CYBR3000

Introduction to Vulnerability Assessment

Dr Dan Kim

Associate Professor in Cybersecurity,
School of EECS
The University of Queensland, Australia
Homepage: https://researchers.uq.edu.au/researcher/23703

Learning objectives

- At the end of this lecture, you will be able to understand/explain
  - Vulnerability
  - Vulnerability assessment
  - Scanning techniques
  - Some tools
  - Scanning defences

Outline

- Red Teaming
- Vulnerability assessment
- Scanning
  - Footprinting
  - Ping scan
  - UCP/TCP Scan
- Scanning tools: Nessus, OpenVAS
- Defences

Red Teaming vs. Blue Teaming

- Red Team:
  - **A group of people** authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture.
  - Its objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.
  - Also known as Cyber Red Team.
- **Red teaming**
  - **is a proactive approach** to cybersecurity, where a group of ethical hackers simulates real-world attacks on an organization's systems to identify vulnerabilities and test its defenses. This process helps organizations improve their security posture by revealing weaknesses before malicious actors can exploit them.
  - is the **overarching** strategy or methodology.
- Red team exercise
  - An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
  - Red team exercises are **specific** events or activities conducted within the framework of red teaming.
- vs. Blue team:
  - The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team).

- Red Team: https://csrc.nist.gov/glossary/term/red_team
- Red teaming: https://www.schellman.com/blog/cybersecurity/what-is-red-teaming

VAPT vs. Red Teaming

- Vulnerability Assessment and Penetration Testing (VAPT)
  - is a more focused approach that aims to identify and address specific vulnerabilities in an organization's IT infrastructure.
  - The process typically involves a combination of vulnerability scans, penetration testing, and manual testing to identify vulnerabilities, assess their impact, and provide recommendations for remediation.
- Red Teaming
  - Red Teaming takes a broader approach that simulates a real-world attack and tests an organization's people, processes, and technology.
  - The goal of a Red Team engagement is to identify weaknesses in an organization’s security posture that may be missed by traditional security assessments.

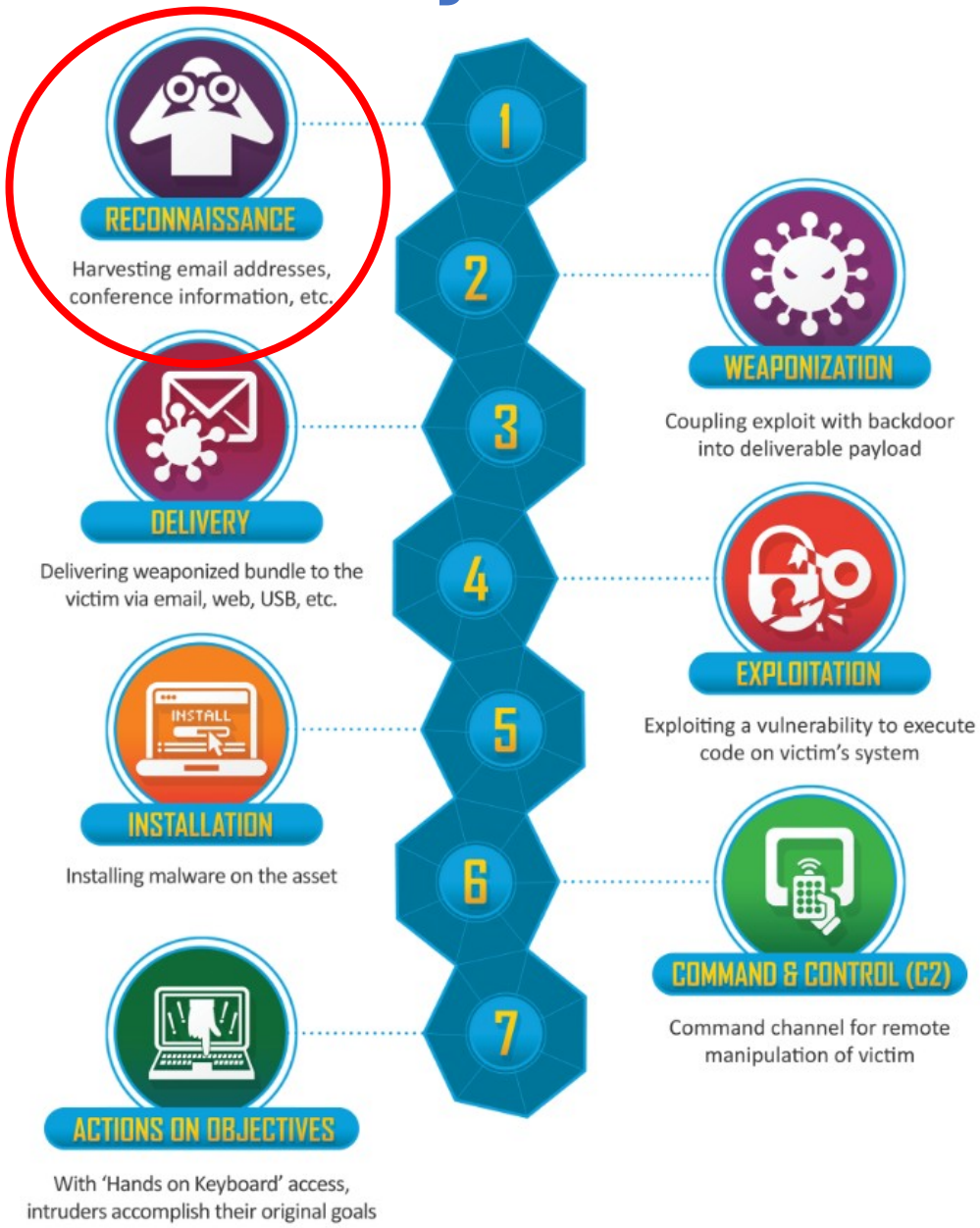
https://westadvancedtechnologies.medium.com/vapt-vs-red-teaming-which-is-right-for-your-organization-af9f078c3eca#:~:text=VAPT%20is%20a%20more%20focused,people%2C%20processes%2C%20and%20technology.

