Evasion Report for 192.168.1.113

Generated: 2025-09-01 14:52:40

Port Summary

Port	Final State	Notes

| 22 | open | Opened according to ACK |

| 53 | closed | |

| 80 | open | Opened according to NMAP |

| 139 | open | Opened according to ACK |

| 443 | open | Opened according to NMAP |

| 445 | open | Opened according to ACK |

| 3389 | closed | |

| 50000 | closed | |

Overview

This report documents firewall/IDS/IPS evasion tests, the exact commands executed, and observed outcomes.

Executed Steps and Results

1. TCP ACK scan (firewall rule mapping)

- **Tool**: nmap
- **Command**: `nmap 192.168.1.113 -n -Pn -p 22,80,445,139,443,3389,53 -sA`
- **Why this step**: Map stateful filtering: ACK reveals filtered vs unfiltered without opening connections.
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: unfiltered=7

Output (stdout)

~~~~
``` Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 14:12 +01 Nmap scan report for 192.168.1.113 Host is up (0.0024s latency). PORT STATE SERVICE 22/tcp unfiltered ssh 53/tcp unfiltered domain 80/tcp unfiltered http 139/tcp unfiltered netbios-ssn 443/tcp unfiltered https 445/tcp unfiltered microsoft-ds 3389/tcp unfiltered ms-wbt-server MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds ```
~~~~

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

2. SYN scan baseline

- **Tool**: nmap
- **Command**: `nmap 192.168.1.113 -n -Pn -p 22,80,445,139,443,3389,53 -sS --scan-delay 100ms`
- **Why this step**: Establish baseline open/closed ports with stealthy SYN before evasion.
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: closed=2; open=5

Output (stdout)

~~~~
``` Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 14:12 +01 Nmap scan report for 192.168.1.113 Host is up (0.00023s latency). PORT STATE SERVICE 22/tcp open ssh 53/tcp closed domain 80/tcp open http 139/tcp open
~~~~

netbios-ssn 443/tcp open https 445/tcp open microsoft-ds 3389/tcp closed ms-wbt-server MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

3. Decoy SYN scan

- **Tool**: nmap
- **Command**: `sudo -n nmap 192.168.1.113 -p 80 -sS -Pn -n --disable-arp-ping --packet-trace -D RND:5`
- **Why this step**: If baseline hints at monitoring, use decoys to obscure scanner identity while validating reachability.
- **Status**: Failed (rc=1)
- **What happened**: No parsable Nmap port table; possibly filtered or host unreachable

Output (stderr)
``` sudo: a password is required ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

4. SYN scan with spoofed source port 53

- **Tool**: nmap
- **Command**: `sudo -n nmap 192.168.1.113 -p 50000 -sS -Pn -n --disable-arp-ping --packet-trace --source-port 53`
- **Why this step**: Test firewall trust of DNS by sending from source port 53 to traverse ACLs.
- **Status**: Failed (rc=1)
- **What happened**: No parsable Nmap port table; possibly filtered or host unreachable

Output (stderr)
``` sudo: a password is required ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

5. FIN stealth scan

- **Tool**: nmap
- **Command**: `nmap 192.168.1.113 -n -Pn -p 22,80,445,139,443,3389,53 -sF --max-retries 2 --scan-delay 150ms`
- **Why this step**: FIN probes can slip past stateless filters; closed ports should RST.
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: closed=2; open|filtered=5

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-01 14:12 +01 Nmap scan report for 192.168.1.113 Host is up (0.00037s latency). PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp closed domain 80/tcp open|filtered http 139/tcp open|filtered netbios-ssn 443/tcp open|filtered https 445/tcp open|filtered microsoft-ds 3389/tcp closed ms-wbt-server MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 3.76 seconds ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

6. NULL stealth scan

- **Tool**: nmap

- **Command**: `nmap 192.168.1.113 -n -Pn -p 22,80,445,139,443,3389,53 -sN --max-retries 2 --scan-delay 150ms`

- **Why this step**: NULL probes can bypass simplistic detection; closed ports RST.

