



More ▾

Create Blog Sign In

TECHNOLOGY REDEFINE

Home

ETHICAL HACKING

LINUX

EBOOKS

SECURITY+

TOOLS

Wednesday, September 27, 2017

IDS, IPS AND FIREWALL EVASION USING NMAP



NIDS - Network Intrusion Detection System

- It Uses a network tap, span port, or hub to collect packets on the network
- Attempts to identify unauthorized, illicit, and anomalous



SEARCH

STATISTICS

33950

DON'T MISS OUR UPDATE

FOLLOW BY EMAIL

behavior based on network traffic

- Methods: signature file comparisons, anomaly detection, stateful protocol analysis
- Using the captured data, the IDS system processes and flags any suspicious traffic

HIDS – Host Intrusion Detection System

- Generally involves an agent installed on each system, monitoring and alerting on local OS and application activity
- Attempts to identify unauthorized, illicit, and anomalous behavior on a specific device/OS
- The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorized activity

IDS : Only reports that there was an intrusion.

IPS : Also takes actions against the issue to fix it or at least lessen its impact.

Evasion Techniques

- Decoys
- Proxies
- MAC Address Spoofing
- Ping Suppression
- Half Open Scan
- Fragmentation
- Timing

LABEL

- Cracking Hashes
- CVE-2018-0802
- DNS Enumeration & Interrogation
- Dump Hashes
- Dumpster-Diving
- Enumeration
- Evasion Techniques
- Finding Open Ports
- Firewall Evasion Countermeasures
- Footprinting Tools and Techniques
- Information Gathering
- Installing And Removing Application
- Installing VirtualBox Guest Addition
- Introduction To Linux
- Least privilege
- Linux Basic Commands
- MAC Spoofing

- Changing Data length
- Transmission Unit
- Random Scan
- Sending Bad Checksums
- Using Multiple Techniques

Decoys

Not strictly an evasion technique, It is used to obscure the source of the scan. we still need to send packets from our IP address but we can spoof other IP addresses while scanning so that it appears that the scan is coming from other hosts.

This might make it more difficult for the security device to automatically block our IP and more difficult for a forensic investigation to figure our IP.

```
nmap -sS --top-ports 10 -D 192.168.43.1 192.168.43.103
```

