Network Reconnaissance Attacks

COMP 4670 - Network Security

Lesson 03

Outlines

- Reconnaissance Attacks
- Network Services Reconnaissance
- Vulnerability Identification
- Vulnerability Verification

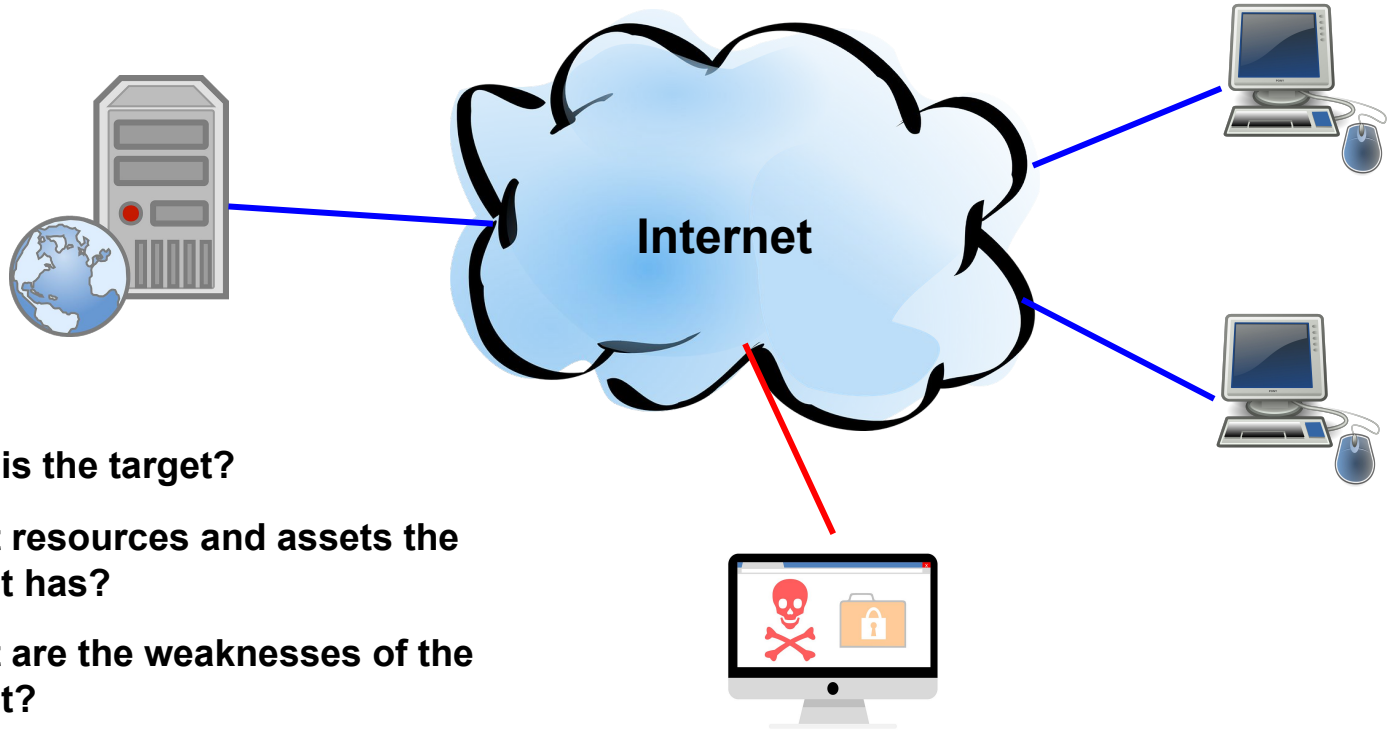
Network Attacks

Network attacks range from a simple, naive attack executed by script kiddie to a complex multistage attack executed by an elite hacker.

What is a Script Kiddie?

Someone who use existing scripts or tools to hack into computers system while lacking the expertise to write his own. In addition, a script kiddie does not understand how the script work.

Reconnaissance Attack



1. **Who is the target?**
2. **What resources and assets the target has?**
3. **What are the weaknesses of the target?**

