Attack Methodology

NMAP
DURATION : 0'30

NMAP

- **Basic scan**

Command	Description
nmap 10.0.0.1	Scan a single host IP
nmap 192.168.10.0/24	Scan a range
nmap 10.1.1.5-100	Scan the range of IPs between 10.1.1.5 up to 10.1.1.100
nmap -iL hosts.txt	Scan the IP addresses listed in text file “hosts.txt”
nmap 10.1.1.3 10.1.1.6 10.1.1.8	Scan the 3 specified IPs only
nmap www.somedomain.com	First resolve the IP of the domain and then scan its IP address

NMAP

- **Scan types**

Command	Description
nmap -sS 10.1.1.1	TCP SYN scan
nmap -sT 10.1.1.1	TCP connect scan
nmap -sU 10.1.1.1	UDP scan
nmap -sn 10.1.1.0/24	Do a Ping scan only / No port scan (often called ping sweep)
nmap -Pn 10.1.1.1	Don't ping the hosts, assume they are up.

NMAP (UDP Scan 1/3) : -sU

- While most popular services on the Internet run over the TCP protocol, UDP services are widely deployed (DNS 53, SNMP 161/162, and DHCP 67/68).
- UDP scanning is generally slower and more difficult than TCP. This is a mistake, as exploitable UDP services are quite common and attackers certainly don't ignore the whole protocol.
- UDP scan works by sending a UDP packet to every targeted port. For most ports, this packet will be empty (no payload), but for a few of the more common ports a protocol-specific payload will be sent. Based on the response, or lack thereof, the port is assigned to one of four states, as shown below:

Response	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

NMAP (UDP Scan 2/3) : -sU

- The most curious element of this table may be the open | filtered state. It is a symptom of the biggest challenges with UDP scanning: open ports rarely respond to empty probes.
- UDP Scan example:

```
krad# nmap -sU -v felix

Starting Nmap ( http://nmap.org )
Nmap scan report for felix.nmap.org (192.168.0.42)
(The 997 ports scanned but not shown below are in state: closed)
PORT    STATE         SERVICE
53/udp  open|filtered domain
67/udp  open|filtered dhcpserver
111/udp open|filtered rpcbind
MAC Address: 00:02:E3:14:11:02 (Lite-on Communications)

Nmap done: 1 IP address (1 host up) scanned in 999.25 seconds
```

- This scan of “felix” demonstrates the open | filtered ambiguity issue as well as another problem: UDP scanning can be slow.
- Scanning a thousand ports took almost 17 minutes in this case due to ICMP response rate limiting performed by the OS target.

NMAP (UDP Scan 3/3) : -sU

- Nmap provides ways to work around both problems, as described by the following two sections.
- The reason these services don't respond often is that the empty packets Nmap sends are considered invalid. Unfortunately, UDP services generally define their own packet structure rather than adhering to some common general format. An SNMP packet looks completely different than a SunRPC, DHCP, or DNS request packet.
- To send the proper packet for every popular UDP service, Nmap would need a large database defining their probe formats (nmap-service-probes).
- When version scanning is enabled with -sV (or -A), it will send UDP probes to every open|filtered port (as well as known open ones). If any of the probes elicit a response from an open|filtered port, the state is changed to open.

```
krad# nmap -sUV -F felix.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for felix.nmap.org (192.168.0.42)
Not shown: 997 closed ports
PORT    STATE         SERVICE    VERSION
53/udp  open          domain     ISC BIND 9.2.1
67/udp  open|filtered dhcpserver
111/udp open          rpcbind    2 (rpc #100000)
MAC Address: 00:02:E3:14:11:02 (Lite-on Communications)

Nmap done: 1 IP address (1 host up) scanned in 1037.57 seconds
```

NMAP (TCP SYN Scan) : -sS

- SYN scan is the default and most popular scan option for good reason :
  - It can be performed quickly (scanning thousands of ports per second),
  - It's not hampered by intrusive firewalls (unobtrusive and stealthy because it never completes TCP connections),
  - It also allows clear, reliable differentiation between open, closed, and filtered states.