- Network Access Control
- Nmap Cheatsheet
- Nmap Scanning
- NTLM Hashes
- Password Hacking
- Password Hacking Countermeasures
- Password Sniffing
- payload generator
- post exploitation
- Reconnaissance
- Remote Access
- Reverse Proxy Server
- Risk Assessment
- Router Attacks
- Scanning
- Scanning Types
- Social Engineering
- Surveillance
- Virtual Ports
- Zone Transfer

```
Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal X Parrot Terminal X Parrot Terminal X

--top-ports should be an integer 1 or greater
QUITTING!
[~/root@parrot:~]
# nmap -sS --top-ports 10 -D 192.168.43.1 192.168.43.103

Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-27 04:01 EDT
Nmap scan report for Virus (192.168.43.103)
Host is up (0.0010s latency).
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
80/tcp    filtered http
110/tcp   filtered pop3
139/tcp   open  netbios-ssn
443/tcp   filtered https
445/tcp   open  microsoft-ds
3389/tcp  filtered ms-wbt-server
MAC Address:

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

No.	Time	Source	Destination	Protocol	Length	Info
78	13.885988158	192.168.43.1	192.168.43.103	TCP	58	38165 - 110 [SYN] Seq=0 Win=0
79	13.886052446	192.168.43.185	192.168.43.103	TCP	58	38165 - 3389 [SYN] Seq=0 Win=0
80	13.886116122	192.168.43.1	192.168.43.103	TCP	58	38165 - 3389 [SYN] Seq=0 Win=0
81	13.886179931	192.168.43.185	192.168.43.103	TCP	58	38165 - 21 [SYN] Seq=0 Win=0
82	13.886233508	192.168.43.1	192.168.43.103	TCP	58	38165 - 21 [SYN] Seq=0 Win=0
83	13.886297112	192.168.43.185	192.168.43.103	TCP	58	38165 - 25 [SYN] Seq=0 Win=0
84	13.886414773	192.168.43.1	192.168.43.103	TCP	58	38165 - 25 [SYN] Seq=0 Win=0
85	13.886467393	192.168.43.185	192.168.43.103	TCP	58	38165 - 88 [SYN] Seq=0 Win=0
86	13.886478149	192.168.43.1	192.168.43.103	TCP	58	38165 - 88 [SYN] Seq=0 Win=0
87	13.886482215	192.168.43.185	192.168.43.103	TCP	58	38165 - 443 [SYN] Seq=0 Win=0
88	13.886674335	192.168.43.1	192.168.43.103	TCP	58	38165 - 443 [SYN] Seq=0 Win=0
89	13.886451661	192.168.43.185	192.168.43.103	TCP	58	38165 - 23 [SYN] Seq=0 Win=0
90	13.886579329	192.168.43.1	192.168.43.103	TCP	58	38165 - 23 [SYN] Seq=0 Win=0
91	13.886643133	192.168.43.185	192.168.43.103	TCP	58	38165 - 22 [SYN] Seq=0 Win=0
92	13.886709843	192.168.43.1	192.168.43.103	TCP	58	38165 - 22 [SYN] Seq=0 Win=0
93	14.055261899	192.168.43.185	192.168.43.103	TCP	58	38174 - 139 [SYN] Seq=0 Win=0
94	14.036371164	192.168.43.1	192.168.43.103	TCP	58	38174 - 139 [SYN] Seq=0 Win=0
95	14.036844888	192.168.43.103	192.168.43.185	TCP	60	139 - 38174 [SYN, ACK] Seq=0
96	14.037062775	192.168.43.185	192.168.43.103	TCP	54	38174 - 139 [RST] Seq=1 Win=0
97	14.075865206	192.168.43.103	192.168.43.185	TCP	60	445 - 38163 [SYN, ACK] Seq=0
98	14.075913617	192.168.43.185	192.168.43.103	TCP	54	38163 - 445 [RST] Seq=1 Win=0

`nmap -sS -D Rnd:5 192.168.43.103`

Rnd:5 will generate 5 random decoys

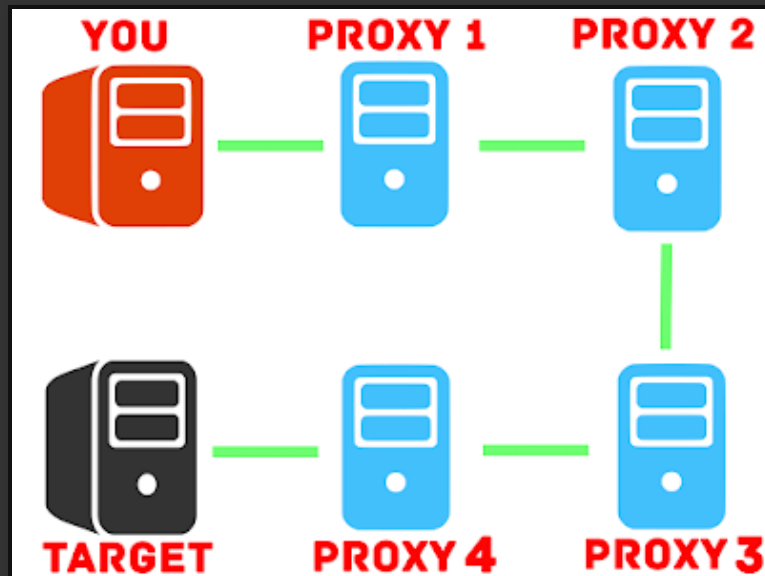


No.	Time	Source	Destination	Protocol	Length	Info
94	35.427014515	192.168.43.79	192.168.43.185	TCP	60	53 → 49388 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
95	35.427048002	192.168.43.185	192.168.43.79	TCP	54	49388 → 63 [RST] Seq=1 Win=0 Len=0
96	35.427186762	192.168.43.79	192.168.43.79	TCP	58	49388 → 5990 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
97	35.427295495	78.67.178.54	192.168.43.79	TCP	58	49388 → 5990 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
98	35.427376926	7.101.49.152	192.168.43.79	TCP	58	49388 → 5990 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
99	35.427450042	192.168.43.185	192.168.43.79	TCP	58	49388 → 5990 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
100	35.427529766	91.41.187.230	192.168.43.79	TCP	58	49388 → 5990 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
101	35.427601538	192.168.43.79	192.168.43.79	TCP	58	49388 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
102	35.427814588	78.67.178.54	192.168.43.79	TCP	58	49388 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
103	35.427887679	7.101.49.152	192.168.43.79	TCP	58	49388 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
104	35.427954294	192.168.43.185	192.168.43.79	TCP	58	49388 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
105	35.428021436	91.41.187.230	192.168.43.79	TCP	58	49388 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
106	35.428094504	192.168.43.79	192.168.43.79	TCP	58	49388 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
107	35.428167919	78.67.178.54	192.168.43.79	TCP	58	49388 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
108	35.428251794	7.101.49.152	192.168.43.79	TCP	58	49388 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
109	35.428327764	192.168.43.185	192.168.43.79	TCP	58	49388 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
110	35.428400431	91.41.187.230	192.168.43.79	TCP	58	49388 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
111	35.428485344	192.168.43.79	192.168.43.79	TCP	58	49388 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
112	35.428561695	78.67.178.54	192.168.43.79	TCP	58	49388 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
113	35.428638444	7.101.49.152	192.168.43.79	TCP	58	49388 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
114	35.428709557	192.168.43.185	192.168.43.79	TCP	58	49388 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
115	35.428779662	91.41.187.230	192.168.43.79	TCP	58	49388 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
116	35.428850066	192.168.43.79	192.168.43.79	TCP	60	49388 → 1750 [ACK] Seq=0 Win=1024 Len=0 MSS=1460

Using Proxies

We can use proxies between ourselves and the target system. By using proxies, the IP address of the proxies is recorded at the target, rather than our own. Makes it VERY difficult to trace the source of the scan.

