique simulates an attack from an insider or a trusted user with knowledge of the system. In white box testing, the tester has access to the source code, network diagrams, and other technical documentation related to the system being tested. The goal is to identify vulnerabilities and potential attack vectors that could be exploited by an attacker with insider knowledge. White box testing requires the tester to use a combination of manual and automated techniques to identify weaknesses in the system. The tester may use tools such as code analyzers, network scanners, and vulnerability scanners to identify potential attack vectors. One of the advantages of white box testing is that it provides a comprehensive understanding of the system being tested, which can help identify vulnerabilities that may not be apparent from an external perspective. However, it may not simulate a realistic attack scenario, and it can be costly and time-consuming.

Grey box hacking is a type of penetration testing or ethical hacking technique that combines elements of black box and white box testing. In grey box testing, the tester has limited knowledge or access to the internal workings or architecture of the system being tested. The tester may have partial knowledge of the system, such as a basic understanding of the network topology or access to certain user accounts or system logs. The goal is to identify vulnerabilities and potential attack vectors that could be exploited by an attacker with limited insider knowledge. Rey box testing requires the tester to use a combination of manual and automated techniques to identify weaknesses in the system. The tester may use tools such as vulnerability scanners, password cracking software, and social engineering techniques to identify potential attack vectors. One of the advantages of grey box testing is that it provides a more realistic simulation of an attack scenario than black box testing, while still allowing the tester to identify potential vulnerabilities that may not be apparent from an external perspective. However, it can still be time-consuming and may not identify all possible vulnerabilities in the system. Overall, grey box testing is an important part of any comprehensive security testing program and can help identify and address potential security weaknesses before they are exploited by attackers.

Hacking modalities

Hacking modalities refer to the different methods and techniques that are used by hackers to gain unauthorized access to computer systems and networks.

- **Social engineering**: Social engineering is the practice of manipulating people into divulging sensitive information or performing actions that they should not.
- **Password cracking**: Password cracking involves using software or tools to guess or brute-force passwords to gain access to a system or network.
- **Malware**: Malware refers to malicious software, such as viruses, Trojans, and worms, that can be used to gain access to a system, steal data, or cause damage.
- **Phishing**: Phishing is a type of social engineering attack that uses email or other electronic communication to trick individuals into revealing sensitive information, such as usernames and passwords.
- **Denial-of-service (DoS) attacks**: A DoS attack involves flooding a system with traffic or requests in an attempt to overwhelm it and cause it to crash or become unavailable.
- **SQL injection**: SQL injection involves exploiting vulnerabilities in web applications that allow an attacker to execute malicious SQL commands and gain access to sensitive data.
- **Man-in-the-middle (MitM) attacks**: A MitM attack involves intercepting communications between two parties in order to eavesdrop, steal data, or manipulate the communication

Social engineering

Social engineering hacking is a type of cyber attack that involves the manipulation of human behavior to gain access to confidential information, computer systems, or networks. It is a technique that attackers use to exploit human trust, emotions, and natural inclinations in order to trick individuals into divulging sensitive information or granting access to computer systems or networks.

Social engineering attacks can take many forms, such as phishing emails, pretexting, baiting, and many others. These attacks can be highly effective because they exploit the weakest link in the security chain, which is the human element. They can cause significant damage to individuals, organizations, and their computer systems or networks.

Wardialing is a technique used to scan and identify active phone numbers by dialing a range of phone numbers sequentially with the help of an automated system. It is a type of reconnaissance or information-gathering activity that can be used for various purposes, such as identifying vulnerable systems or discovering hidden or unlisted phone numbers.

Example kismet : sudo airmong –ng start wirless ide

: sudo kismet –c wirless ide

Physical security ethical hacking involves testing the security measures of a physical space, such as a building or data center, by attempting to gain unauthorized access or bypass security controls. This is typically done with the permission of the owner or organization responsible for the security of the space, as part of a comprehensive security assessment

Designing a security-related operating system (OS) is a complex and challenging task, requiring expertise in multiple areas such as computer science, cybersecurity, and system design. Here are some high-level considerations for designing a security-related OS:

Secure Boot: The OS should have a secure boot process, which ensures that the system starts with a trusted and verified bootloader. This prevents malware or other unauthorized software from being loaded onto the system during boot-up.

Access Control: The OS should have strong access control mechanisms to prevent unauthorized access to the system or specific files. This can include features like user authentication, file permissions, and encryption.

Network Security: The OS should have strong network security capabilities to prevent unauthorized access or data breaches. This can include features like firewalls, intrusion detection and prevention, and secure communication protocols.

Application Security: The OS should have strong application security capabilities to prevent unauthorized or malicious applications from running on the system. This can include features like sandboxing, whitelisting, and application isolation.

System Monitoring: The OS should have strong system monitoring capabilities to detect and respond to potential security threats. This can include features like system logs, intrusion detection, and real-time alerts.

Update Management: The OS should have a robust update management process to ensure that security patches and other updates are applied in a timely and secure manner. This can include features like automatic updates, patch management, and rollback capabilities.

Secure Configuration: The OS should be configured in a secure manner by default, with minimal attack surface and strong security controls. This can include features like disabling unnecessary services and applications, hardening system configurations, and disabling insecure protocols.

Purpose for hacking : area , use friendly operating system

Identify Tool : which tool can use and identify opensource and commercial tools

Example foot printing

exploitation tool

System Hacking tool

Reconnaissance or footprinting

Reconnaissance, also known as foot printing, is the process of gathering information about a target system or network in order to identify potential vulnerabilities and weaknesses that could be exploited by an attacker

Reconnaissance techniques can involve passive information gathering, such as searching for publicly available information about the target through search engines, social media, or public records. Active reconnaissance methods can also be used, such as scanning the target network for open ports, identifying the operating systems and software versions in use, and mapping the network topology.

Google hacking

Google operators:

+ (plus symbol): is used to include words that because they are very common are not included on Google search results. For example, say that you want to look for company The X, given that the article “the” is very common, it is usually excluded from the search. If we want this word to be included, then we write our search text like this: Company +The X

- (minus symbol): is used to exclude a term from results that otherwise could include it. For example, if we are looking for banking institutions, we could write: banks -furniture

”” (double quotes): if we need to find a text literally, we framed it in double quotes. Example: “Company X”

~ (tilde): placing this prefix to a word will include synonyms thereof. For example, search by ~company X will also include results for organization X

OR: This allows you to include results that meet one or both criteria. For example, “Company X General Manager” OR “Company X Systems Manager”

Scanning

HTTrack is a free and open-source website copier that allows users to download a website from the internet to a local directory on their computer. It works by recursively downloading all the web pages, images, videos, and other resources that are linked from the website's pages.
https://www.httrack.com/

Ethical hacking scanning is the process of systematically examining a computer system or network to identify vulnerabilities that could be exploited by attackers. Ethical hackers use a variety of scanning tools and techniques to identify weaknesses in a system, with the goal of providing recommendations for improving security. There are several types of scanning that ethical hackers may use during their assessments, including:

Network Scanning: This type of scanning involves examining the network to identify open ports, services, and other devices that are connected to the network. Network scanning tools can help identify potential vulnerabilities in the network, such as unpatched software, weak passwords, or misconfigured systems.

Vulnerability Scanning: This type of scanning involves using automated tools to search for known vulnerabilities in the system. These tools can help identify vulnerabilities in operating systems, applications, and other software that could be exploited by attackers.