Types of Security Assessments

- Vulnerability Assessment (Scanning)
  - **Finds vulnerabilities.**
  - is an automated process that searches for **known** vulnerabilities in your network and systems.
  - scans host/network, using software, and identifies any known vulnerabilities, such as missing patches or misconfigured systems.
  - The goal is to identify vulnerabilities that need to be patched or otherwise addressed.
- Penetration Testing (aka Pen Testing)
  - **Exploits vulnerabilities.**
  - digs deeper into the broad amount of vulnerabilities provided by a vulnerability assessment, demonstrating the true impact of a compromise should the vulnerabilities remain open.
- IT security auditing (information security auditing)
  - often involves interviews and reviewing available documents
  - Focuses on policies and procedures
  - Identification of risks and weaknesses
  - Assurance of compliance with requirements

- Source 1: https://insights.integrity360.com/the-penetration-testing-red-teaming-vulnerability-assessments-debate-which-one-is-right-for-your-business
- Source2: https://versprite.com/blog/vulnerability-assessment-vs-penetration-testing-vs-red-teaming/

The Cyber Kill Chain (CKC) framework



- Developed by Lockheed Martin
- is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity.
- identifies what the adversaries must complete to achieve their objective.
- The seven steps enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

The MITRE’s ATT&CK framework

- The Adversarial Tactics Techniques and Common Knowledge
- Tactics
  - PRE-ATT&CK, Enterprise, Mobile, ICS
  - **Reconnaissance**, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Later Movement, Collection, Command & Control, Exfiltration, Impact
- Techniques with target systems
  - PRE-ATT&CK, Enterprise (Windows, macOS, Linux, Cloud, Network, Containers), Mobile (Android, iOS), and ICS
  - include Possible methods of detection and mitigation for each techniques
- Mitigations
  - Enterprise, Mobile, ICS

https://attack.mitre.org/tactics/enterprise/

The MITRE’s ATT&CK framework (cont.)

- Reconnaissance?
  - The adversary is trying to gather information they can use to plan future operations.
  - consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting.
  - Such information may include details of the victim organization, infrastructure, or staff/personnel.

Scanning == Footprinting

- is the technique of gathering information about computer systems and the entities they belong to
- one of the pre-attack phases; tasks performed prior to doing the actual attack

Identifying services and operating systems type and narrows our scope of vulnerability identification

Vulnerability Scanners

- IP/Port Scanners
  - nmap
- Vulnerability Scanners
  - Nessus
  - OpenVAS
- Nslookup
  - querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record
- Many are available, so many that you will most likely never use all of them

Q: principle of scan?

Scan classification

- Ping
  - a computer network tool used to test whether a particular host is reachable across an IP network

1) Ping (Internet Control Message Protocol (ICMP)) scan
   - Server scan

2) TCP and UDP scans
   - Port scan

Ping demo?

Ping

- uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway.
- man ping

NAME

ping - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS

ping [-aAbBdCDfhHLnOqrRUvV46] [-c count] [-e identifier]
[-F flowlabel] [-i interval] [-I interface] [-l preload]
[-m mark] [-M pmtudisc_option] [-N nodeinfo_option]
[-w deadline] [-W timeout] [-p pattern] [-Q tos]
[-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp option]
[hop...] {destination}

Ping: an example

```
$ ping -c 3 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=2.23
ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64
time=0.028 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64
time=0.028 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time
2032ms
```

OS detection

- Passive vs. Active detection
- Passive tools – examples
  - Ettercap: Man in The Middle Network Security Tool
    - ✓ Man-in-the-middle attacks; DNS spoofing; Credentials capture; DoS attack
  - p0f: Scalable Passive OS Fingerprinter Tool
    - ✓ uses a fingerprinting technique based on analyzing the structure of a TCP/IP packet to determine the operating system and other configuration properties of a remote host.
  - PacketFence: Passive OS Fingerprinting Tool
- Active tools - examples
  - **Nmap**

Source 1: https://www.ubuntupit.com/best-open-source-passive-os-fingerprinting-tools/

Scan – TCP/UDP scans

- Ping
  - a computer network tool used to test whether a particular host is reachable across an IP network
- 1) Ping and ICMP (Internet Protocol Messaging Protocol) scan
  - Server scan

- 2) TCP and UDP scans
  - Port scan

TCP and UDP scan – nmap options (examples)

- UDP scan*: -sU
  - *Requires root privileges.

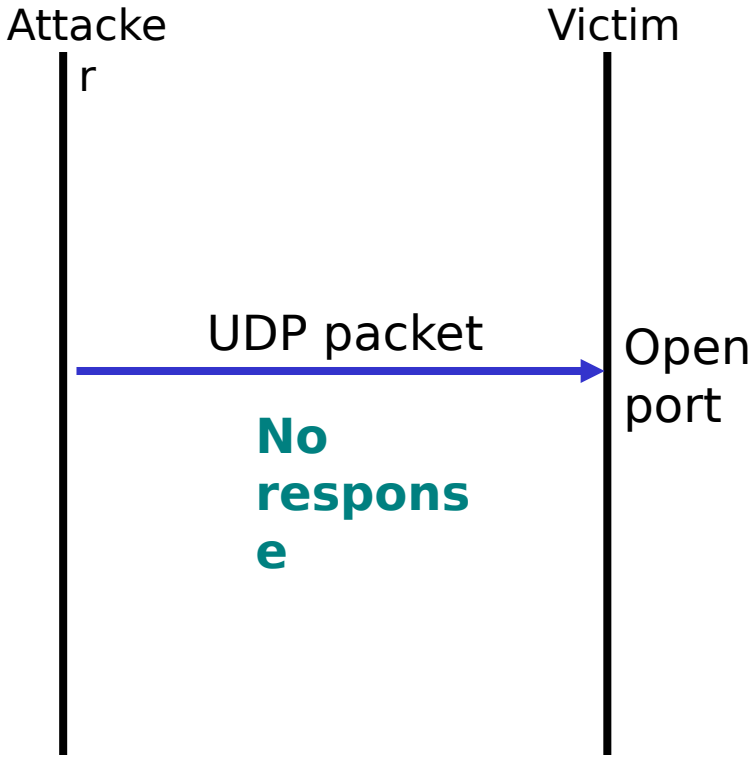
- TCP scan:
  - TCP open scan: -sT (TCP connect scan)
  - Stealth scans*
    - ✓TCP half open: -sS (TCP SYN scan)
    - ✓NULL, FIN, XMAS: -sN; -sF; -sX