```
nmap -sS --proxies socks4://115.29.161.103:1080,  
http://213.85.92.10:80 Target
```



You can also scan using Tor network or Proxychain

MAC Address Spoofing

This technique can be very effective especially if there is a

MAC filtering rule to allow only traffic from certain MAC addresses so you will need to discover which MAC address you need to set in order to obtain results.

Specify MAC address from a Vendor `--spoof-mac Dell/Apple/`

Generate a random MAC address `--spoof-mac 0`

Specify your own MAC address `--spoof-mac 00:01:02:25:56:AE`

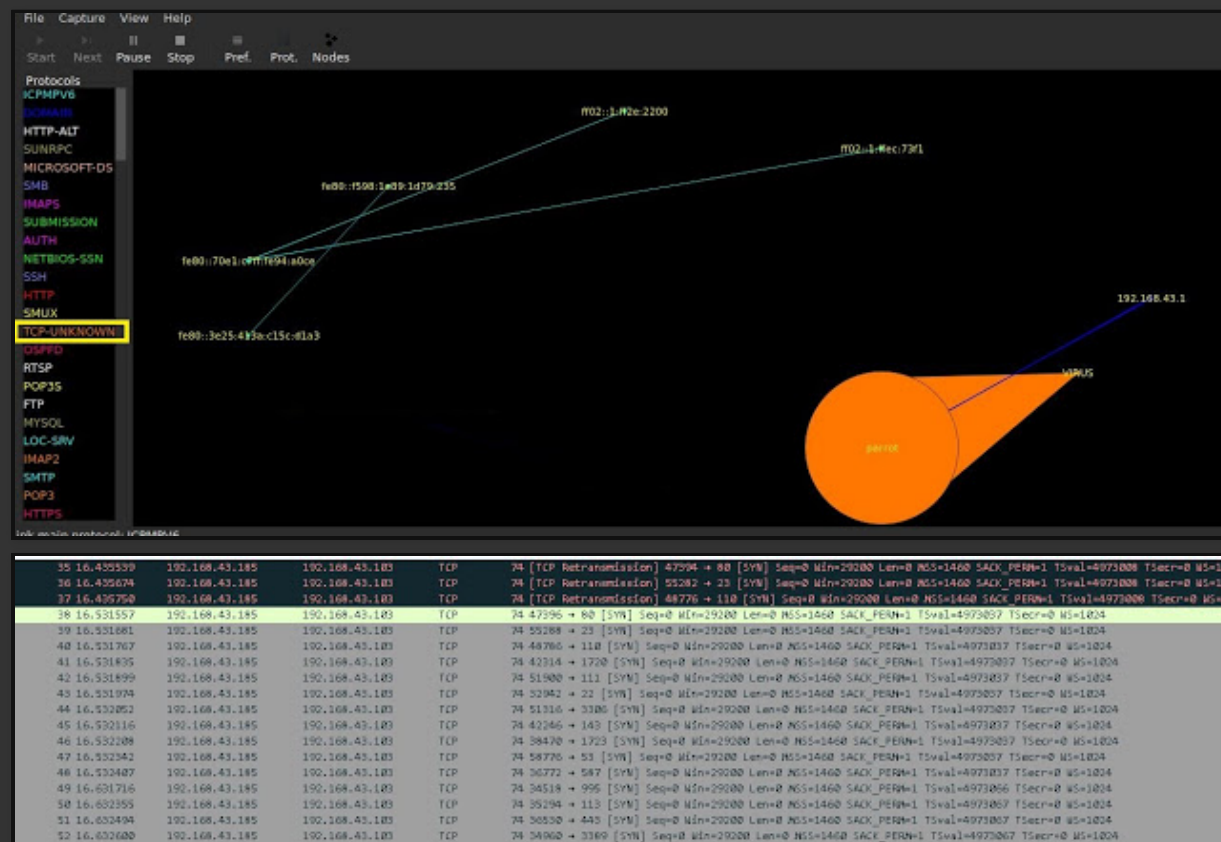


Ping Suppression

Often security administrators block ICMP (echo request, echo reply) ping on firewall to keep outside attackers from being able to find active hosts.

When we Scan With Nmap it sends out an ICMP Request to see if the host exists and is up. If it doesn't receive a response, it will report back that the host is down. By using the -Pn switch we can scan our target without sending the default ICMP.