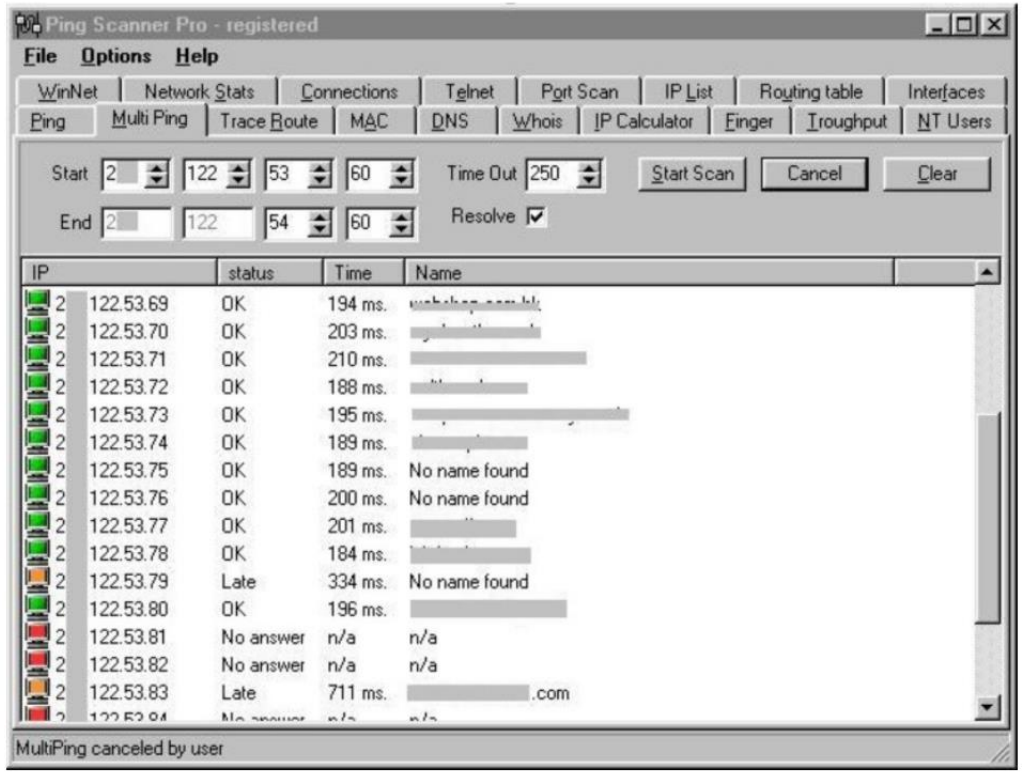
Web Application Scanning: This type of scanning involves examining web applications to identify vulnerabilities such as SQL injection, cross-site scripting, and other security weaknesses that could be exploited by attackers.

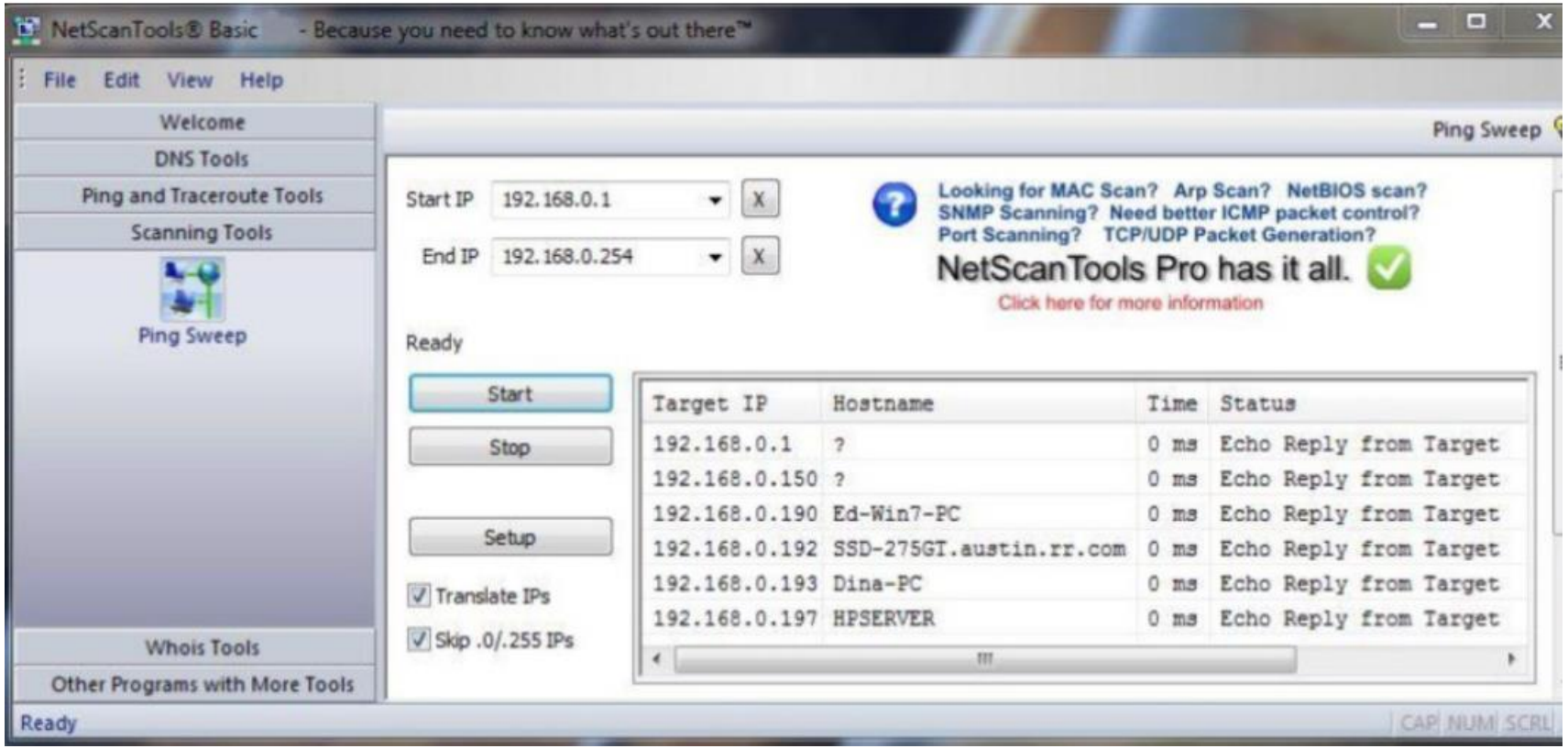
Wireless Scanning: This type of scanning involves examining wireless networks to identify potential vulnerabilities, such as weak encryption or unauthorized access

- Ping sweepers

- A ping sweeper is a tool that sends ICMP (Internet Control Message Protocol) echo requests to a range of IP addresses to determine which hosts are live and reachable on a network. This is also known as an ICMP sweep. Ping sweepers can be useful for network administrators to quickly identify all devices connected to a network, troubleshoot connectivity issues, or detect unauthorized devices on the network

There are many free and commercial ping sweeper tools available, such as Fping, Angry IP Scanner, Nmap, and SolarWinds Ping Sweep.