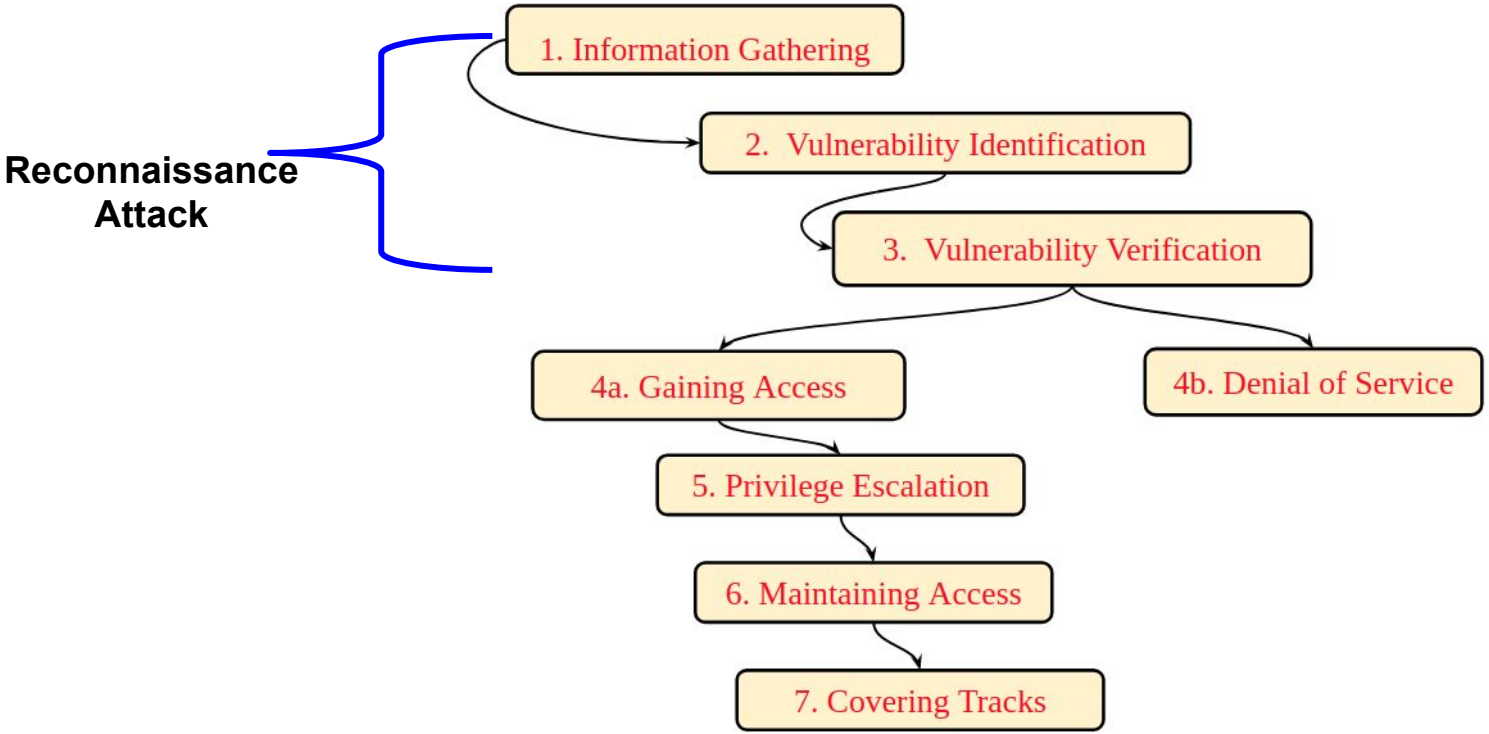
Reconnaissance Attack

- It is the first step in any computer-network attack seeking to exploit a target system.
- Reconnaissance is a type of computer attack where the attacker tries to find out information about the vulnerable points of the target network.
- The term reconnaissance is borrowed from its military use, where it refers to a mission into enemy territory to gather intelligence

Stages of a Reconnaissance Attack

- In general, reconnaissance attack consists of three stages, namely,
  - Information Gathering
  - Vulnerability Identification
  - Vulnerability Verification (Partially)
- Stages of the reconnaissance attack include both be **passive** or **active**.

Network Attack Anatomy



Information Gathering Attacks

- Unauthorized data collection process to learn about the resources and assets of the target system.
- The objective of the information gathering stage is to collect as much data as possible about the target.
- The target system resources and assets are not limited to computer systems. Target network employees, customers, and suppliers are usually part of the information gathering process.
- Information Gathering could be **passive** or **active** process.

Information Gathering Attacks

Passive Information Gathering

1. Collect Publicly Available Information
2. Analyze collected data to discover, host IPs, email addresses, employee roles, etc
3. Determining the network range

Active Information Gathering

1. Identifying active machines
2. Finding open ports and access points
3. OS Fingerprinting
4. Services Fingerprinting
5. Mapping the network

Passive Information Gathering

- Collect information without direct contact with the target.
- Focuses on searching for information directly or indirectly related to target network
- Possible searches include:
  - **Employee information**, physical location, business activity
  - **Target web presence:** Website address(es), web server type, server locations etc.
  - **Web groups** containing company/employees comments
  - **Domain/company information** available by querying domain registrar

Passive Information Gathering

- Sources for Passive Information Gathering
  - Internet Service Registration
  - Domain Name System
  - Search Engines
  - Email Systems
  - Naming Conventions
  - Website Analysis
  - Social Networks
- Tools for Passive Information Gathering.
  - E.g. WHOIS? - Web Crawler - Harvesters

Passive Information Gathering

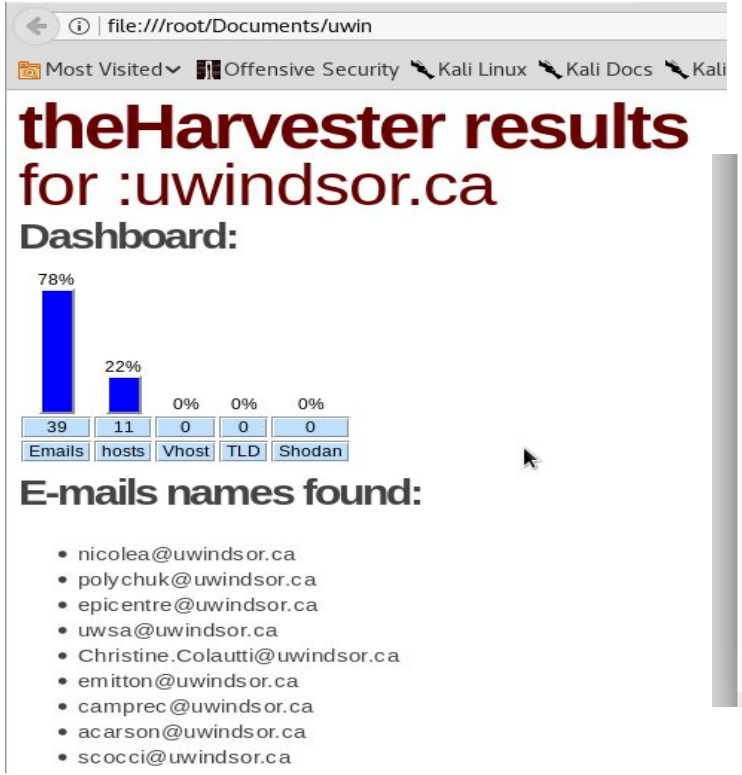
- Let us try to see what could we learn about uwindsor.ca using passive information gathering.

theharvester -d uwindsor.ca -l 500 -b google -f /root/Documents/uwin

```
root@CS60467:~#
root@CS60467:~# theharvester -d uwindsor.ca -l 500 -b google -f /root/Documents/uwin_google
```

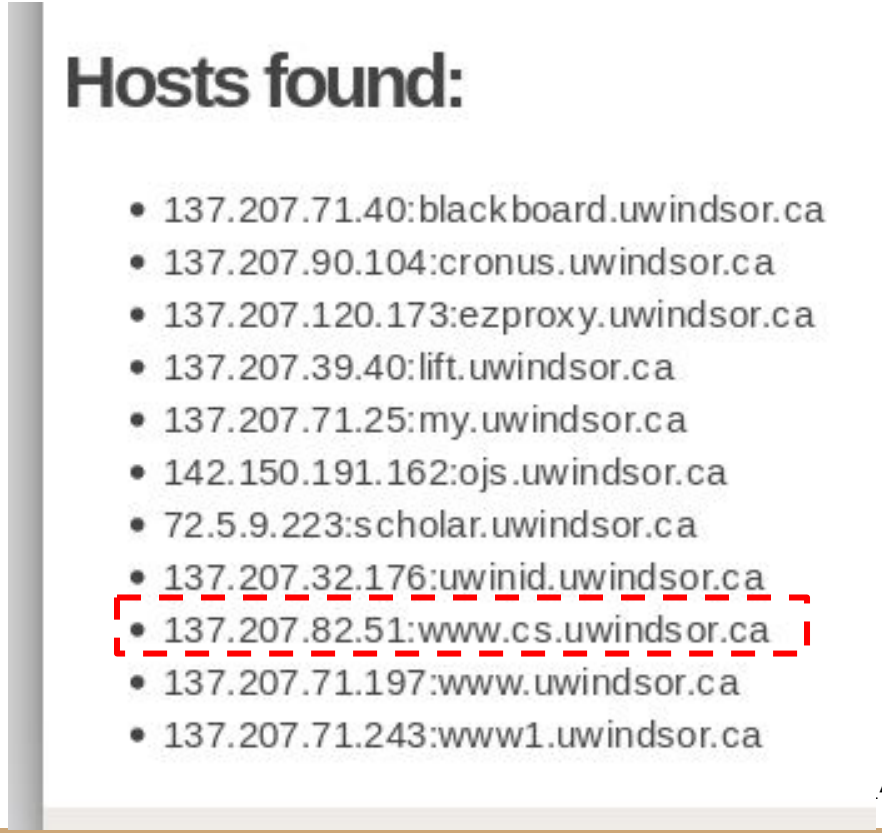
https://tools.kali.org/information-gathering/theharvester