https://nmap.org/book/man-port-scanning-techniques.html

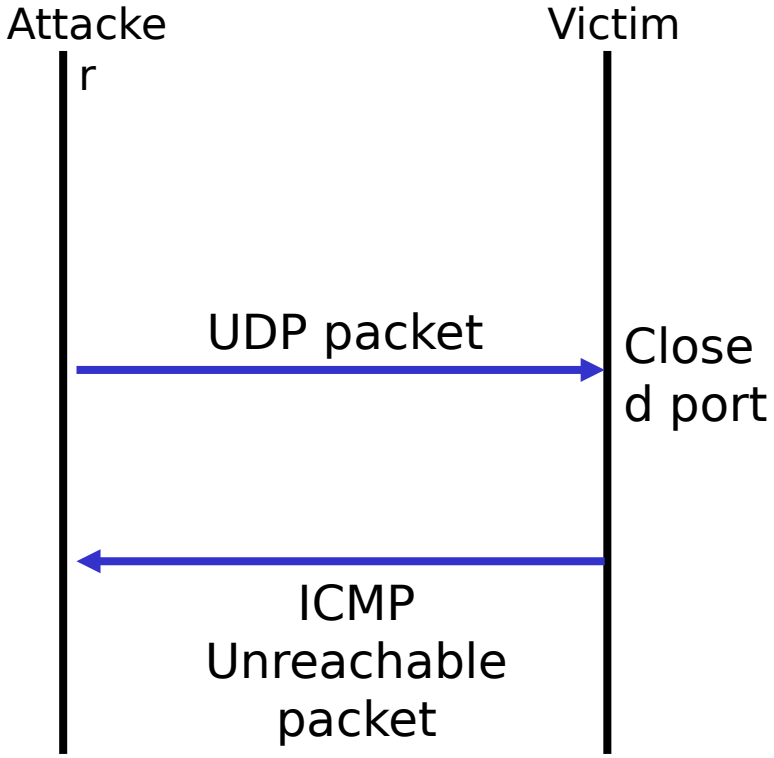
UDP: user datagram protocol
TCP: transmission control protocol

UDP scan

- Port is open



- Port is closed



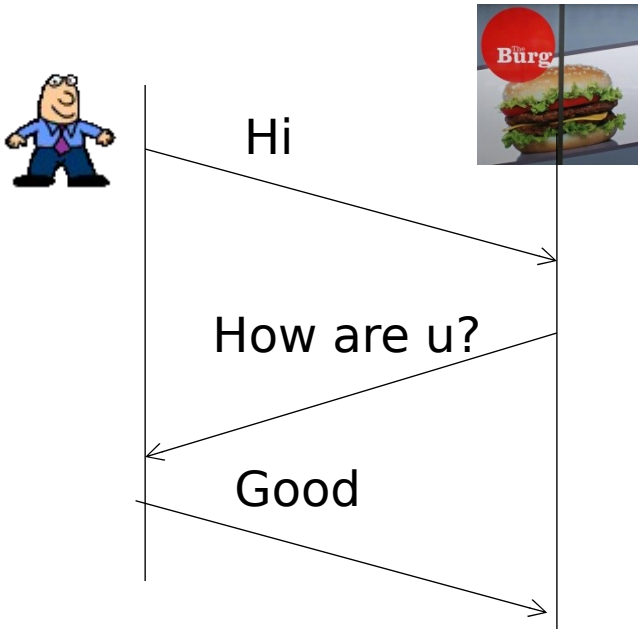
Response for UDP scan

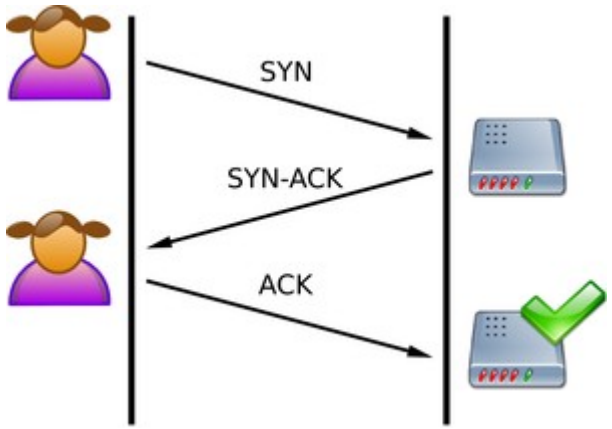
Probe Response	Assigned State
Any UDP response from target port (unusual)	open
No response received (even after retransmissions)	open|filtered
ICMP port unreachable error (type 3, code 3)	closed
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	filtered

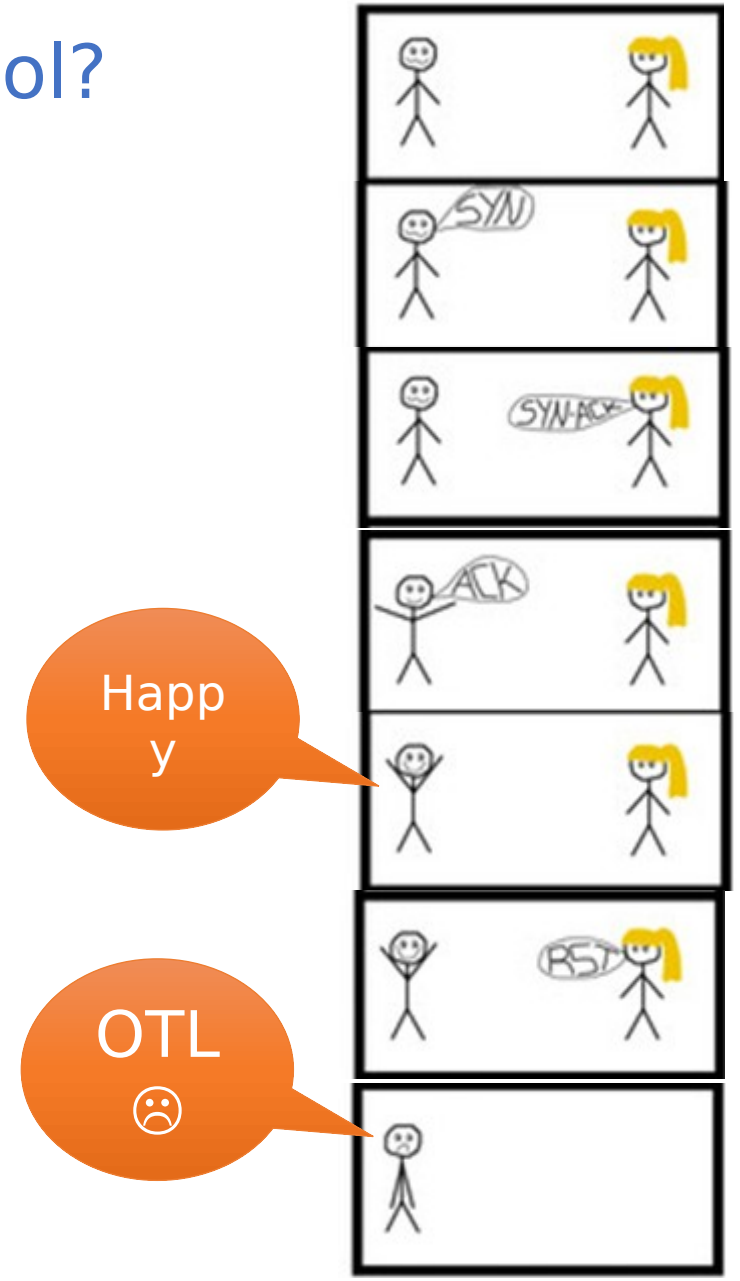
Q: Is this reliable?