NetScanTools® Basic - Because you need to know what's out there™
File Edit View Help
Welcome
DNS Tools
Ping and Traceroute Tools
Scanning Tools
Ping Sweep
Whois Tools
Other Programs with More Tools
Ping Sweep
Start IP 192.168.0.1
End IP 192.168.0.254
Looking for MAC Scan? Arp Scan? NetBIOS scan?
SNMP Scanning? Need better ICMP packet control?
Port Scanning? TCP/UDP Packet Generation?
NetScanTools Pro has it all.
Click here for more information
Ready
Start
Stop
Setup
Translate IPs
Skip .0/.255 IPs
Target IP Hostname Time Status
192.168.0.1 ? 0 ms Echo Reply from Target
192.168.0.150 ? 0 ms Echo Reply from Target
192.168.0.190 Ed-Win7-PC 0 ms Echo Reply from Target
192.168.0.192 SSD-275GT.austin.rr.com 0 ms Echo Reply from Target
192.168.0.193 Dina-PC 0 ms Echo Reply from Target
192.168.0.197 HPSERVER 0 ms Echo Reply from Target
Ready
CAP NUM SCRL

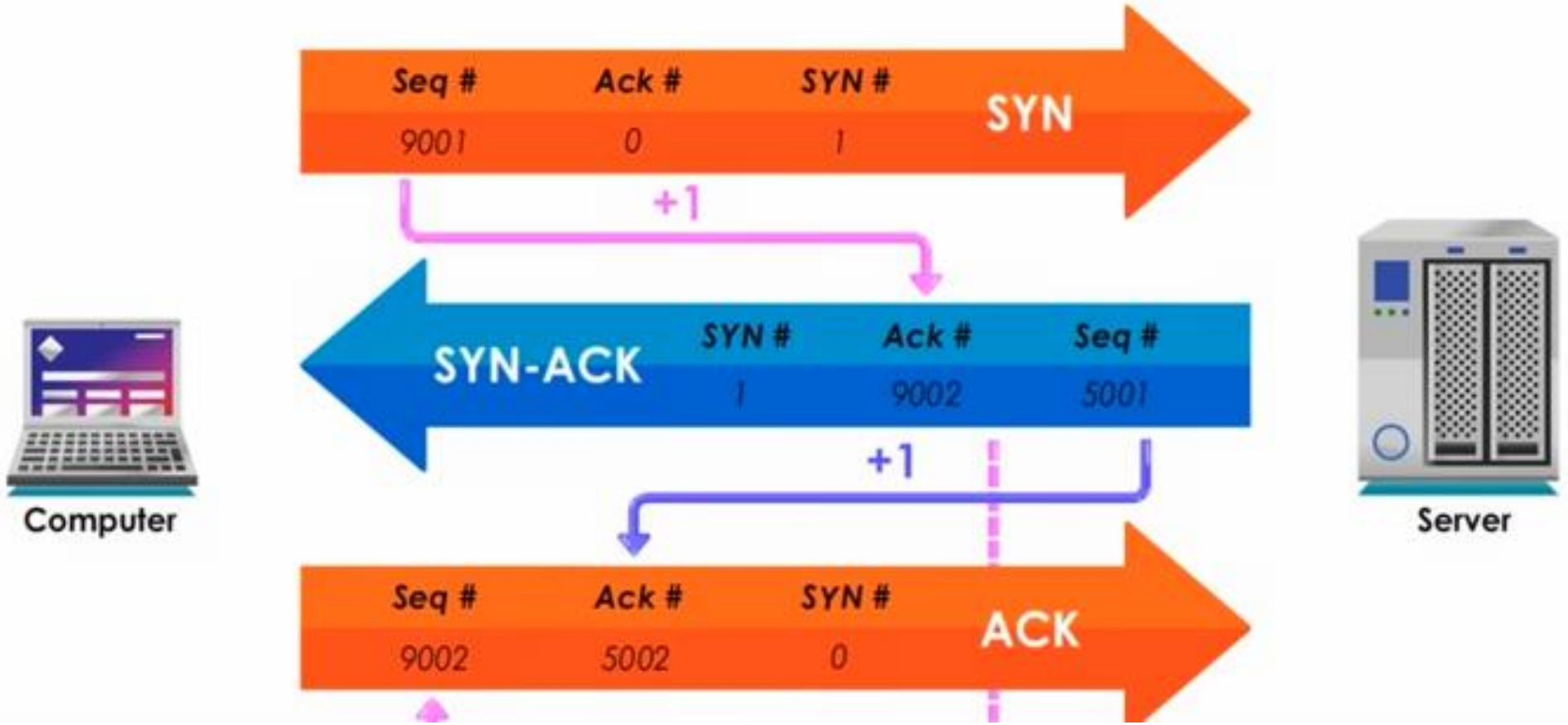
A three-way handshake is a method used by the Transmission Control Protocol (TCP) to establish a reliable connection between two networked devices. The three-way handshake involves a series of messages exchanged between the two devices to synchronize the sequence numbers used for data transfer and establish the connection.

The three steps in a TCP three-way handshake are:

1.SYN (Synchronize): The client sends a SYN message to the server to initiate the connection. The message includes a sequence number, which is a unique identifier used to keep track of the data being transferred.

2.SYN-ACK (Synchronize-Acknowledge): The server responds with a SYN-ACK message, acknowledging the SYN request and sending its own sequence number. The server's sequence number is an acknowledgement of the client's sequence number, and the server's SYN message is a request for the client to acknowledge its sequence number.

3.ACK (Acknowledge): The client sends an ACK message to the server to acknowledge the server's sequence number. This completes the three-way handshake, and the connection is established.


Seq #
Ack #
SYN #
9001
0
1
SYN
+1
SYN-ACK
SYN #
Ack #
Seq #
1
9002
5001
+1
Seq #
Ack #
SYN #
9002
5002
0
ACK
Computer
Server

Null Scan, Fin Scan, and XMAS Scan are three types of TCP port scans that are commonly used in network reconnaissance by ethical hackers or security analysts to identify open ports on a target system.

Null Scan: A Null Scan is a TCP port scan in which the scanner sends a TCP packet with no flags set (i.e., a "null" packet) to the target system's port. If the port is open, the target system will not respond with a RST (reset) packet, which indicates that the port is closed.

Fin Scan: A Fin Scan is a TCP port scan in which the scanner sends a TCP packet with only the FIN flag set to the target system's port. If the port is open, the target system will not respond with a RST packet, which indicates that the port is closed.