```
nmap -Pn 192.168.43.103
```



Half Open Scan (ACK Scan)

When the TCP three-way handshake establishes (SYN, SYN-ACK, ACK), every packet sent subsequently in the communication will have the ACK bit set. Firewall will assume that this ACK packet is part of an established communication between the client and server and, thereby, let it pass.

```
[root@parrot]# nmap -sA --top-ports 10 192.168.43.103
Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-26 06:28 EDT
Nmap scan report for Virus (192.168.43.103)
Host is up (0.00033s latency).
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
25/tcp    filtered  smtp
80/tcp    filtered  http
110/tcp   filtered  pop3
139/tcp   filtered  netbios-ssn
443/tcp   filtered  https
445/tcp   filtered  microsoft-ds
3389/tcp  filtered  ms-wbt-server
MAC Address: 08:00:27:00:00:00

Nmap done: 1 IP address (1 host up) scanned in 8.55 seconds
```

- Only provides "filtered" or "unfiltered"
- Useful in reconnaissance for a more detailed scan

Fragmentation

In this attack nmap will break the IP header into many small pieces to evade the IDS. The pieces are then reassembled at

the destination. Since IDS's rely on signatures very similar to AV software the pieces would not match the signature the IDS is looking for. This would allow the pieces to traverse the network where they would be reassembled at the destination machine and do their dirty work.

For increasingly more smaller fragments use the `-ff` switch.