A: No, UDP packets can be lost during transmission by routers and/or firewall.

Transmission Control Protocol?







Love can be unreliable even when you use TCP

http://portadiferro.blogspot.co.nz/2011/04/tcp-split-handshake-issue.html

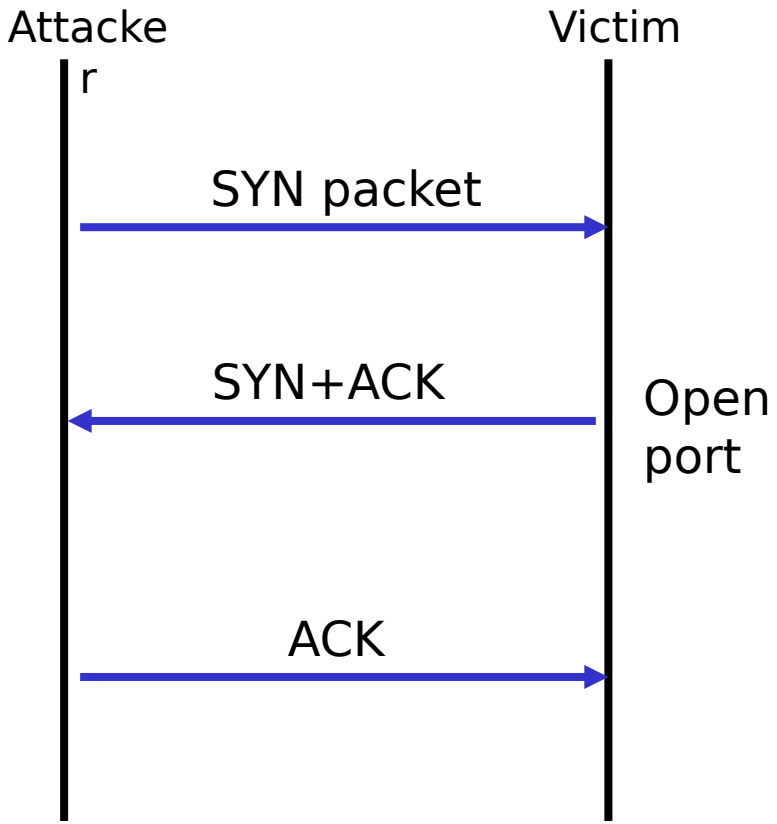
Well-known ports used by TCP

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

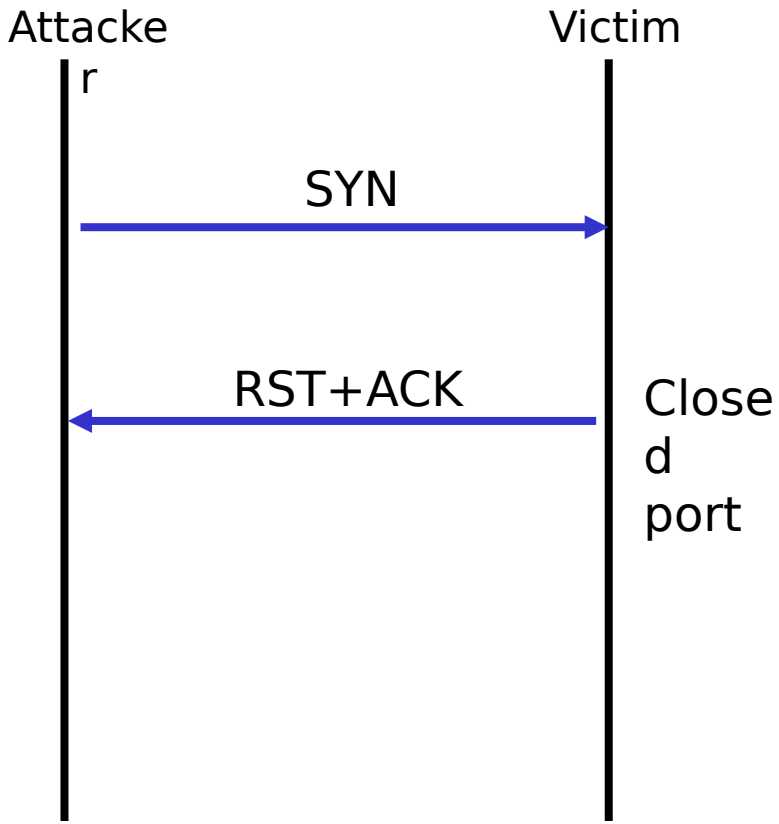
TCP open scan

(aka, TCP *connect* scan)

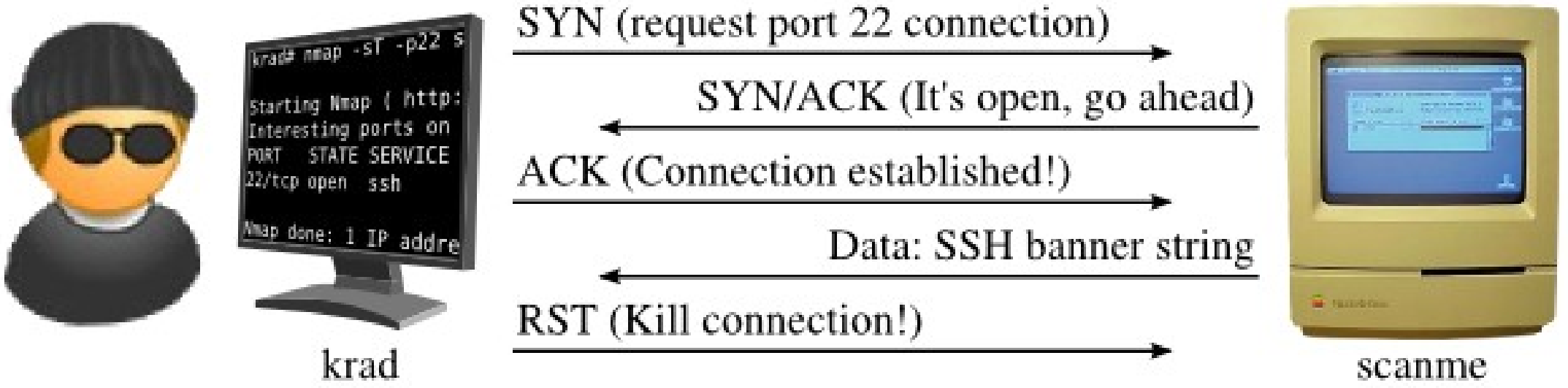
- Port is open



- Port is closed



TCP open scan example



TCP open scan (cont.)