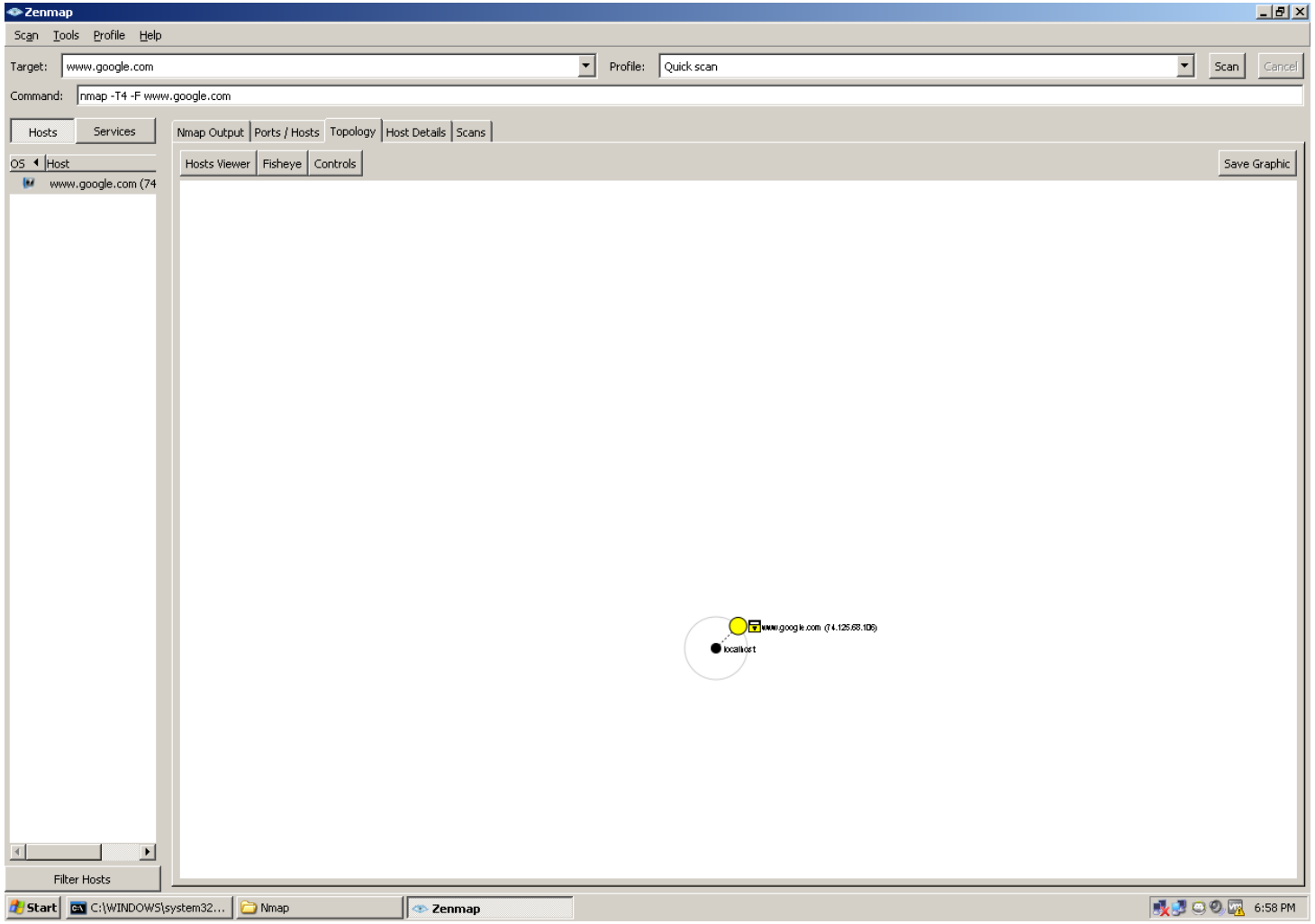
XMAS Scan: An XMAS Scan is a TCP port scan in which the scanner sends a TCP packet with the URG, PUSH, and FIN flags set to the target system's port. If the port is open, the target system will not respond with a RST packet, which indicates that the port is closed.

Public network scanning refers to the process of scanning networks that are accessible from the internet, such as public-facing servers, websites, and other services. This type of scanning is often used by security researchers and attackers to identify vulnerabilities and potential targets.

Private network scanning, on the other hand, refers to the process of scanning networks that are not accessible from the internet, such as internal corporate networks or home networks. This type of scanning is typically used for network troubleshooting and management purposes, as well as for security testing to identify potential vulnerabilities within the internal network.

- NMAP

- NMAP is undoubtedly the most popular port scanner among networking and computer security specialists, partly because of its ease of use, but mainly because of its versatility to scan.



Enumeration is a process used in ethical hacking to gather information about a target system, network or application. Enumeration is the process of identifying usernames, passwords, user accounts, network shares, services, open ports, and other system information that can be used to plan further attacks. Enumeration is often used after a scanning process to obtain additional information about the target.

Enumeration techniques used by ethical hackers may include:

Banner Grabbing: This involves connecting to a network service or application and retrieving the banner message that is displayed when a connection is established. Banner grabbing can be used to identify the version of the service or application being used, which can be useful in identifying vulnerabilities.

User Enumeration: User enumeration is the process of discovering valid usernames on a system, which can be used for further attacks such as password guessing or brute-forcing.

Network Share Enumeration: This involves identifying network shares on a system and determining the permissions associated with those shares. Network shares can provide access to sensitive information, so it's important to identify them and assess the security controls around them.

SNMP Enumeration: Simple Network Management Protocol (SNMP) is a protocol used for managing and monitoring network devices. SNMP enumeration involves querying a network device using SNMP to gather information about the device, including its configuration and network topology

- ✓ nmap -v -A scanme.nmap.org
- ✓ nmap -v -sn 192.168.0.0/16 10.0.0.0/8
- ✓ nmap -v -iR 10000 -Pn -p 80
- ✓ nmap –o 192.168.85.137

Hping is particularly useful for security testing and penetration testing, as it can be used to perform various attacks such as port scanning, denial-of-service (DoS) attacks, and packet injection attacks. It's important to note that using Hping for malicious purposes is illegal and can result in serious consequences

Hping is a command-line tool used for network exploration, auditing, and testing. It can send custom packets to a target host and analyze the responses, allowing you to diagnose network connectivity issues, identify potential security vulnerabilities, and test firewall rules.

Hping supports a wide range of packet types, including ICMP, TCP, UDP, and RAW-IP packets. It also has advanced features such as packet fragmentation, TCP/IP stack fingerprinting, and port scanning.

hping3 -1 target : Sending ICMP echo requests:

hping3 -S target -p 80 : sends TCP SYN packets to port 80 of the target host.

hping3 -2 target -p 53

hping3 -S target -p 80 –flood : "--flood"

hping3 -F target : TCP/IP stack fingerprinting:

Port scanning tool

Ping tester

https://docs.trendmicro.com/all/ent/officescan/v10.6/en-us/osce_10.6_sp1_olh/gls_trojan_port.html

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Banner grabbing

Banner grabbing is a technique used to gather information about a target system or network by inspecting the "banner" or metadata that is returned by a network service when a connection is established.

Passive banner grabbing: Passive banner grabbing involves monitoring the network traffic to capture the banner messages that are sent by the server in response to client connections. This approach does not involve actively initiating connections to the server, and therefore, is less likely to be detected by intrusion detection systems.

Active banner grabbing: Active banner grabbing involves actively connecting to a server and requesting its banner message. This approach can be more effective than passive banner grabbing since it provides more control over the connection and can be used to test for specific vulnerabilities. However, active banner grabbing is more likely to be detected by intrusion detection systems and can generate a large volume of network traffic.

Tools

ID Serve TM : https://www.grc.com/id/idserve.htm

Netcraft

Netcat : Netcat, also known as "nc," is a versatile command-line utility for reading, writing, and redirecting network connections using TCP or UDP protocols. Netcat can be used to create network connections between computers, to transfer data between computers, and to perform other network-related tasks.

countermeasures

•Hide banner messages: One of the most effective ways to prevent banner grabbing is to disable or hide banner messages altogether. This can be accomplished by configuring servers and network services to not send banner messages or to send generic, non-specific banner messages that do not disclose sensitive information.

•Firewalling: Another effective countermeasure is to implement firewall rules that block incoming connections from known banner-grabbing tools or from suspicious IP addresses. Firewall rules can also be used to restrict access to sensitive network services, limiting the opportunities for banner grabbing.