```
nmap -sT -f --top-ports 10 192.168.43.103
```

The screenshot displays two windows. The left window is a Parrot Terminal showing the output of an Nmap scan. The right window is Wireshark showing a packet capture of the scan.

Parrot Terminal Output:

```
Nmap done: 1 IP address (1 host up) scanned in 0.28s
root@parrot:~# nmap -sT -f --top-ports 10 192.168.43.103
Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-2
Nmap scan report for Virus (192.168.43.103)
Host is up (0.00001s latency).
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
80/tcp    filtered http
110/tcp   filtered pop3
139/tcp   open  netbios-ssn
443/tcp   filtered https
445/tcp   open  microsoft-ds
3389/tcp  filtered ms-wbt-server
MAC Address: ..

Nmap done: 1 IP address (1 host up) scanned in 0.31s
root@parrot:~#
```

Wireshark Packet Capture:

No.	Time	Source	Destination	Protocol	Length	Info
48	12.662613844	192.168.43.185	192.168.43.1	DNS	132	Standard query 0x8131 PTR 1.f.3.7.c.e.
49	12.662790461	192.168.43.185	192.168.43.1	DNS	132	Standard query 0x8131 PTR 0.0.2.2.e.3.
50	13.341532399	192.168.43.185	192.168.43.103	TCP	74	59318 → 23 [SYN] Seq=0 Win=29200 Len=0
51	13.341697858	192.168.43.185	192.168.43.103	TCP	74	36966 → 22 [SYN] Seq=0 Win=29200 Len=0
52	13.341782246	192.168.43.185	192.168.43.103	TCP	74	59514 → 21 [SYN] Seq=0 Win=29200 Len=0
53	13.341876290	192.168.43.185	192.168.43.103	TCP	74	51434 → 80 [SYN] Seq=0 Win=29200 Len=0
54	13.341973742	192.168.43.185	192.168.43.103	TCP	74	48752 → 139 [SYN] Seq=0 Win=29200 Len=0
55	13.342077398	192.168.43.185	192.168.43.103	TCP	74	34342 → 25 [SYN] Seq=0 Win=29200 Len=0
56	13.342395569	192.168.43.185	192.168.43.103	TCP	74	52826 → 118 [SYN] Seq=0 Win=29200 Len=0
57	13.342415582	192.168.43.185	192.168.43.103	TCP	74	139 → 48752 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0
58	13.342468037	192.168.43.185	192.168.43.103	TCP	66	48752 → 139 [ACK] Seq=1 Ack=1 Win=29200 Len=0
59	13.342568089	192.168.43.185	192.168.43.103	TCP	74	38978 → 3389 [SYN] Seq=0 Win=29200 Len=0
60	13.342654821	192.168.43.185	192.168.43.103	TCP	74	46552 → 443 [SYN] Seq=0 Win=29200 Len=0
61	13.343161409	192.168.43.185	192.168.43.103	TCP	66	48752 → 139 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	13.808715277	192.168.43.103	239.255.255.255	SSDP	175	M-SEARCH * HTTP/1.1

Wireshark Details:

- Frame 57: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: AmpakTec
- Internet Protocol Version 4, Src: 192.168.43.103, Dst: 192.168.43.103
- Transmission Control Protocol, Src Port: 139, Dst Port: 48752, Seq: 0, Ack: 1, Len: 0

Timing (--Scan_delay, -T0-T5, -ttl)

Most IDS's only alert on threshold level of scans takes place. For instance, Snort on the default setting only alerts on scans when 15 or more ports are scanned per second. If we can slow down the speed of our scan, it can go right past the IDS without alerting the administrator.

Using the `--scan_delay` We can set the minimum amount of time between each probe that nmap sends to the target.