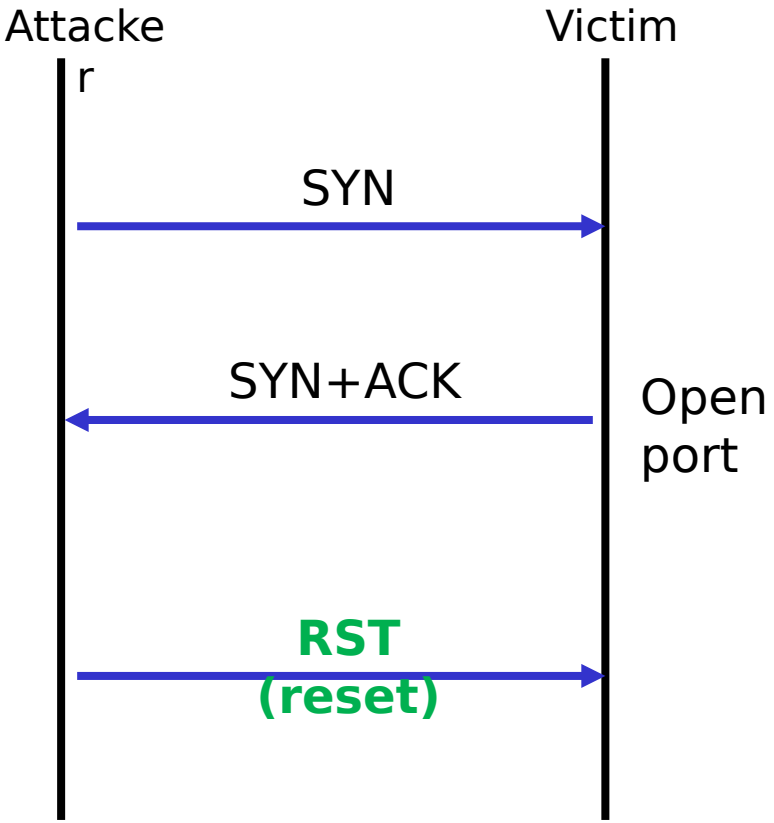
- Use `connect()` system call on each port, following normal TCP connection protocol (3-way handshake).
- `connect()` will succeed if port is listening.

- Advantages: fast, requires no privileges
- Disadvantages: easily detectable and blockable.

Stealth scan: TCP half open scan

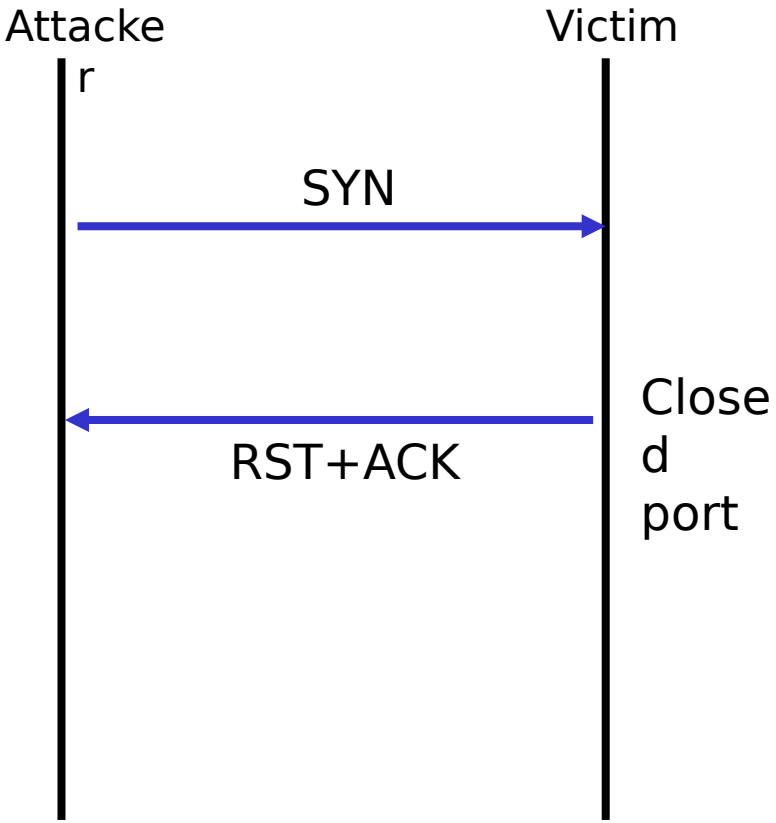
(aka, TCP *SYN* Scan), default and most popular

- Port is open



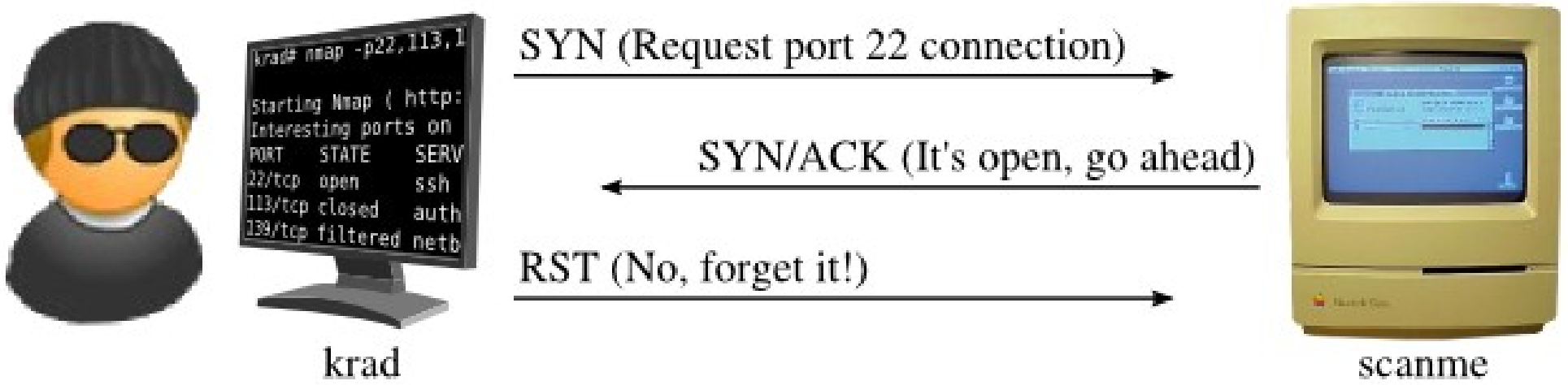
Q: Difference compared to TCP open scan ?