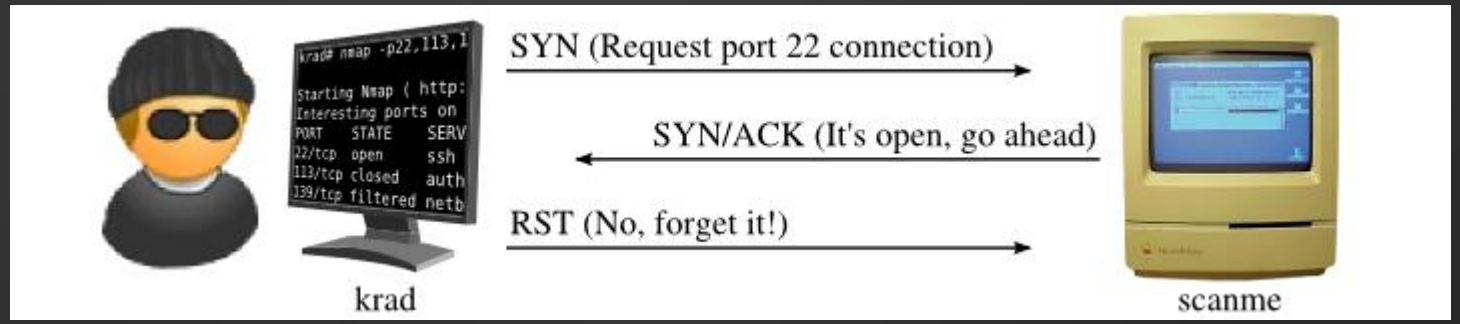
Response	State
TCP SYN/ACK response	open
TCP RST response	closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

NMAP : SYN scan of open port 22


```
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
```

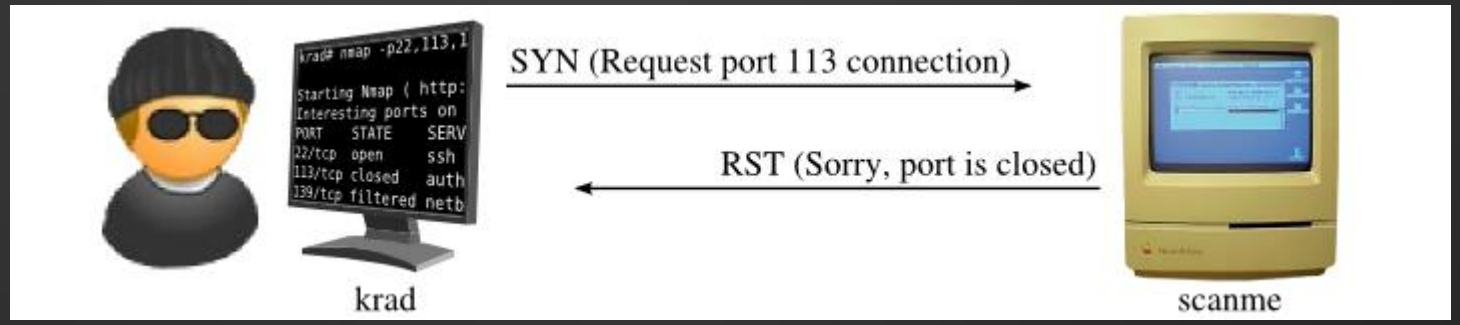


NMAP : SYN scan of closed port 113


```
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
```

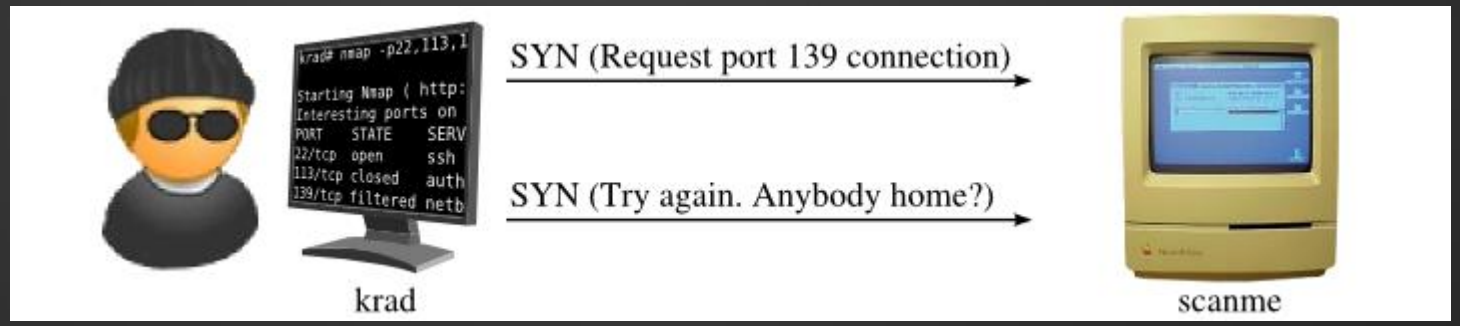


NMAP : SYN scan of filtered port 139


```
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
```