```
nmap -sS --scan_delay 5s Target
```

We can also use the built in `-T` timing switch to slow down our scan

```
nmap -sS -T0 Target
```

```
nmap -sS --ttl <value> Target
```

`ttl` is useful if you are in a slow network and you don't want your scan to time out early.

`ttl` sets the IPv4 time-to-live field in sent packets to the given value in milliseconds.

Changing Data length

Some firewalls and IDS's have signatures of nmap scans based upon the length of the packet. These signatures include the default data length of nmap's scanning packets. These packets are generally very small (TCP scan is 40 bytes and an ICMP scan is just 28 bytes). If we can change the length of these packets by appending random data to it we can at least get past this signature component and may be able to get past the

IDS to the network.

By choosing a data length other than the default, nmap will pad the packet so that it doesn't look like a typical scanning packet and hopefully, more like a legitimate packet.

Before

The image shows a terminal window on the left and a Wireshark packet capture window on the right. The terminal window displays the output of an Nmap scan performed on 192.168.43.103. The scan report indicates that the host is up and lists several open ports: 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), and 5357/tcp (wsdapi). The Wireshark window shows a list of captured packets. Packet 4043 is selected, and its details are expanded, showing the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The size of the frame is highlighted as 58 bytes on wire.

```
Nmap done: 1 IP address (1 host up) scanned
[root@parrot]~# nmap -sS 192.168.43.103

Starting Nmap 7.40 ( https://nmap.org ) at
Nmap scan report for Virus (192.168.43.103)
Host is up (0.00053s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrcpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsdapi
```

No.	Time	Source
4041	85.077127564	192.168.43.
4042	85.085003466	192.168.43.
4043	85.085121343	192.168.43.
4044	85.085189301	192.168.43.
4045	85.088012735	192.168.43.
4046	85.088305940	192.168.43.

Frame 4043: 58 bytes on wire (46 bytes captured)

Ethernet II, Src: PcsCompu...

Internet Protocol Version 4, Src...

Transmission Control Protocol, S...

After Adding `--data-length 120` $58+120=178$

```
Nmap done: 1 IP address (1 host up) scanned
(root@parrot)~# #nmap -sS --data-length 120 192.168.43
Starting Nmap 7.40 ( https://nmap.org ) at
Nmap scan report for Virus (192.168.43.103)
Host is up (0.00073s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
```

The image shows a Kali Linux terminal window on the left and a Wireshark network traffic analysis window on the right.

Terminal Window:

```

Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal  X Parrot Terminal  X Parrot Terminal  X Parrot Terminal

~[root@parrot]-[~]
-- #nmap -sS --data-length 1488 192.168.43.103
ARNING: Payloads bigger than 1488 bytes may not be sent successfully.

tarting Nmap 7.40 ( https://nmap.org ) at 2017-08-27 05:20 EDT
map scan report for Virus (192.168.43.103)
ost is up (0.00056s latency).
ot shown: 996 filtered ports
ORT      STATE SERVICE
35/tcp   open  msspc
39/tcp   open  netbios-ssn
45/tcp   open  microsoft-ds
357/tcp  open  wsddapi
AC Address:

map done: 1 IP address (1 host up) scanned in 12.15 seconds
~[root@parrot]-[~]

```

Wireshark Window:

The Wireshark window shows a packet capture of a TCP connection. The packet list pane on the left shows a single packet (No. 2952) from 192.168.43.185 to 192.168.43.103, destination port 1488. The packet details pane on the right shows the TCP header with source port 1488 and destination port 55778. The packet bytes pane on the right shows the raw data of the packet.

Transmission Unit (--mtu)

mtu of 16. The Maximum Transmission Unit (mtu) must be a multiple of eight (8,16,24,32. . .).