- Port is closed



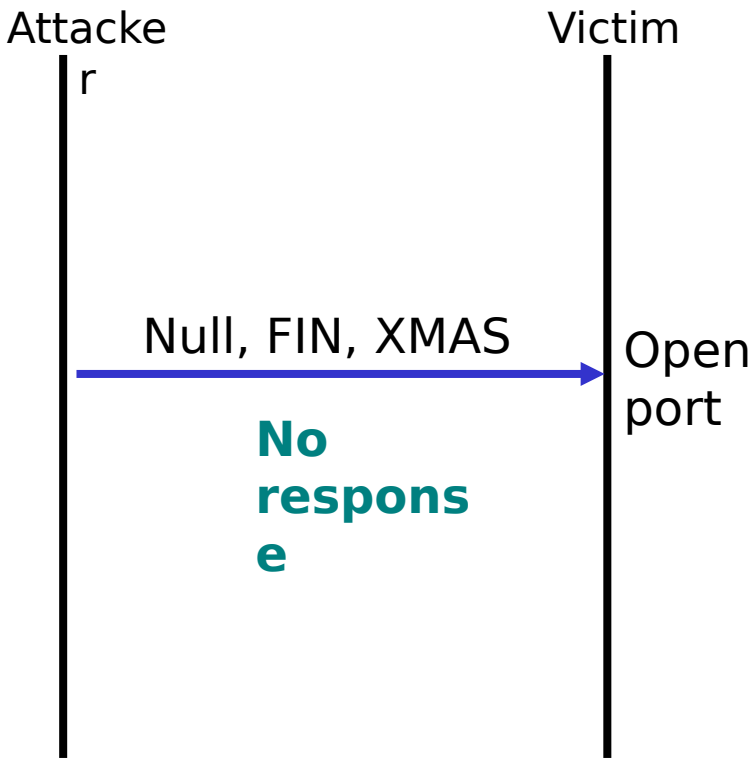
A: No session log but requires root privilege

TCP stealth scan example

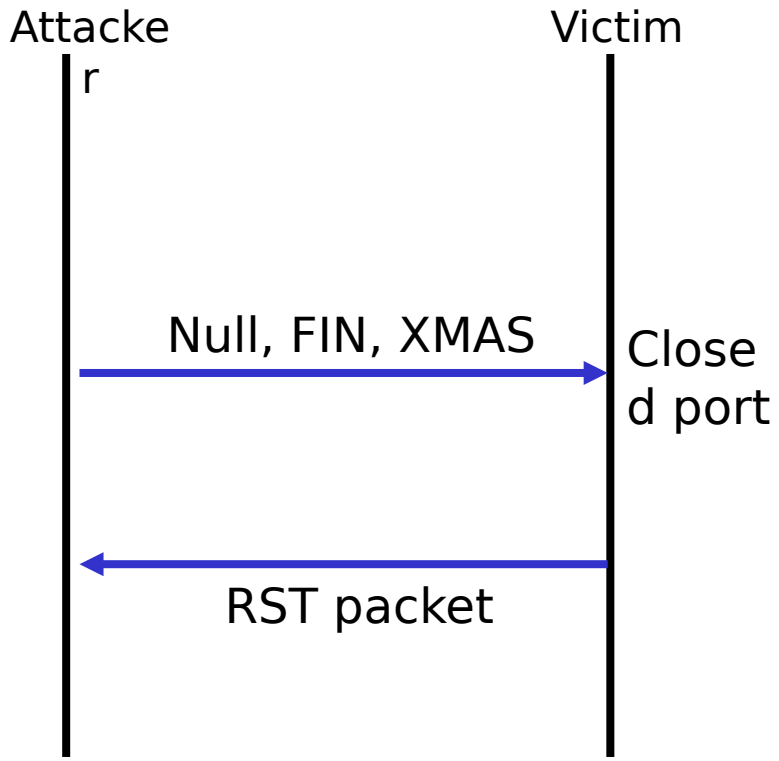


Stealth scan: Null, FIN, XMAS scan

- Port is open



- Port is closed



Stealth scan: Null, XMAS scan

- Null Scan: Turns off all TCP flags: Does not set any bits (TCP flag header is 0)
- FIN scan: Sets just the TCP FIN bit.
- Xmas Scan: Sets the FIN, PSH, and URG flags, lighting the packet up like a

The **URG flag** is used to indicate that the packet contains information that is of higher priority than other data within the stream

Responses

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

- If an RST packet is received, the port is considered closed, while no response means it is open|filtered.
- The port is marked filtered if an ICMP unreachable error (type 3, code 0, 1, 2, 3, 9, 10, or 13) is received.

Fragmentation Scan

- Modify TCP stealth scan (SYN, FIN, Xmas, NULL) to use tiny fragmented IP datagrams.
  - sudo nmap –f <target>
  - sudo nmap --mtu 160 <target>

- Advantages: increases difficulty of scan detection and blocking.

- Disadvantages: does not work on all OSes and may crash some firewalls/sniffers.

Nmap scan - demo

Nmap scan

- for a privledged user, the default option is the -sS scan (TCP SYN scan)

- for an unpriledged user, the default option is the -sT scan (TCP connect() scan)

Nmap scan

- Single IP scan
  - nmap 192.168.1.1
- Host(s) scan
  - nmap www.testnetwork.com
  - nmap www.google.com
- Multiple IPes scan
  - nmap 192.168.1.1-20
- Subnet scan
  - nmap 192.168.1.0/25

Nmap scan (cont.)

- OS scan
  - nmap 10.1.0.2 **– A**
  - Takes longer time

- Save the scanning result
  - nmap –sV 192.16.1.1 –oX nmapresult.xml

Nmap UDP scan

- **Use nmap with Tuning Options:**
  - nmap -sU -p <port_range> --max-retries 2 --max-scan-delay 20ms <target>

- Examples
  - sudo nmap -sU -p 80 --max-scan-delay 10ms 10.0.2.4
  - sudo nmap -sU -p 80-100 --max-scan-delay 300ms 10.0.2.4