•Network intrusion detection systems (NIDS): NIDS can be used to detect banner-grabbing activities on a network. NIDS can analyze network traffic in real-time and alert administrators if suspicious activity is detected.

•Update software: Keeping software up-to-date with the latest security patches can help to reduce the risk of vulnerabilities being exploited through banner grabbing. This is because many banner-grabbing techniques rely on identifying specific software versions that are known to be vulnerable.

Password-based authentication: This is the most common type of authentication system and involves users providing a username and password to verify their identity. Password-based authentication systems may also use additional security measures such as password complexity requirements, password expiration policies, and two-factor authentication.

Biometric authentication: Biometric authentication involves using physical characteristics such as fingerprints, facial recognition, or iris scans to verify the identity of a user.

Multi-factor authentication: Multi-factor authentication (MFA) involves using more than one type of authentication factor to verify a user's identity. This typically involves combining something the user knows (such as a password) with something the user has (such as a security token) or something the user is (such as a biometric characteristic).

Single sign-on: Single sign-on (SSO) allows users to log in once to access multiple systems or applications. SSO systems typically use a central authentication server to manage user credentials and provide access to authorized systems and applications.

Kerberos authentication: Kerberos is a network authentication protocol that uses encryption to verify the identity of users and secure network communications. Kerberos is commonly used in enterprise environments and is designed to provide strong authentication and secure network access.

System Hacking

- ✓ Brute force attack: A brute force attack involves systematically guessing passwords until the correct one is found. This type of attack is typically only effective against weak passwords or those with a limited character set.

- ✓ Dictionary attack: A dictionary attack involves using a list of common words or phrases to try to guess a user's password. This type of attack is often more effective than a brute force attack, as many users choose passwords that are easy to remember and can be found in a dictionary.

- ✓ Hybrid attack: A hybrid attack combines elements of both brute force and dictionary attacks. This type of attack may use a dictionary of common words, but also incorporate variations such as adding numbers or special characters to the end of each word.

- ✓ Rainbow table attack: A rainbow table attack involves using precomputed tables of hashes to quickly crack passwords. This type of attack is typically used against systems that use unsalted password hashes.

- ✓ Social engineering: Social engineering attacks involve manipulating users to reveal their passwords through deception. For example, an ethical hacker may use phishing emails or phone calls to trick users into revealing their passwords.

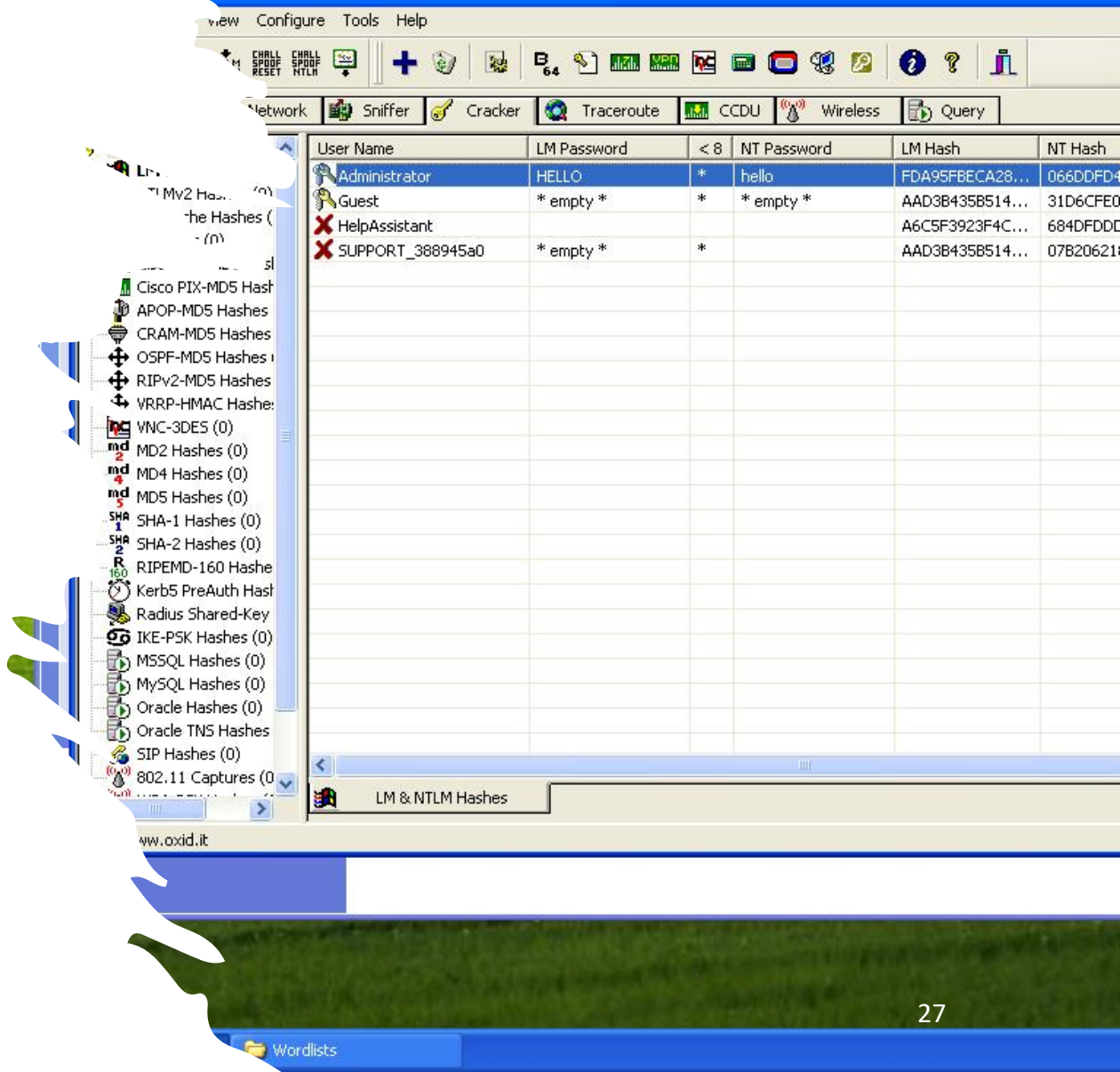
- LM Hash:

- LM Hash is an older password hashing algorithm that was used in earlier versions of Windows. It was designed to be used with the LAN Manager authentication protocol, which was used in Windows NT and earlier versions of Windows. LM Hash works by splitting the password into two 7-byte halves and encrypting each half separately using a weak encryption algorithm. The resulting hash is 16 bytes long and is not considered to be very secure. LM Hash is vulnerable to several types of attacks, including brute force and dictionary attacks.

- NTLM Hash:

- NTLM Hash is a newer password hashing algorithm that was introduced with Windows NT. It is designed to be used with the NTLM authentication protocol, which is used in Windows NT and later versions of Windows. NTLM Hash works by using a more secure encryption algorithm to encrypt the password. The resulting hash is 16 bytes long and is considered to be more secure than LM Hash. However, NTLM Hash is still vulnerable to certain types of attacks, including pass-the-hash attacks and dictionary attacks.

- Tool : Johne and ripper , cain and abel : https://web.archive.org/web/20160311154514/http://www.oxid.it/downloads/ca_setup.exe



countermeasures

Use strong and complex passwords: Strong passwords should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using predictable phrases or words that can be easily guessed.