- **Status**: Success (rc=0)

- **What happened**: Nmap parsed states: closed=2; open|filtered=5

Output (stdout)

~~~~
``` Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 14:12 +01 Nmap scan report for 192.168.1.113 Host is up
(0.0013s latency). PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp closed domain 80/tcp open|filtered http 139/
tcp open|filtered netbios-ssn 443/tcp open|filtered https 445/tcp open|filtered microsoft-ds 3389/tcp closed ms-wbt-
server MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP
address (1 host up) scanned in 3.71 seconds ```
~~~~

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

7. XMAS stealth scan

- **Tool**: nmap

- **Command**: `nmap 192.168.1.113 -n -Pn -p 22,80,445,139,443,3389,53 -sX --max-retries 2 --scan-delay 150ms`

- **Why this step**: XMAS probes test RFC compliance and filtering behavior.

- **Status**: Success (rc=0)

- **What happened**: Nmap parsed states: closed=2; open|filtered=5

Output (stdout)

~~~~
``` Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 14:12 +01 Nmap scan report for 192.168.1.113 Host is up
(0.0022s latency). PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp closed domain 80/tcp open|filtered http 139/
tcp open|filtered netbios-ssn 443/tcp open|filtered https 445/tcp open|filtered microsoft-ds 3389/tcp closed ms-wbt-
server MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP
address (1 host up) scanned in 4.23 seconds ```
~~~~

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

8. Packet fragmentation

- **Tool**: nmap

- **Command**: `nmap 192.168.1.113 -n -Pn -p 22,80,445,139,443,3389,53 -sS -f --mtu 16 -T0`

- **Why this step**: Fragment TCP headers to evade stateless ACLs and signature-based IDS.

- **Status**: Success (rc=0)

- **What happened**: Nmap parsed states: closed=2; open=5

Output (stdout)

~~~~
``` Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 14:12 +01 Nmap scan report for 192.168.1.113 Host is up
(0.00073s latency). PORT STATE SERVICE 22/tcp open ssh 53/tcp closed domain 80/tcp open http 139/tcp open
netbios-ssn 443/tcp open https 445/tcp open microsoft-ds 3389/tcp closed ms-wbt-server MAC Address:
08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned
in 2400.47 seconds ```
~~~~

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

9. DNS version.bind (CHAOS)

- **Tool**: dig

- **Command**: `dig @192.168.1.113 version.bind CHAOS TXT`

- **Why this step**: If DNS responds, reveal BIND version to assess defense stack exposure.

- **Status**: Failed (rc=9)

- **What happened**: DNS CHAOS query failed (no DNS reachable on target)

Output (stdout)

```
;; communications error to 192.168.1.113#53: connection refused ;; communications error to 192.168.1.113#53: connection refused ;; communications error to 192.168.1.113#53: connection refused ; <<>> DiG 9.20.9-1-Debian <<>> @192.168.1.113 version.bind CHAOS TXT ; (1 server found) ;; global options: +cmd ;; no servers could be reached
```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

10. nc validate from source port 53

- **Tool**: ncat
- **Command**: `ncat -nv --source-port 53 192.168.1.113 50000`
- **Why this step**: Validate port accessibility using DNS-like source port to confirm Nmap findings.
- **Status**: Failed (rc=1)
- **What happened**: Netcat refused (port closed but reachable)

Output (stderr)

```
Ncat: Version 7.95 ( https://nmap.org/ncat ) Ncat: Connection refused.
```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

11. proxychains nmap TCP connect

- **Tool**: proxychains,nmap
- **Command**: `proxychains nmap -sT -Pn -p 80,443 192.168.1.113`
- **Why this step**: Demonstrate scanning via proxies to bypass IP-based blocks/EDR egress rules.
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: open=2

Output (stdout)

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 14:52 +01 Nmap scan report for 192.168.1.113 (192.168.1.113) Host is up (0.00093s latency). PORT STATE SERVICE 80/tcp open http 443/tcp open https Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Output (stderr)