Passive Information Gathering



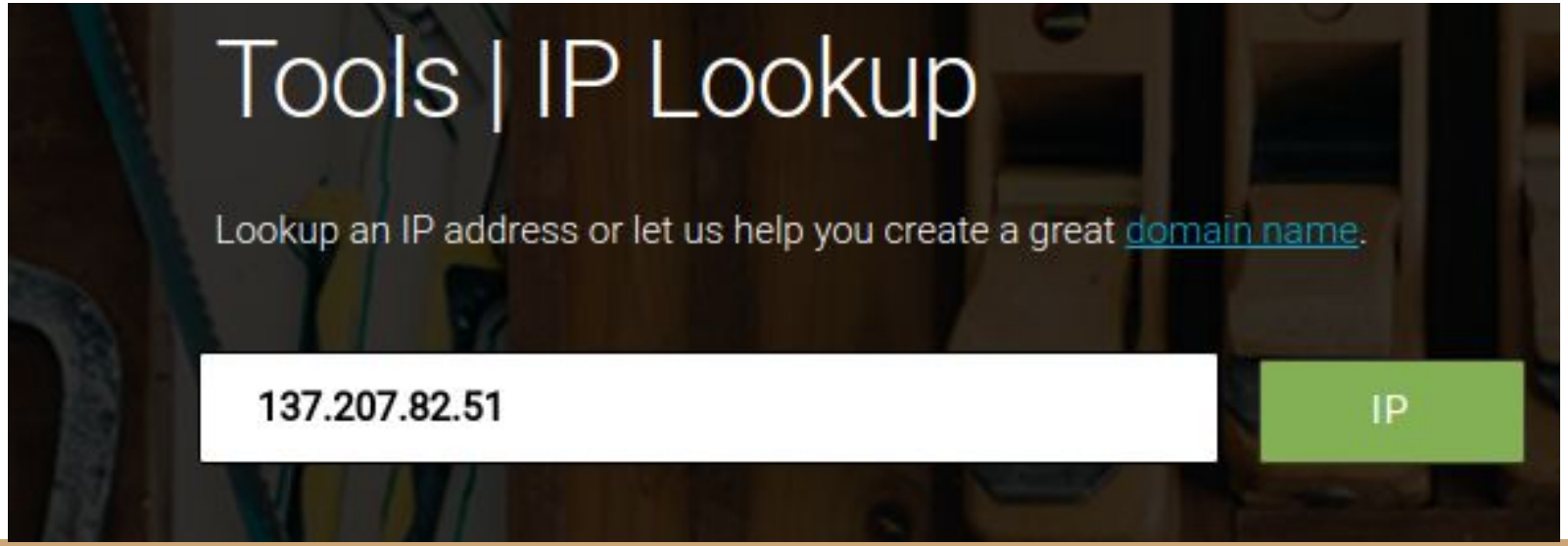
Passive Information Gathering

- Let see how we can find the network range by query.
- Let us take one IP address of a host discovered earlier and enter it into the **Whois** lookup at **www.arin.net**



Passive Information Gathering

https://www.whois.com.au/whois/ip.html



Passive Information Gathering

```
NetRange:       137.207.0.0 - 137.207.255.255
CIDR:           137.207.0.0/16
NetName:        UWINDSORNET
NetHandle:      NET-137-207-0-0-1
Parent:         NET137 (NET-137-0-0-0-0)
NetType:        Direct Assignment
```

- This means that the target network has **65534** total addresses. The attacker can now focus his efforts on the range:

  from 137.207.0.1 to 137.207.255.254

Active Information Gathering

Usually the next step after passive information gathering.

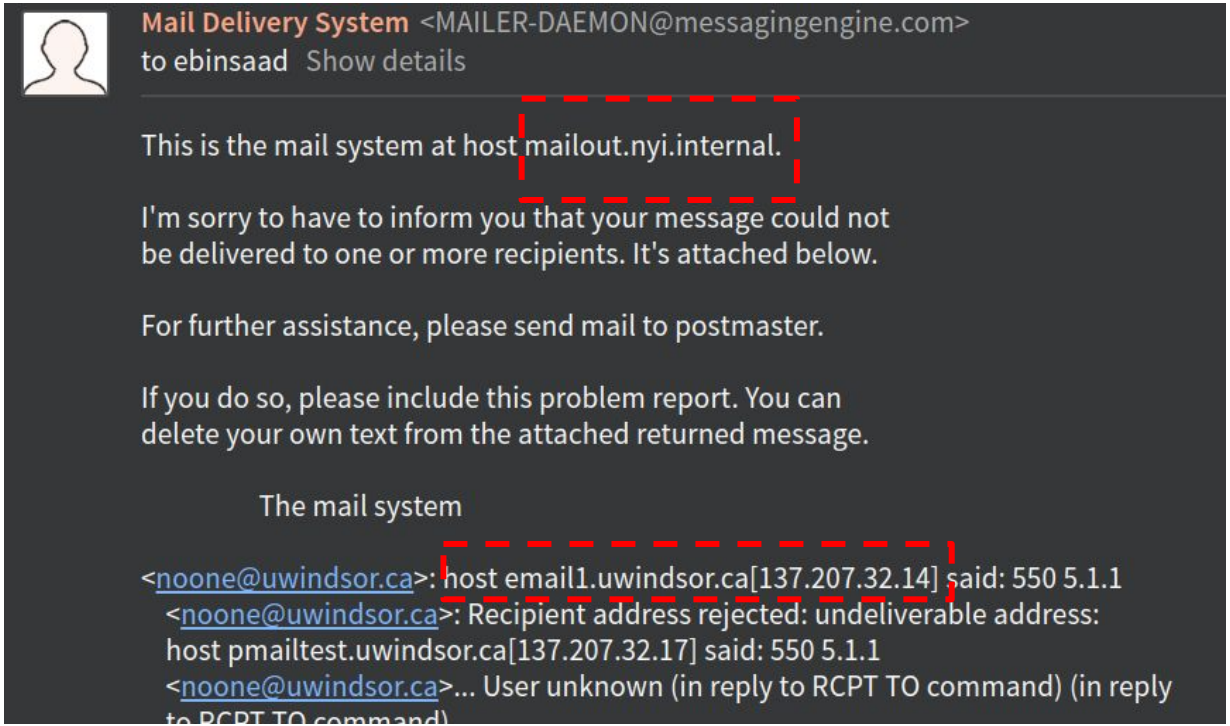
The attacker connects directly to the target based on the information he/she gathered during the passive stage.