Enable two-factor authentication (2FA): 2FA is an extra layer of security that requires a user to provide two forms of identification before accessing an account. This can be a code sent to their phone or email, or a physical token.

Limit login attempts: To prevent brute-force attacks, limit the number of login attempts allowed before the account is locked or temporarily suspended.

Use password managers: Password managers are tools that store and encrypt passwords, making it easier to use strong and unique passwords for each account without having to remember them.

Regularly change passwords: It is good practice to change passwords regularly, especially for accounts that contain sensitive information.

Use encryption: Encrypting sensitive data such as passwords can help protect them from being stolen or accessed by unauthorized users

- Steganography is the practice of hiding a message or information within a non-secret file, such as an image, audio file, or video, without altering the original file's appearance. This technique allows users to communicate privately and securely without arousing suspicion

- Slient Eye : https://achorein.github.io/silenteye/

- LSB (Least Significant Bit) Substitution: This method involves replacing the least significant bits of the carrier file with the hidden message bits. Since the least significant bits have the least impact on the overall image, this technique is very effective.
- Spread Spectrum: This method involves spreading the hidden message across several carrier files. This makes it difficult for an attacker to identify the exact file that contains the hidden message.
- Distortn Techniques: This method involves slightly modifying the pixels or data in the carrier file to encode the hidden message. This technique is more complex than LSB substitution and requires advanced algorithms.

countermeasures that can be used to detect or prevent steganography:

Signature Analysis: This involves analyzing the digital signature of the carrier file to detect any anomalies or changes. Any changes in the signature can indicate that the file has been modified and may contain hidden information.

Statistical Analysis: This involves analyzing the statistical properties of the carrier file, such as the distribution of pixel values, to identify any abnormal patterns that may indicate the presence of hidden information.

Content Inspection: This involves inspecting the content of the carrier file to detect any discrepancies between the visual or auditory content and the expected content. For example, if an image appears to contain random patterns or noise, it may indicate the presence of hidden information.

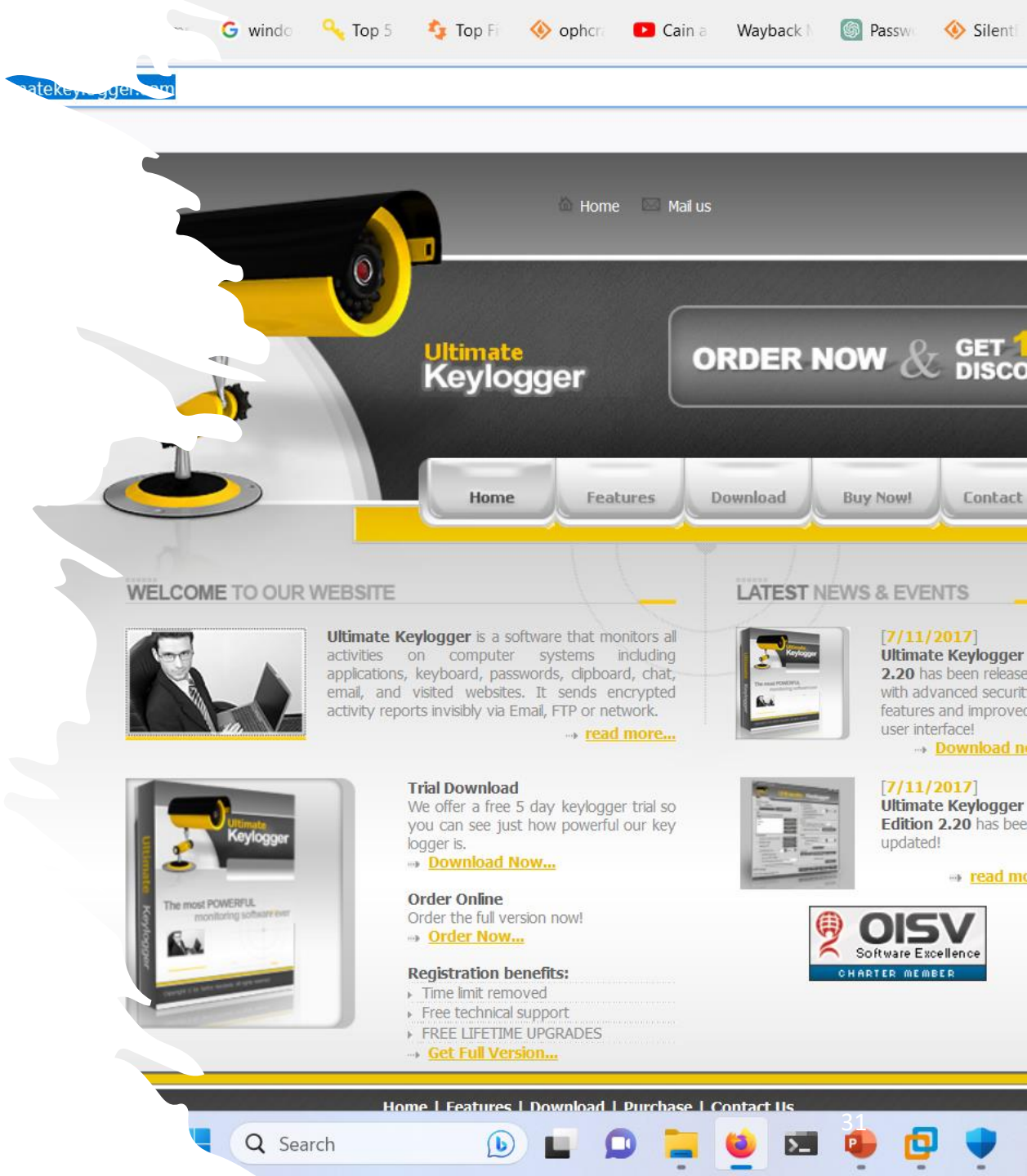
Steganalysis Tools: These are specialized software tools that are designed to detect steganography. They use a combination of signature analysis, statistical analysis, and content inspection to identify hidden information.

Encryption: Encrypting the hidden message before embedding it into the carrier file can make it more difficult to detect. This can be done using standard encryption techniques such as AES or RSA.

Use of Trusted Sources: Only use carrier files from trusted sources to reduce the risk of malware or hidden information being embedded in the files.

keylogger and spyware

- A keylogger is a type of software or hardware device that records every keystroke made on a computer or mobile device. This information can then be used to steal sensitive information such as usernames, passwords, credit card numbers, and other personal data.
- Spyware, on the other hand, is a type of software that is installed on a device without the user's knowledge or consent. Spyware can monitor a user's online activity, capture personal information, and report this data back to the attacker.
- Ultimate keyloggyer : http://www.ultimatekeylogger.com/