Nmap TCP scan

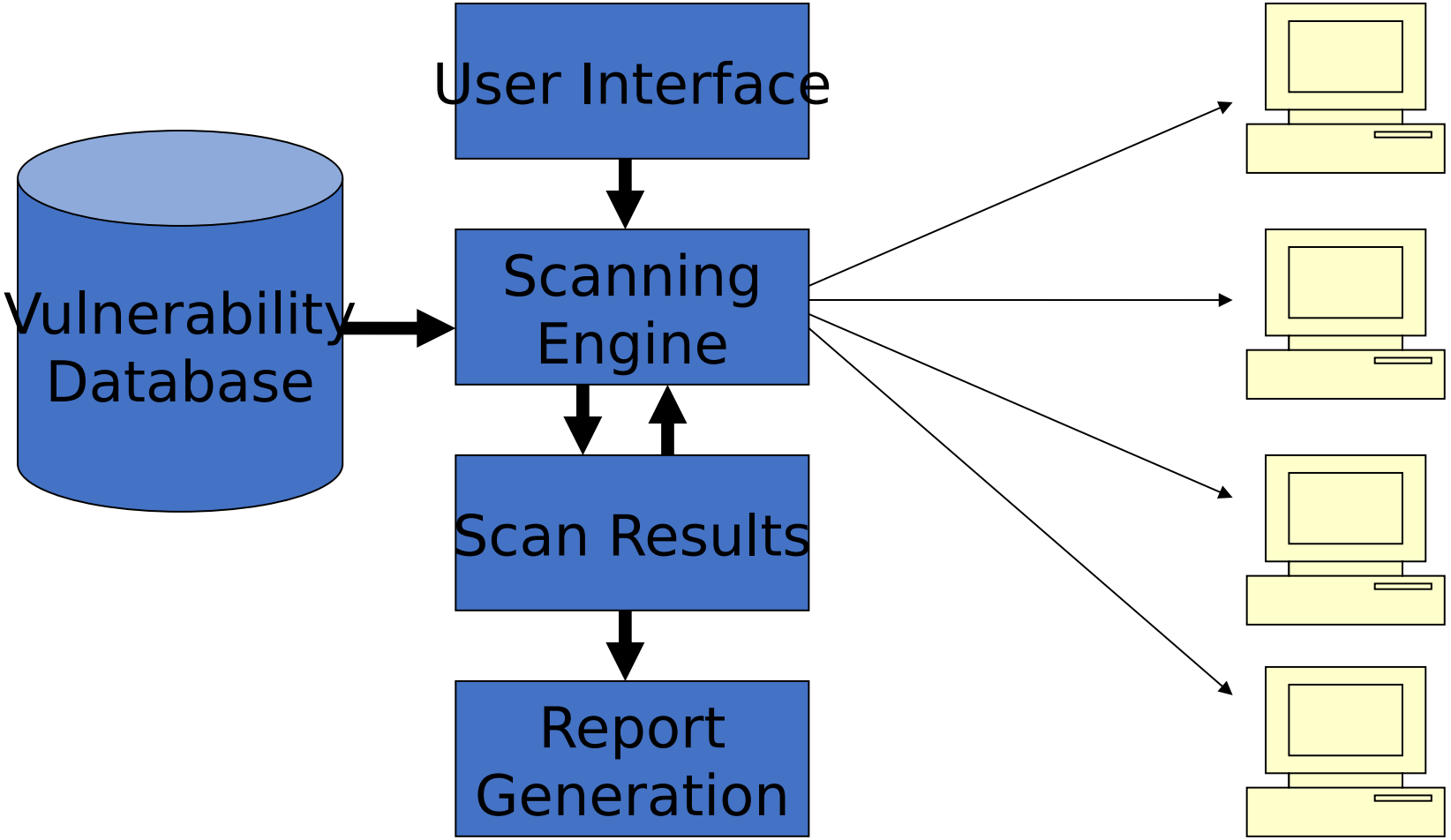
- nmap -sT 10.0.2.4

Nmap other scans

- Stealth scans*
  - TCP half open: -sS (TCP SYN scan)
  - NULL, FIN, XMAS: -sN; -sF; -sX

- Fragmentation scans
  - sudo nmap –f <target>
  - sudo nmap --mtu 160 <target>
    - ✓Sets the packet MTU size to 160 bytes
  - e.g.: sudo nmap -p 80 --mtu 1000 10.0.2.4
  - e.g.: sudo nmap –sS –mtu 160 –p80 10.0.2.4

Vulnerability Scanner Architecture (example)



Vulnerability scanners

- are a tool that network administrators use to scan networks for vulnerabilities.
- can highlight known vulnerabilities and misconfigurations that leave a network at risk of a cyberattack or a data breach
- Many commercial tools available, some examples are
  - Tenable Nessus
  - IBM Security QRadar
  - OpenVAS

https://www.comparitech.com/net-admin/nessus-vs-openvas/

https://www.enterprisestorageforum.com/security/openvas-vs-nessus/#:~:text=Nessus%3A%20Best%20for%20businesses%20seeking,more%20than%2050%2C000%20vulnerability%20tests.

Scanning with Nessus

- Runs on Linux, Unix and Windows
- Nessus doesn’t use large Database of vulnerabilities that gets updated
- It uses **Nessus Attack Scripting Language (NASL)**
  - Allows people to write their own scripts, plug-ins
- It provides plug-in interface; many free plug-ins are available from
- What vulnerabilities can it discover?
  - software flaws, missing patches, malware, denial-of-service vulnerabilities, default passwords and misconfiguration errors, among other potential flaws
- Nessus for education
  - https://www.tenable.com/tenable-for-education/nessus-essentials

Scanning with Nessus (cont.)

- Each vulnerability is ranked with respect to risk
  - Low, medium and high
  - Should interpret the risk results only in view of your own system
  - Same vulnerability may not be high risk for you
- Recommendations are made for fixing vulnerability

OpenVAS

- Open Vulnerability Assessment System (OpenVAS)
- OpenVAS was originally proposed by pentesters at Portcullis Computer Security around 2005
- OpenVAS is actively being developed and supported
- The Greenbone Enterprise TRIAL
  - https://www.greenbone.net/en/testnow/

Vul. Scanner - demo

Kali Linux commands

- Display list of installed packages
  - dpkg –l
  - dpkg –l | grep z*
- Tar
- ifconfig
  - Ifconfg eth0 down
  - Ifconfig eth0 up
  - Ifconfig
- dhclient

Nessus installation

- Dowload Nessus
  - https://www.tenable.com/downloads/nessus?loginAttempted=true
- Install package
  - sudo dpkg –I Nessus ….
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner

Nessus Attack Scripting Language (NASL)

- Designed specifically for security testing, making it easy to write scripts that check for vulnerabilities, misconfigurations, and compliance issues.
- Used for both Nessus and OpenVAS
- Detecting an Open Telnet Port

```
if ( get_port_state(23) ) {
    security_warning(port:23, proto:"tcp", "Telnet service is running on this
port.");
}
```

- These scripts are illustrative and simplified. Actual NASL scripts may need more specific details based on the vulnerability's behavior.