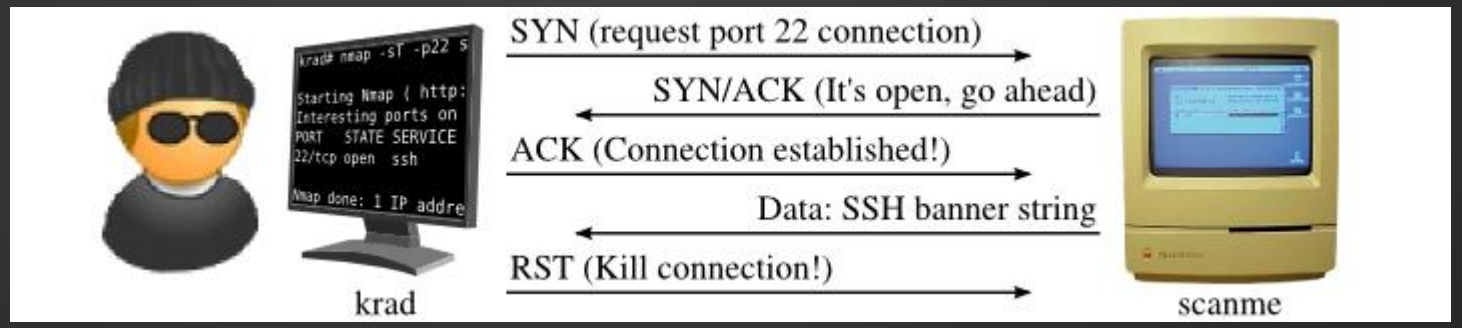


NMAP : TCP connect scan


```
krad~> nmap -T4 -sT scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  closed smtp
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http
113/tcp closed auth

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
```



NMAP

- **Other TCP scan type (based on TCP flags)**

Command	Description
nmap -sN 10.1.1.1	Scan TCP with not set any bits (TCP flag header is 0)
nmap -sF 10.1.1.1	Scan TCP with sets just the TCP FIN bit.
nmap -sX 10.1.1.1	Scan TCP with sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

TCP segment header

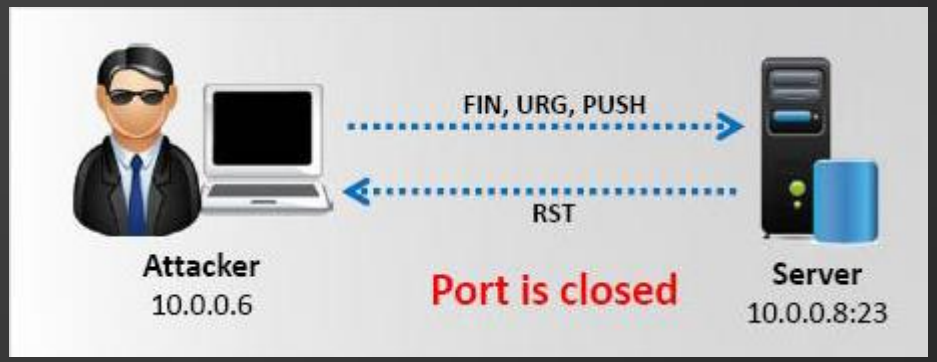
Offsets	Octet	0								1								2								3							
Octet	Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																	Urgent pointer (if URG set)														
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

Response	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

NMAP : TCP FIN or URG or PUSH scan


```
# nmap -sF -T4 docsrv.caldera.com

Starting Nmap ( http://nmap.org )
Nmap scan report for docsrv.caldera.com (216.250.128.247)
Not shown: 961 closed ports
PORT      STATE         SERVICE
7/tcp     open|filtered echo
9/tcp     open|filtered discard
11/tcp    open|filtered systat
13/tcp    open|filtered daytime
15/tcp    open|filtered netstat
19/tcp    open|filtered chargen
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
37/tcp    open|filtered time
79/tcp    open|filtered finger
80/tcp    open|filtered http
110/tcp   open|filtered pop3
111/tcp   open|filtered rpcbind
135/tcp   open|filtered msrpc
```



NMAP : ACK scan (-sA)

- ACK scan is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

```
krad# nmap -sA -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
53/tcp  unfiltered domain
70/tcp  unfiltered gopher
80/tcp  unfiltered http
113/tcp unfiltered auth

Nmap done: 1 IP address (1 host up) scanned in 4.01 seconds
```

Response	State
TCP RST response	unfiltered
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