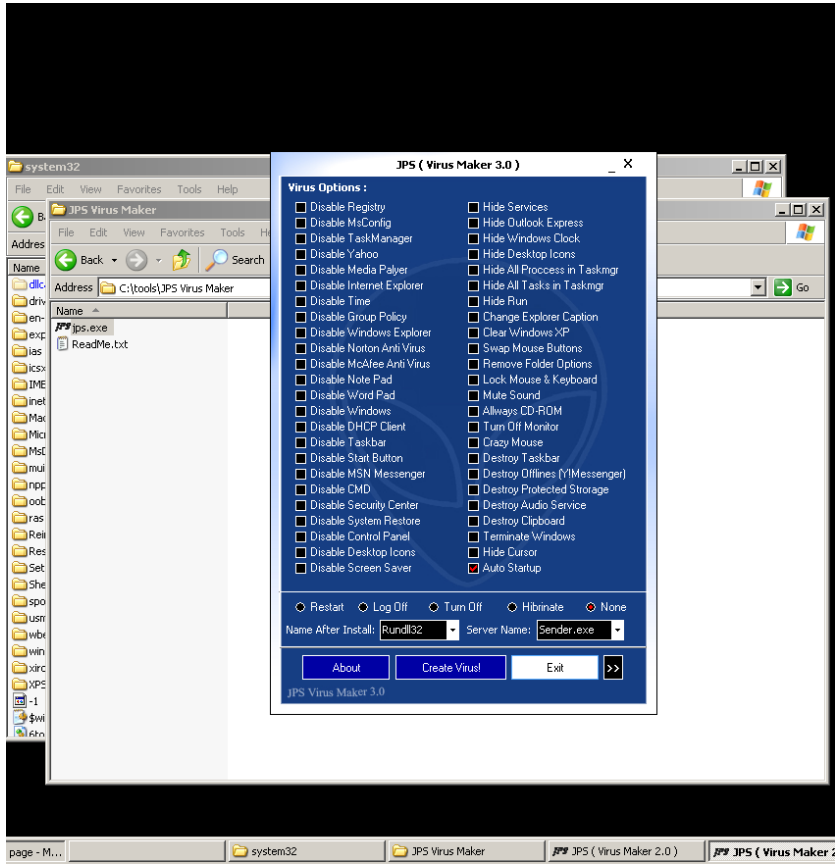
Malware and Virus backdoors

- A backdoor is a type of malicious software (malware) that allows an attacker to gain unauthorized access to a computer system, network, or device. Backdoors can be installed by attackers for the purpose of stealing sensitive information, compromising the system, or using it to launch further attacks on other systems or networks.

- A virus is a type of malware that replicates itself and infects other files or systems. A virus can also contain a backdoor that allows an attacker to gain unauthorized access to a system or network. Once a virus infects a system, it can spread to other systems or files, causing damage or stealing sensitive information.

- Backdoors and viruses can be installed on a system or network through a variety of methods, such as phishing emails, malicious attachments, software vulnerabilities, or even physical access to the system. Once installed, they can give attackers access to sensitive information, control of the system, or the ability to launch further attacks.

- It is important to have proper security measures in place, such as using antivirus software, keeping software up to date, and regularly monitoring systems for suspicious activity. This can help prevent the installation of backdoors and viruses and reduce the risk of a successful attack.



Metasploit

Phases of penetration testing life cycle

- Metasploit is an open-source penetration testing framework that provides a suite of tools and exploits to test the security of computer systems and networks. It was developed by Rapid7 and is widely used by security professionals, ethical hackers, and researchers.

- Metasploit can be used to conduct a variety of penetration testing activities, including reconnaissance, scanning, vulnerability identification, exploitation, and post-exploitation. The framework supports a range of operating systems, including Windows, Linux, and Mac OS X, and can be used in a variety of environments, such as local networks, remote networks, and the internet.

Framework: The Metasploit Framework is the main component of the tool. It provides an interface for executing and creating exploit code against a target system.

Payloads: Payloads are the code that is executed on the target system once an exploit is successful. Metasploit provides a range of payloads, including reverse shells, meterpreter, and others, that can be used to gain access to a target system.

Exploits: Exploits are the pieces of code that take advantage of vulnerabilities in a system or application. Metasploit includes a large database of known exploits that can be used to test the security of a system.

Auxiliary: Auxiliary modules are used to perform various activities that do not require an exploit, such as scanning for vulnerabilities, gathering information about a system, and testing passwords.

Encoders: Encoders are used to modify payloads in order to avoid detection by antivirus software.

Post-exploitation: Post-exploitation modules are used to perform various activities after a successful exploit, such as privilege escalation, lateral movement, and data exfiltration.

Nops: Nops are used to insert no-operation instructions in the payload code in order to keep the payload size constant and avoid detection.

Plugins: Plugins are used to extend the functionality of Metasploit. They can be used to create custom modules or integrate with other security tools.

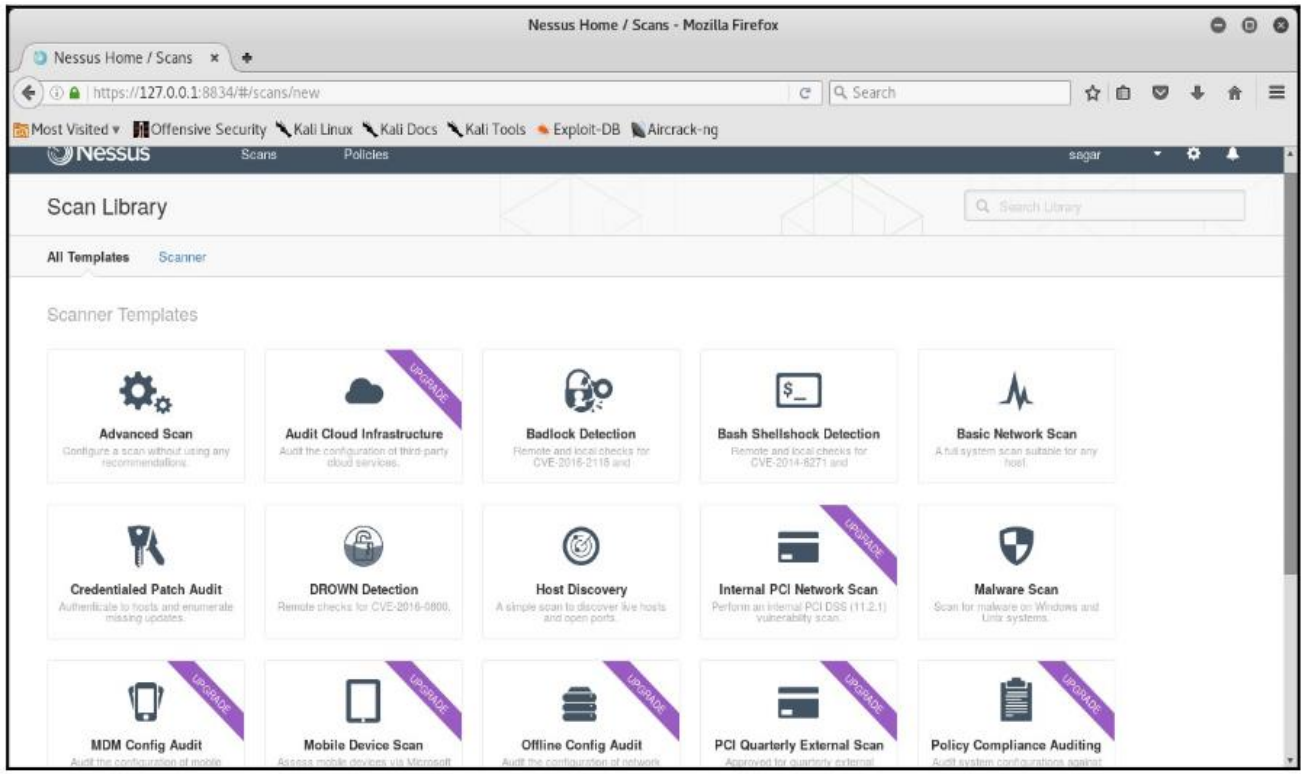
Sr. No.	Penetration testing phase	Use of Metasploit
1	Information Gathering	`Auxiliary modules: portscan/syn, portscan/tcp, smb_version, db_nmap, scanner/ftp/ftp_version`, and `gather/shodan_search`
2	Enumeration	`smb/smb_enumshares`, `smb/smb_enumusers`, and `smb/smb_login`
3	Gaining Access	All Metasploit exploits and payloads
4	Privilege Escalation	`meterpreter-use priv` and `meterpreter-getsystem`
5	Maintaining Access	`meterpreter - run persistence`
6	Covering Tracks	Metasploit Anti-Forensics Project

We'll gradually cover all previous components and modules as we progress through the book.