```
nmap -sS --mtu 24 Target
```

Scan with Random Order (--randomize-hosts)

Shuffles each group of up to 16384 hosts before it scans them. This technique combined with slow timing options in nmap can be very effective when you don't want to alert firewall.

```
nmap --randomize-hosts 192.168.1.60-74
```

Sending Bad Checksums (--badsum)

Checksums are used by the TCP/IP protocol to ensure the data integrity. By sending packets with incorrect checksums can help you to discover information from systems, Because Some firewall or IDS will respond if they are not properly configured.

```
nmap -sS --badsum Target
```

Using Multiple Techniques

To make sure that your scans are not detected, you may want to use several of these techniques combined. For instance, you

may want to slow the scan to T1, fragment the packets (-f), lengthen the packet to 1200 bytes, use proxies, such as this;

```
nmap -sS -T1 -f --badsum --data-length 1200 --proxies  
sock4://176.57.216.214:80,http://213.85.92.10:80 Target
```

Scans, such as this, will be very slow, but nearly undetectable.

Countermeasures:

- Configure IDS, IPS & Firewall Properly
- Manage system, IDS, IPS logs
- Filter inbound ICMP Request & Response
- Filter all outbound ICMP type 3 unreachable messages
- Check how IDS Reacts on heavy traffic & handles fragmented IP packets
- Be aware of all Evasion techniques & bypass techniques
- Perform Scanning From Internet to your system & check available ports
- Monitor traffic

Tools:

- Nmap
- Wireshark
- EtherApe

References

Etutorials.org

Hackers-arise

Best Open Source IDS

By [Himanshu](#) - [September 27, 2017](#)

Ph?n ?ng: ☐ funny (0) ☐ interesting (0) ☐ cool (0)



Labels: [Badsum](#), [Decoy scan](#), [Evasion Techniques](#), [Firewall Evasion Countermeasures](#), [frag](#), [MAC Spoofing](#), [mtu](#), [Proxy scan](#), [scan-delay](#)

1 comment

Google+



Add a comment

Top comments ▾



Himanshu shared this via Google+ 8 months ago - Shared publicly

+1 · Reply

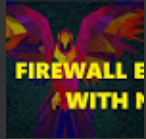
[Newer Post](#)

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)

Popular Posts



IDS, IPS AND FIREWALL EVASION USING NMAP

NIDS – Network Intrusion Detection System • It Uses a network tap, span port, or hub to collect packets on the network • Attempts t...



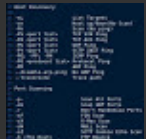
INCIDENT RESPONSE PLAN

An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information...



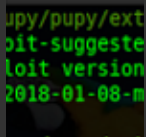
INSTALLING PRESISTENCE BACKDOOR IN WINDOWS

USING METASPLOIT windows/local/s4u_persistence
windows/local/vss_persistence
windows/local/registry_persistence windows/manage...



NMAP CHEAT SHEET

Target Specification 192. 168. 100. 1-50 IP Range 192. 168. 100. 1/24 CIDR Spec. -iL Filename IP Addr File -iR...



WINDOWS-EXPLOIT-SUGGESTER

./windows-exploit-suggester.py --update This will download latest ms bulletin xls file pip install xlrd --upgrade to download xl...



PUPY (RAT, POST EXPLOITATION TOOL)

Installing pupy git clone
<https://github.com/n1nj4sec/pupy.git> pupy cd pupy git
submodule init git submodule update pip install -r pu...

Exploit Office 2016 using CVE-2018-0802



If you don't have Empire download from here Just
run `./setup/install.sh` to install Also Download Exploit for
CVE-2018-0802 Cr...

Comment

Technology Redefine. Simple theme. Powered by [Blogger](#).