At this point, the attacker wants to learn more about the target.

Active Information Gathering

- Let us find the IP address and host name of the mail server @ uwindsor.ca
- Simply send an email to any bad address @uwindsor.ca to trigger the mail server at uwindosr to send a bounce message

Active Information Gathering



Mail Delivery System <MAILER-DAEMON@messagingengine.com>
to ebinsaad Show details

This is the mail system at host mailout.nyi.internal.

I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can delete your own text from the attached returned message.

The mail system

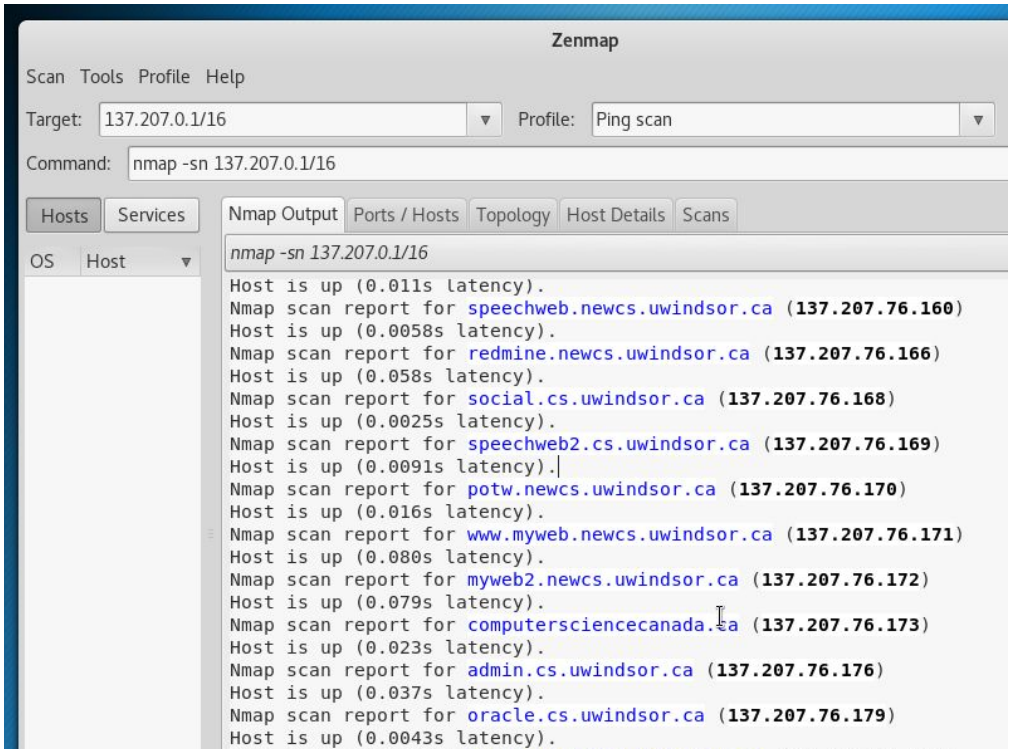
<noone@uwindsor.ca>: host email1.uwindsor.ca[137.207.32.14] said: 550 5.1.1 <noone@uwindsor.ca>: Recipient address rejected: undeliverable address: host pmailtest.uwindsor.ca[137.207.32.17] said: 550 5.1.1 <noone@uwindsor.ca>... User unknown (in reply to RCPT TO command) (in reply to RCPT TO command)

Discover Active Hosts

- Different ICMP scanning and TCP|UDP scanning methods could be used to discover active hosts and open/closed/filtered ports.
- Examples of Probing attacks: ***SYN Scan***, ***FIN Scan***, ***Connect Scan***, ***Ack Scan***
- Popular Scanners tools: Nmap **(nmap.org)**, Xscan **(www.xfocus.org/programs.php).**

Discover Active Hosts

Using NMAp to execute a ping scan against the network 137.207.0.1/16



Scan for Open Port and Running Services

- TCP SYN SCAN:
  - Check for open ports by sending SYN packets in succession to different ports.
  - Open ports respond with a SYN-ACK, and closed ports with a RST.
  - If a port is opened the attacker usually tears down the connection with a reset.
- One of the most common scanning method
- The traffic logs will show a large number of SYNs and RSTs.

OS Fingerprinting

- Many exploits are written for a specific OS
- So finding out the OS is essential
- Two approaches to OS fingerprinting
  - Simple methods will inspect TCP packets and analyze window's size and Time to Live (TTL).
  - Advanced methods will use TCP/IP stack fingerprinting

Network Service Fingerprint

- To identify network service, we always consider the TCP/UDP port to have an idea what service could be running on the target host.
- Knowing the available TCP|UDP port we could guess that the host is running HTTP when port 80 is open, SMTP when port 25 is open and so on.
- However, it is important to detect the type and the version of the service running on the host to be able to identify the potential vulnerabilities and risk.