Nessus

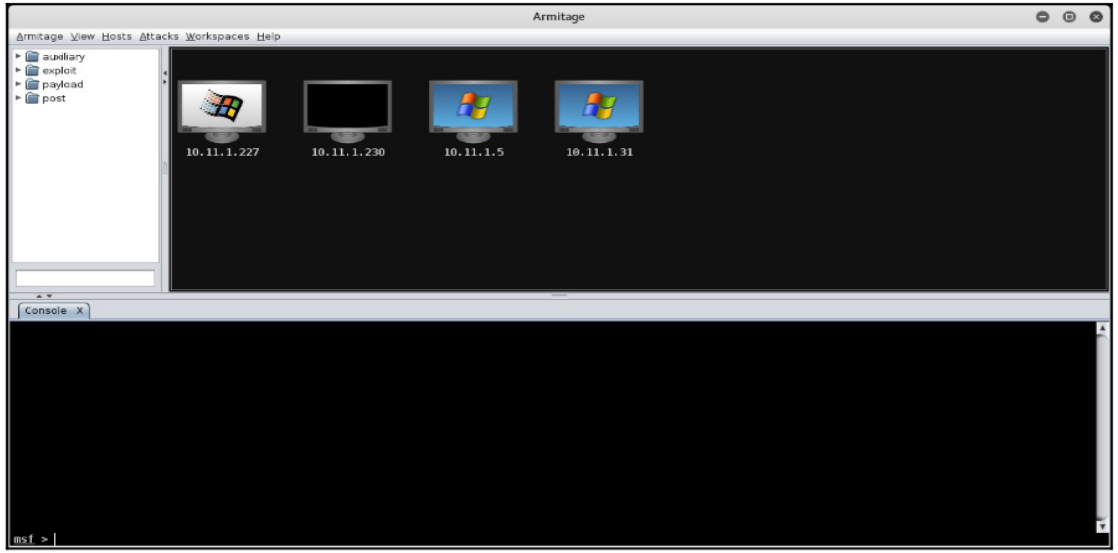
- Nessus is a product from Tenable Network Security and is one of the most popular vulnerability assessment tools. It belongs to the vulnerability scanner category.

- https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial/?utm_campaign=gs-{11596512479}-{110256808942}-{537515898716}_00026644_fy23&utm_promoter=tenable-hv-brand-00026644&utm_source=google&utm_term=nessus%20download&utm_medium=cpc&utm_geo=apac&gclid=Cj0KCQjwiZqhBhCJARIsACHHEH8tyJBdYWrHChktlOQMN7uZpIgaT4IaR97MjR5XFnuAXD3isVb1CN4aAi7iEALw_wcB



Armitage

- Armitage is an exploit automation framework that uses Metasploit at the backend. It
- belongs to the exploit automation category. It offers an easy-to-use user interface for finding
- hosts in the network, scanning, enumeration, finding vulnerabilities, and exploiting them
- using Metasploit exploits and payloads



Armitage console for exploit automation.

Information gathering and enumeration

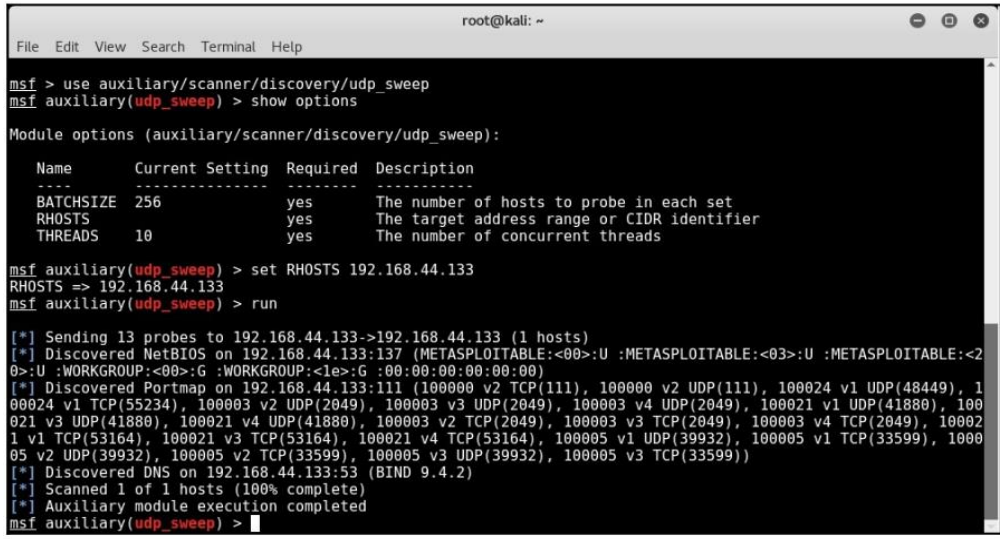
- auxiliary/scanner/portscan/tcp

  RHOSTS: IP address or IP range of the target to be scanned

  PORTS: Range of ports to be scanned

- User Datagram Protocol
  auxiliary/scanner/discovery/udp_sweep
  RHOSTS: IP address or IP range of the target to be scanned

  auxiliary/scanner/ftp/ftp_login

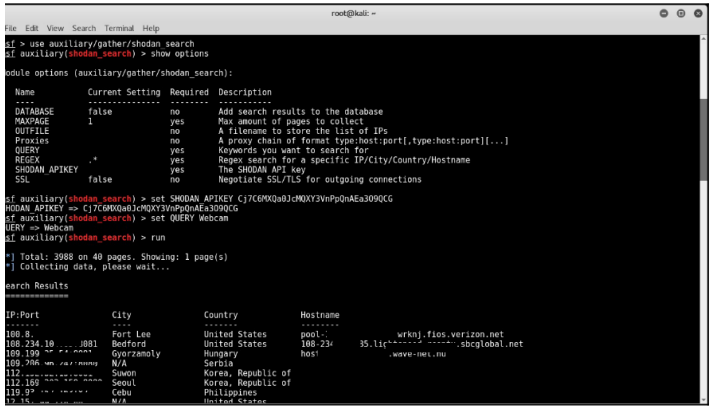


shodan

- Advanced search with shodan
- Shodan is an advanced search engine that is used to search for internet connected devices
- such as webcams and SCADA systems

Api key Setup
https://www.youtube.com/watch?v=NsyiumNlvYo

https://developer.shodan.io/api/requirements



WEB and SQL Injection

- **FINDING SQL INJECTION VULNERABILITIES**
-

scan and find the SQL injection hole in targets. Lets take a simple dork, and let SQLiv scan trough every single target and look for an ecommerce vulnerability at the following URL pattern ‘item.php?id=’. To find other patterns just google for “google dork list”.