NMAP

- **Basic port scan**

Command	Description
nmap -p80 10.1.1.1	Scan only port 80 for specified host
nmap -p20-23 10.1.1.1	Scan ports 20 up to 23 for specified host
nmap -p80,88,8000 10.1.1.1	Scan ports 80,88,8000 only
nmap -p- 10.1.1.1	Scan ALL ports for specified host
nmap -sS -sU -p U:53,T:22 10.1.1.1	Scan ports UDP 53 and TCP 22
nmap -p http,ssh 10.1.1.1	Scan http and ssh ports for specified host

NMAP

- **Identify Versions of Services and Operating Systems**

Command	Description
nmap -sV 10.1.1.1	Version detection scan of open ports (services)
nmap -O 10.1.1.1	Identify Operating System version
nmap -A 10.1.1.1	This combines OS detection, service version detection, script scanning and traceroute.

NMAP

- **Scan timings**

Command	Description
nmap -T0 10.1.1.1	Slowest scan (to avoid IDS)
nmap -T1 10.1.1.1	Sneaky (to avoid IDS)
nmap -T2 10.1.1.1	Polite (10 times slower than T3)
nmap -T3 10.1.1.1	Default scan timer (normal)
nmap -T4 10.1.1.1	Aggressive (fast and fairly accurate)
nmap -T5 10.1.1.1	Very Aggressive (might miss open ports)

NMAP

- **Output types**

Command	Description
nmap -oN [filename] [IP hosts]	Normal text format
nmap -oG [filename] [IP hosts]	Grepable file (useful to search inside file)
nmap -oX [filename] [IP hosts]	XML file
nmap -oA [filename] [IP hosts]	Output in all 3 formats supported

NMAP

- **Discover live hosts**

Command	Description
nmap -PS22-25,80 10.1.1.0/24	Discover hosts by TCP SYN packets to specified ports (in our example here the ports are 22 to 25 and 80)
nmap -Pn 10.1.1.0/24	Disable port discovery. Treat all hosts as online.
nmap -PE 10.1.1.0/24	Send ICMP Echo packets to discover hosts.
nmap -sn 10.1.1.0/24	Ping scan.

NMAP

- **NSE scripts** (for more information : https://nmap.org/book/man-nse.html)

Command	Description
nmap --script <filename>|<category>|<directory>	Runs a script scan using the comma-separated list of filenames, script categories, and directories.
nmap –script “http-*" 10.1.1.0/24	Loads all scripts whose name starts with http-, such as http-auth and http-open-proxy. The argument to --script had to be in quotes to protect the wildcard from the shell.
nmap –script "http-*" --script-args 'user=foo’ 10.1.1.3	Lets you provide arguments to NSE scripts. Arguments are a comma-separated list of name=value pairs.

NMAP

- **Example of an NSE script**

```
root@bt:/usr/share/nmap/scripts# nmap -p 135,139,445 --script=smb-pwdump.nse --script-args=smbuser=administrator,smbpass=lamepassword 192.168.0.190


Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-09-29 12:18 CDT
Nmap scan report for 192.168.0.190
Host is up (0.0013s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:BE:EF:6B (Cadmus Computer Systems)

Host script results:
| smb-pwdump:
| Administrator:500 => D53AD4A74DD31D5476FDE78389BE2CE2:C1D90F01AB325FA3194D22AA2D201211
| Guest:501 => NO PASSWORD**********************:NO PASSWORD**********************
| SUPPORT_388945a0:1001 => NO PASSWORD**********************:E550E0A3B401BFA01673C201C735072A
| testaccount1:1003 => E52CAC67419A9A2238F10713B629B565:5835048CE94AD0564E29A924A03510EF
| testaccount2:1004 => E52CAC67419A9A22F96F275E1115B16F:E22E04519AA757D12F1219C4F31252F4
|_testaccount3:1005 => E52CAC67419A9A221B087C18752BDBEE:BD7DFBF29A93F93C63CB84790DA00E63

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
root@bt:/usr/share/nmap/scripts#
```

NMAP

- **Always more**

Command	Description
nmap -p80,443 100.100.100.0/24 -oG – | nikto.pl -h –	Find HTTP servers and then run nikto against them
nmap -p80,443 --script http-waf-detect --script-args="http-waf-detect.aggro,http-waf-detect.detectBodyChanges" www.site.fr	Detect if a Website is protected by WAF
nmap -Pn -sV -p80 --script=vulners 10.0.0.6	Find well known vulnerabilities related to an open port

NMAP

- **Test it : https://tryhackme.com/room/nmap01**