Probe Host (137.207.76.168)

```
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 15.864 days (since Sat Jan 13 01:11:08 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

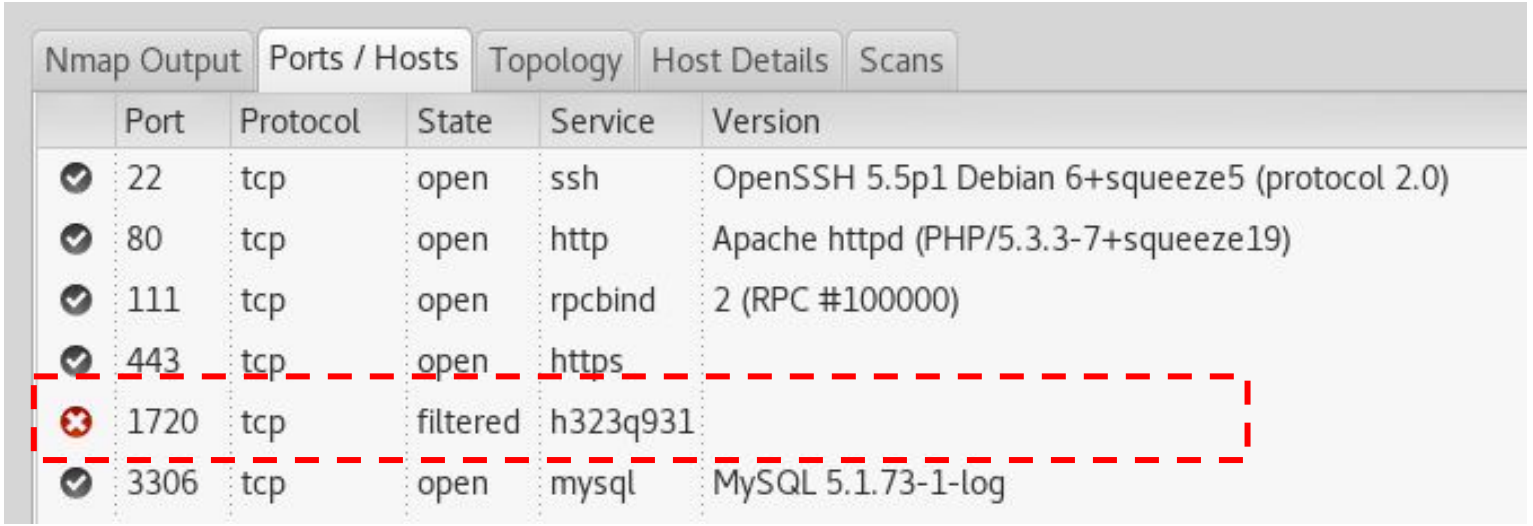
- The host OS in this case seems to be Linux OS. This host has been up and running for almost 16 days

Probe Host (137.207.76.168)