Nessus Attack Scripting Language (NASL)

- NASL script example that checks for an open HTTP port

```
include("http_func.inc");

port =
get_http_port(default:80);

if (get_port_state(port)) {
    security_warning(port:port,
proto:"tcp", "HTTP port is
open.");
}
```

- Detecting SMBv1 Protocol (CVE-2017-0144)

```
include("smb_func.inc");

port = 445;
if (!get_port_state(port))
    exit(0);

# Check for SMBv1
if (smb1_is_enabled()) {
    security_warning(port:port, proto:"tcp",
        "SMBv1 is enabled. This protocol is
vulnerable to several attacks, including
WannaCry.");
}
```

Common Weakness Enumeration (CWE)

- is a formal list or dictionary of common software and hardware weaknesses that can occur in architecture, design, code, or implementation that can lead to exploitable security vulnerabilities.
- A “weakness” is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities.
- Weaknesses examples
  - Software — buffer overflows, format strings, etc.; structure and validity problems…
- The difference between a weakness and a vulnerability?
  - Weaknesses are errors that can lead to vulnerabilities.
- The main goal of the CWE initiative is to stop vulnerabilities at the source by educating software and hardware acquirers, architects, designers, and programmers on how to eliminate the most common mistakes before a product is delivered.

https://cwe.mitre.org/about/faq.html#what_is_cwe_weakness_meaning

Common Vulnerabilities and Exposures (CVE)

- A list of standardized names for vulnerabilities and other information security exposures (CVE)
  - CVE standardizes names for all publicly known vulnerabilities and security exposures and is a community wide effort
  - Content of CVE is collaborative effort of CVE Editorial Board
    - ✓ Includes representatives from over 20 security-related organizations
      - Security tool vendors, academic institutions, and government
  - MITRE Corporation maintains CVE and moderates Editorial Board discussions.
  - http://cve.mitre.org

National Vulnerability Database (NVD)

- NVD, comprehensive cyber security vulnerability database
- Integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources
- Based on and synchronized with the CVE vulnerability naming standard
  - NVD is **a superset of CVE**
  - NVD is **the CVE standard augmented with** additional analysis, a database, and a fine grained search engine.
  - NVD is synchronized with CVE such that any updates to CVE appear immediately on NVD
- Web

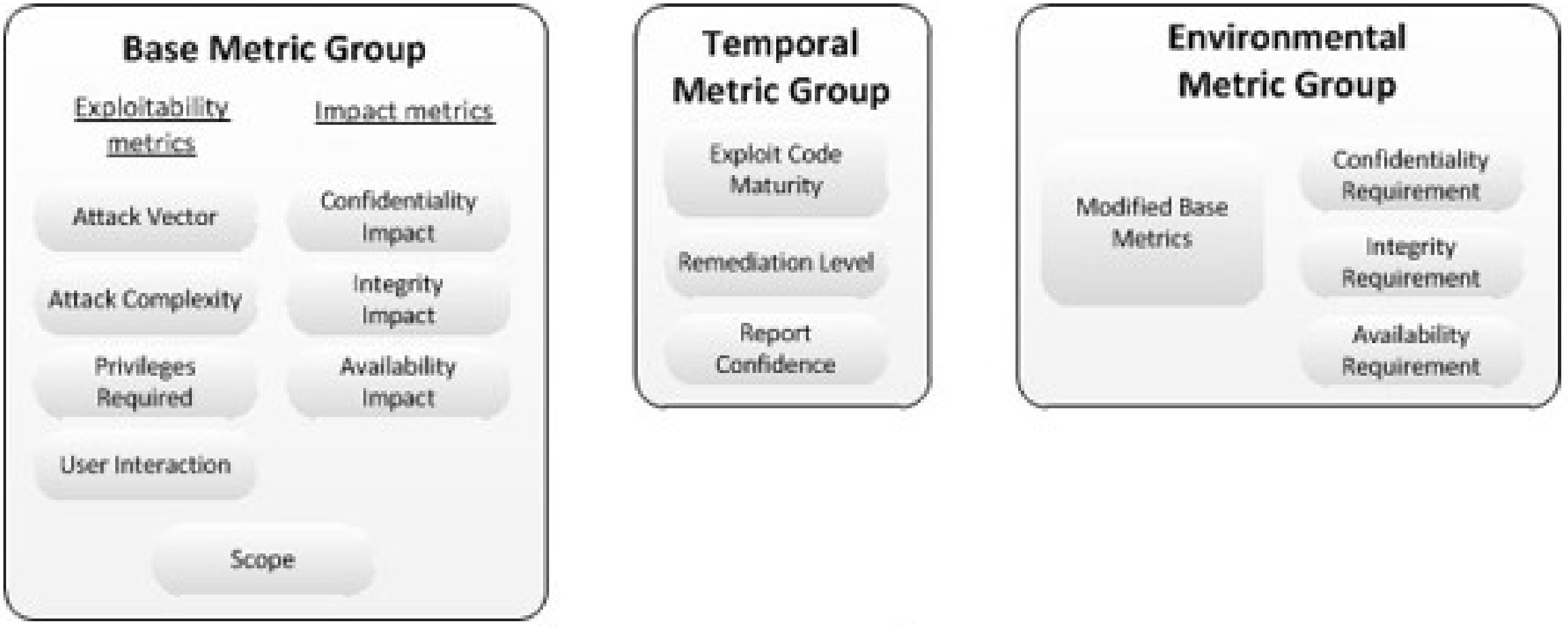
CVE vs. NVD

- The CVE list feeds into the NVD, so both are synchronized at all times.
- The NVD provides enhanced information above and beyond what's in the CVE list, including patch availability and severity scores.
- NVD also provides an easier mechanism to search on a wide range of variables.
- Both CVE and NVD are sponsored by the US Federal Government and are available for free use by anyone.

The Common Vulnerability Scoring System (CVSS)

- provides an open framework for communicating the characteristics and impacts of IT vulnerabilities
- NVD Vulnerability Severity Ratings (examples)
  - Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
  - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
  - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.
- Examples
  - CVE-2020-16894: A remote code execution vulnerability exists when Windows Network Address Translation (NAT) fails to properly handle UDP traffic, aka 'Windows NAT Remote Code Execution Vulnerability’.
  - CVE-2021-26879: Windows NAT Denial of Service Vulnerability

CVSS v3.0 Metric Groups



Fingerprinting Defences

- Software patch management
- Detection
  - NIDS (Network Intrusion Detection System)/NIPS
- Blocking
  - Firewalls
  - Some probes can’t be blocked.
- Deception
  - IP personality changes TCP/IP stack signature to that of another OS in nmap db.
  - Fake nodes/networks
- Moving Target Defence (MTD)
- …