```
Initiating SYN Stealth Scan at 21:34
Scanning social.cs.uwindsor.ca (137.207.76.168) [1000 ports]
Discovered open port 80/tcp on 137.207.76.168
Discovered open port 443/tcp on 137.207.76.168
Discovered open port 111/tcp on 137.207.76.168
Discovered open port 22/tcp on 137.207.76.168
Discovered open port 3306/tcp on 137.207.76.168
Increasing send delay for 137.207.76.168 from 0 to 5 due to 41
out of 101 dropped probes since last increase.
Increasing send delay for 137.207.76.168 from 5 to 10 due to 95
out of 237 dropped probes since last increase.
Completed SYN Stealth Scan at 21:35, 24.82s elapsed (1000 total
ports)
```

- By performing SYN Stealth scan against the target host we discovered 5 open TCP ports

Probe Host (137.207.76.168)



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

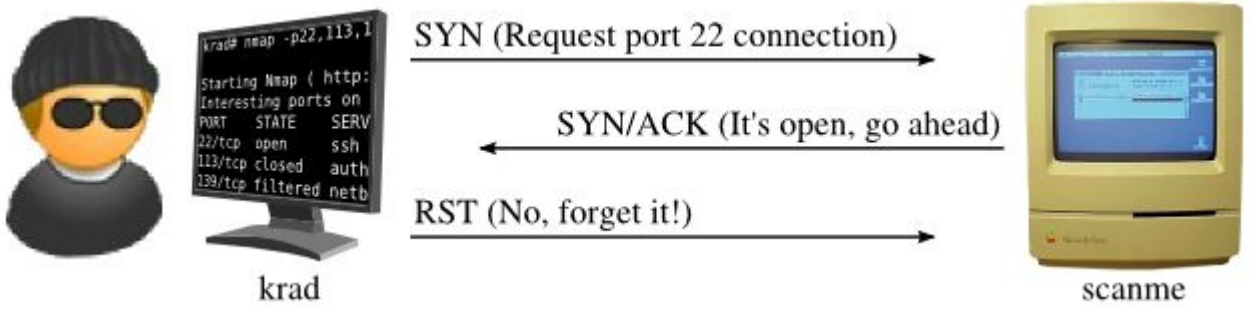
Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
80	tcp	open	http	Apache httpd (PHP/5.3.3-7+squeeze19)
111	tcp	open	rpcbind	2 (RPC #100000)
443	tcp	open	https	
1720	tcp	filtered	h323q931	
3306	tcp	open	mysql	MySQL 5.1.73-1-log

- Detecting the open ports, the type and the version of the services listening on these ports

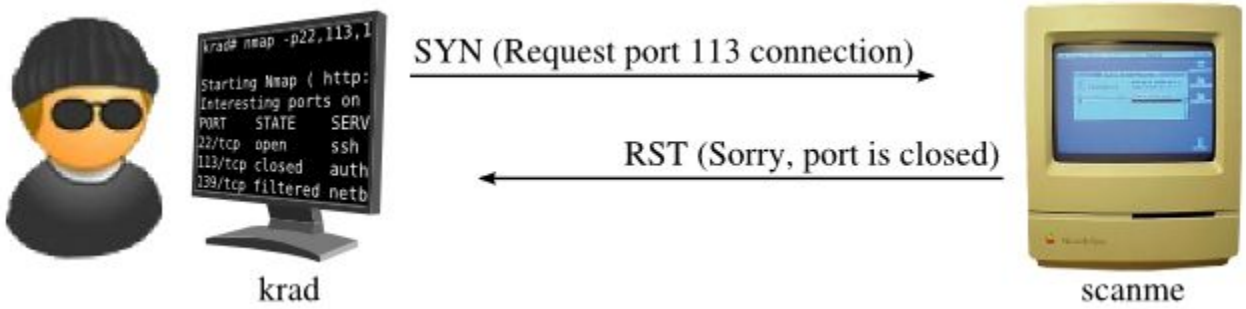
Port Scanning

- In general, there are 3 possible outcome:
  - Open: we are sure the port is open (e.g. received TCP SYN/ACK)
  - Close: The port is closed. We received an ICMP error message or TCP packet with RST flag
  - Filtered: This means there is a packet filtering process (firewall device, router rules, or host-based firewall software). Filtered connections do not reply at all and simply drop the packet.

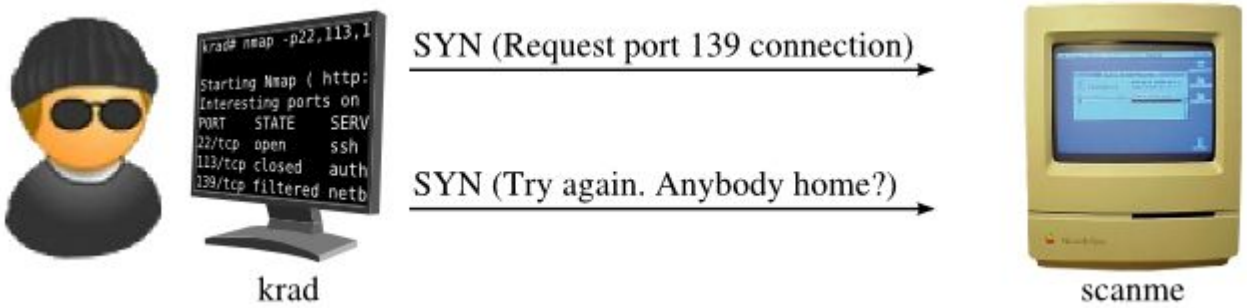
Port Scan with SYN scan: Open Port



Port Scan with SYN scan: Closed



Port Scan with SYN scan: Closed

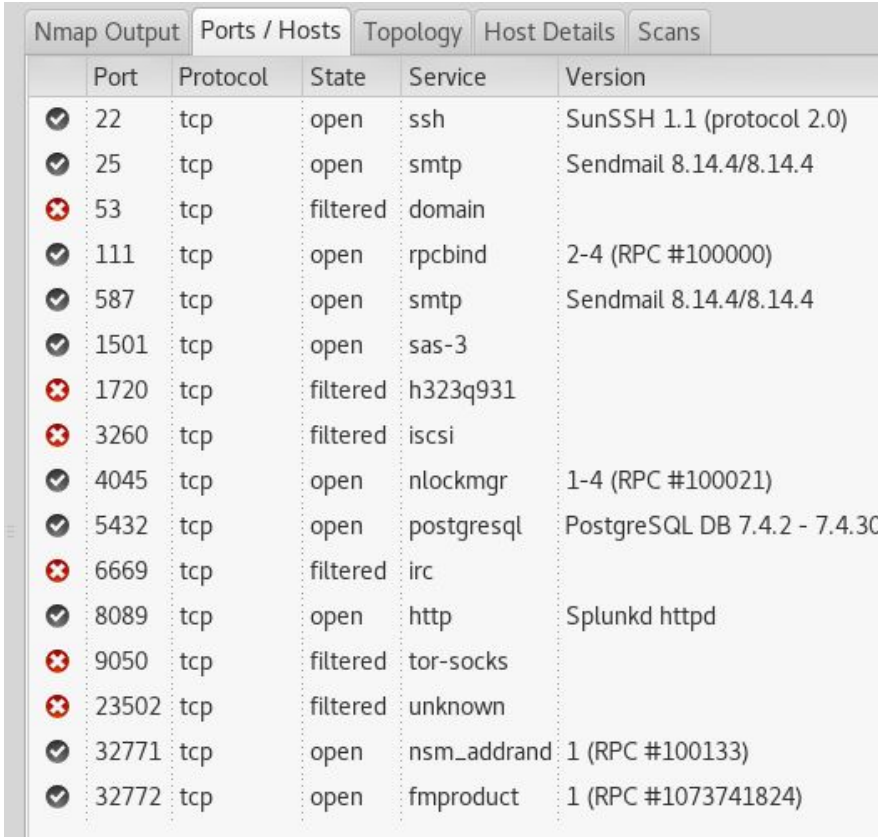


Port Scan with SYN scan

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`

Probe Host (137.207.32.14)



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

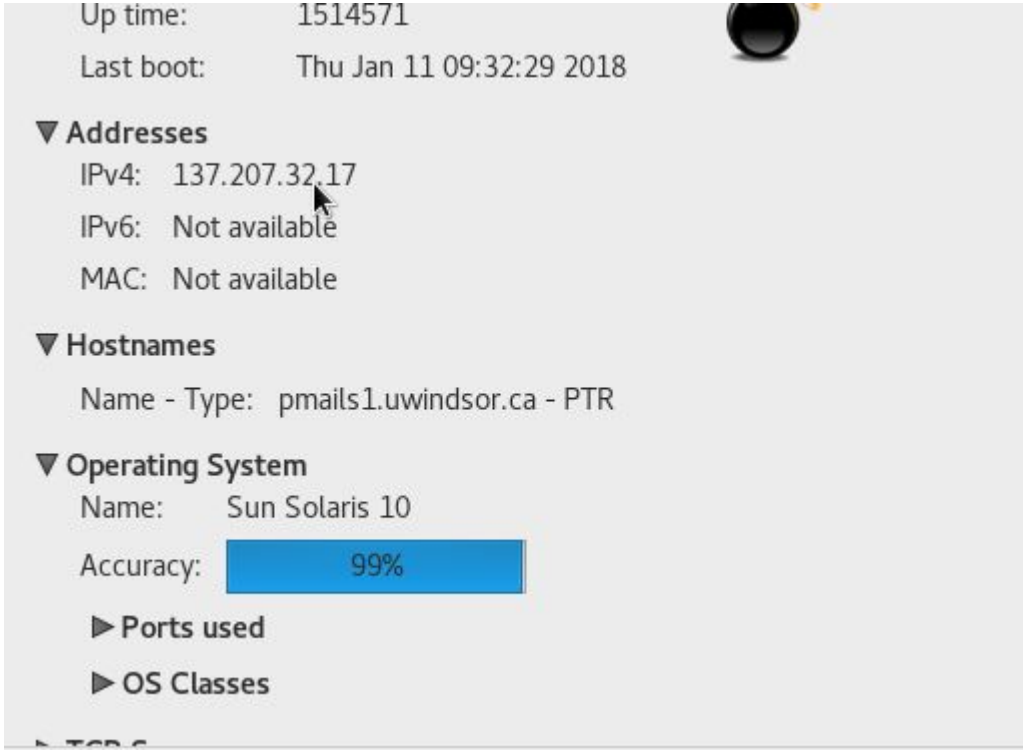
	Port	Protocol	State	Service	Version
✓	22	tcp	open	ssh	SunSSH 1.1 (protocol 2.0)
✓	25	tcp	open	smtp	Sendmail 8.14.4/8.14.4
✗	53	tcp	filtered	domain	
✓	111	tcp	open	rpcbind	2-4 (RPC #100000)
✓	587	tcp	open	smtp	Sendmail 8.14.4/8.14.4
✓	1501	tcp	open	sas-3	
✗	1720	tcp	filtered	h323q931	
✗	3260	tcp	filtered	iscsi	
✓	4045	tcp	open	nlockmgr	1-4 (RPC #100021)
✓	5432	tcp	open	postgresql	PostgreSQL DB 7.4.2 - 7.4.30
✗	6669	tcp	filtered	irc	
✓	8089	tcp	open	http	Splunkd httpd
✗	9050	tcp	filtered	tor-socks	
✗	23502	tcp	filtered	unknown	
✓	32771	tcp	open	nsm_addrand	1 (RPC #100133)
✓	32772	tcp	open	fmproduct	1 (RPC #1073741824)

Probe Host (137.207.32.14)

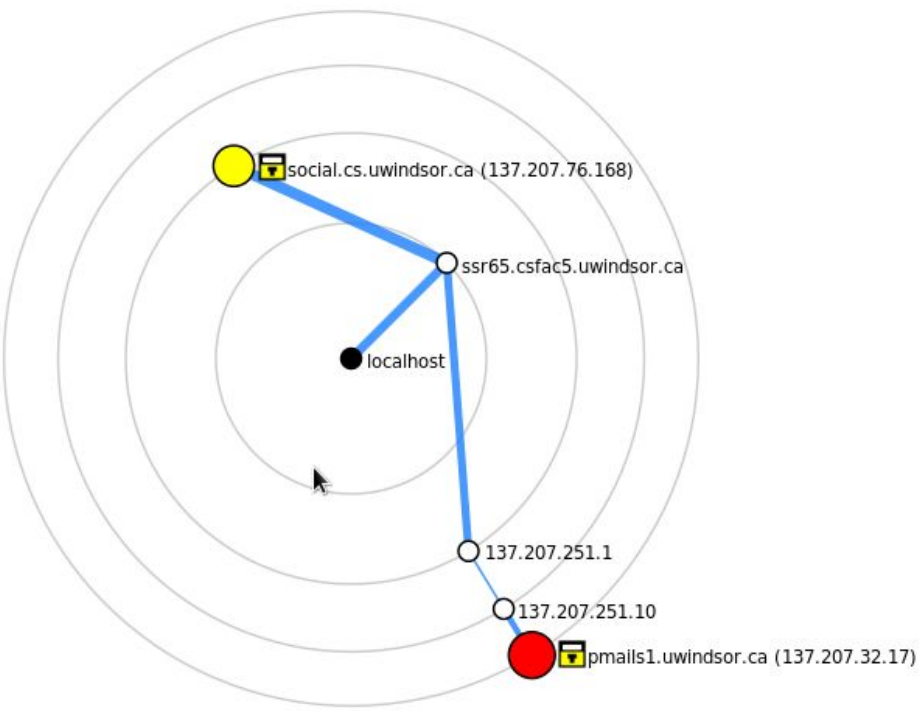
```
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=1/28%OT=22%CT=1%CU=35606%PV=N%DS=4%DC=T%G=Y%TM=5A6E91C
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=96%GCD=1%ISR=A3%TI=I%TS=7)OPS(O1=NNT11M5B
OS:4NW0NNS%O2=NNT11M5B4NW0NNS%O3=NNT11M5B4NW0%O4=NNT11M5B4NW0NNS%O5=NNT11M5
OS:B4NW0NNS%O6=NNT11M5B4NNS)WIN(W1=C050%W2=C330%W3=C1CC%W4=C050%W5=C068%W6=
OS:C0B7)ECN(R=Y%DF=Y%T=3D%W=C1E8%O=M5B4NW0NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=3D%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=41%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=Y%T=100%IPL=70%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=Y%T=100%CD=S)

Uptime guess: 17.530 days (since Thu Jan 11 09:32:29 2018)
Network Distance: 4 hops
```

- Probe another host uwindsor mail server. As we can see this time we are not sure what OS is running on the host

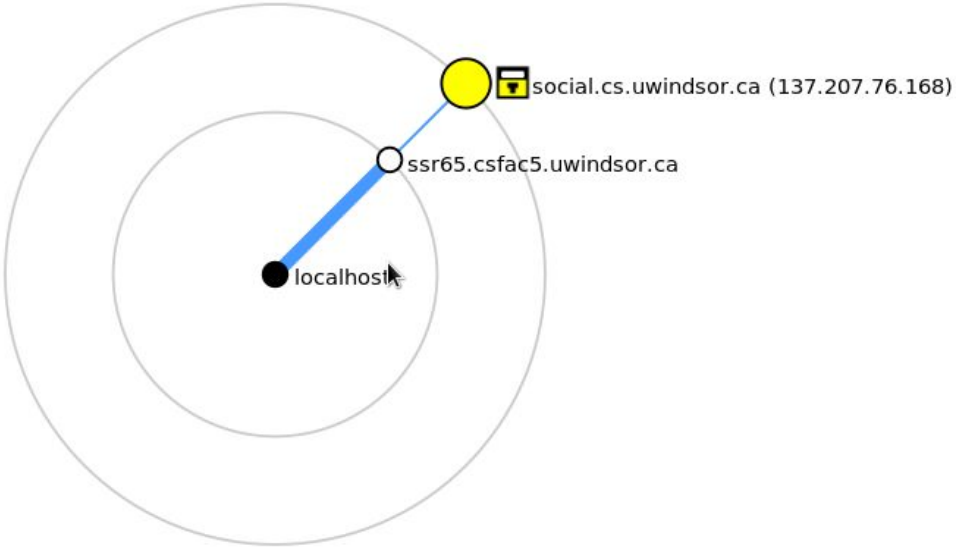
Probe Host (137.207.32.17)



Probe Host (137.207.32.17)



Probe Host (137.207.76.168)



- Using traceroute we could detect the pass from the target to the victim

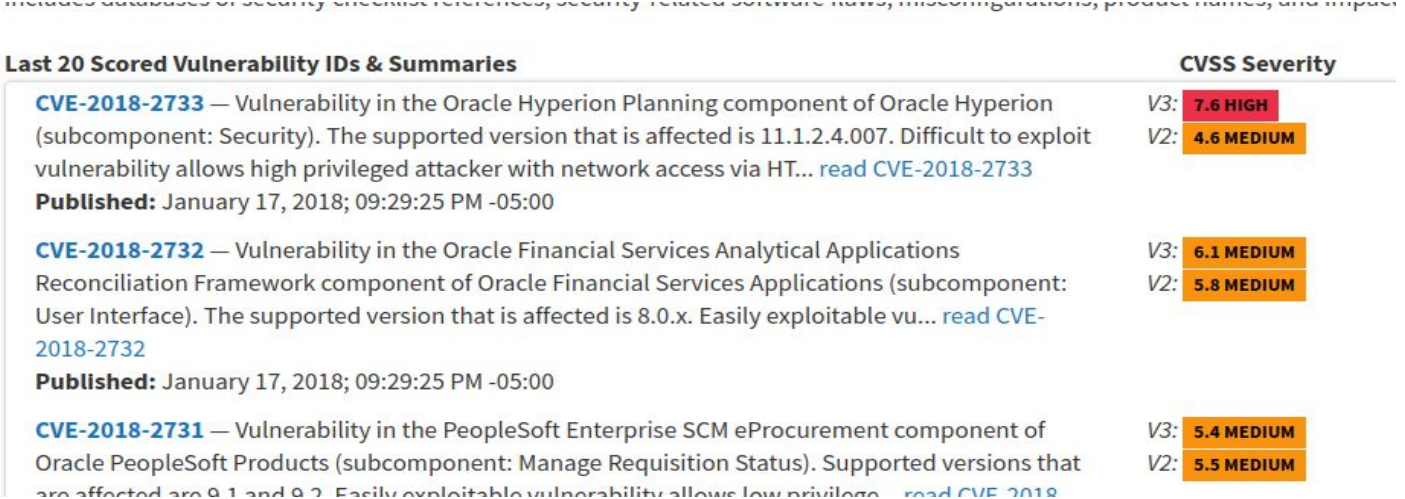
Vulnerability Identification

- What is security vulnerability?
  - A vulnerability is a weakness in a system which allows the attacker to breach the security of the system.
- Vulnerabilities can be identified from lists and reports on common vulnerabilities and also by testing the system using vulnerabilities assessment tools.
- Examples for vulnerability assessment tools are **OpenVAS** and **Nessus**

Vulnerability Identification

- **Online Vulnerabilities Databases**
  - Databases – NIST National Vulnerability Database
  - Vendor advisories – Google directory of computer security advisories and patches
  - CIRT lists and bulletins
    - US-CERT
    - SANS Top 20
    - SANS Internet Storm Center

Vulnerability Identification

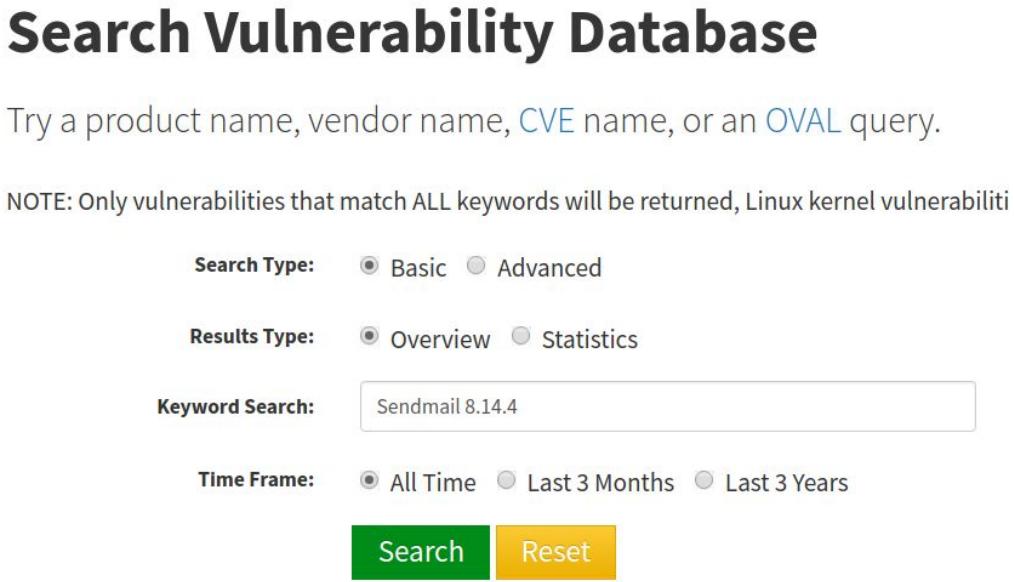


Last 20 Scored Vulnerability IDs & Summaries	CVSS Severity
CVE-2018-2733 — Vulnerability in the Oracle Hyperion Planning component of Oracle Hyperion (subcomponent: Security). The supported version that is affected is 11.1.2.4.007. Difficult to exploit vulnerability allows high privileged attacker with network access via HT... read CVE-2018-2733 **Published:** January 17, 2018; 09:29:25 PM -05:00	*V3:* 7.6 HIGH *V2:* 4.6 MEDIUM
CVE-2018-2732 — Vulnerability in the Oracle Financial Services Analytical Applications Reconciliation Framework component of Oracle Financial Services Applications (subcomponent: User Interface). The supported version that is affected is 8.0.x. Easily exploitable vu... read CVE-2018-2732 **Published:** January 17, 2018; 09:29:25 PM -05:00	*V3:* 6.1 MEDIUM *V2:* 5.8 MEDIUM
CVE-2018-2731 — Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). Supported versions that are affected are 9.1 and 9.2. Easily exploitable vulnerability allows low privilege... read CVE-2018	*V3:* 5.4 MEDIUM *V2:* 5.5 MEDIUM

[NIST National Vulnerability Database]

Vulnerability Identification

- Let us search for known vulnerabilities in "Sendmail 8.14.4"



Vulnerability Identification

- Only one vulnerability with high severity, exist in sendmail 8.14.4 which enable Man-in-the-middle attack.

Vuln ID	Summary	CVSS Severity
CVE-2009-4565	sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408. **Published:** January 04, 2010; 04:30:00 PM -05:00	*V2:* 7.5 HIGH

Vulnerability Verification

- The process of exploiting or attempt to exploit identified vulnerabilities to check if it exists or not.
- Vulnerability verification could be a manual or an automated process.
- Vulnerability verification is an active vulnerability assessment step.
- Examples of vulnerability verification tools are Nessus, OpenVAS, Metasploit and other pentesting tools

Summary

In this class we covered:

- Basic Information Gathering Techniques.
- Service Discovery and Vulnerabilities Identification.

What is Next?

In our next Classes we will focus on:

- Application Layer Exploits
  - Access Control Systems,
  - Web Exploit
  - Database Exploit