```
[proxychains] config file found: /etc/proxychains4.conf [proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4 [proxychains] DLL init: proxychains-ng 4.17 [proxychains] DLL init: proxychains-ng 4.17 [proxychains] DLL init: proxychains-ng 4.17
```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

12. FIN stealth scan (focused)

- **Tool**: nmap
- **Command**: `nmap 192.168.1.113 -n -Pn -p 50000 -sF --max-retries 1 --scan-delay 200ms`
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: closed=1

Output (stdout)

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 14:52 +01 Nmap scan report for 192.168.1.113 Host is up (0.00021s latency). PORT STATE SERVICE 50000/tcp closed ibm-db2 MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

13. NULL stealth scan (focused)

- **Tool**: nmap
- **Command**: `nmap 192.168.1.113 -n -Pn -p 50000 -sN --max-retries 1 --scan-delay 200ms`
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: closed=1

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-01 14:52 +01 Nmap scan report for 192.168.1.113 Host is up (0.00050s latency). PORT STATE SERVICE 50000/tcp closed ibm-db2 MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

14. XMAS stealth scan (focused)

- **Tool**: nmap
- **Command**: `nmap 192.168.1.113 -n -Pn -p 50000 -sX --max-retries 1 --scan-delay 200ms`
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: closed=1

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-01 14:52 +01 Nmap scan report for 192.168.1.113 Host is up (0.0038s latency). PORT STATE SERVICE 50000/tcp closed ibm-db2 MAC Address: 08:00:27:AB:58:94 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

15. nc PoC from source port 53 to 22

- **Tool**: ncat
- **Command**: `printf 'HEAD / HTTP/1.0

' | ncat -nv --source-port 53 192.168.1.113 22`

- **Status**: Success (rc=0)
- **What happened**: Netcat did not establish a connection

Output (stdout)
``` HEAD / HTTP/1.0 ```
Output (stderr)
``` printf: warning: ignoring excess arguments, starting with '|' ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

16. nc PoC from source port 53 to 80

- **Tool**: ncat
- **Command**: `printf 'HEAD / HTTP/1.0

' | ncat -nv --source-port 53 192.168.1.113 80`

- **Status**: Success (rc=0)
- **What happened**: Netcat did not establish a connection

Output (stdout)
``` HEAD / HTTP/1.0 ```
Output (stderr)

``` printf: warning: ignoring excess arguments, starting with ‘|’ ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

17. nc PoC from source port 53 to 139

- **Tool**: ncat

- **Command**: `printf 'HEAD / HTTP/1.0

' | ncat -nv --source-port 53 192.168.1.113 139`

- **Status**: Success (rc=0)

- **What happened**: Netcat did not establish a connection

Output (stdout)
``` HEAD / HTTP/1.0 ```
Output (stderr)
``` printf: warning: ignoring excess arguments, starting with ‘|’ ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

18. nc PoC from source port 53 to 443

- **Tool**: ncat

- **Command**: `printf 'HEAD / HTTP/1.0

' | ncat -nv --source-port 53 192.168.1.113 443`

- **Status**: Success (rc=0)

- **What happened**: Netcat did not establish a connection

Output (stdout)
``` HEAD / HTTP/1.0 ```
Output (stderr)
``` printf: warning: ignoring excess arguments, starting with ‘|’ ```

- **Next decision**: If results suggest filtering (filtered/timeouts), escalate to the next stealth technique; otherwise, keep baseline.

19. nc PoC from source port 53 to 445

- **Tool**: ncat

- **Command**: `printf 'HEAD / HTTP/1.0

' | ncat -nv --source-port 53 192.168.1.113 445`

- **Status**: Success (rc=0)

- **What happened**: Netcat did not establish a connection

Output (stdout)
``` HEAD / HTTP/1.0 ```
Output (stderr)
``` printf: warning: ignoring excess arguments, starting with ‘|’ ```

Techniques Reference

Firewall evasion by Nmap

- Use `-sA` (ACK) to map filtering vs. `-sS` (SYN) baseline.
- Decoys with `-D RND:<n>`; fragmentation `-f`/`--mtu`.
- Spoof DNS source with `--source-port 53`; try FIN/NULL/XMAS.
- Optional `-S <ip> -e <iface>` for source IP spoofing (where supported).
- Slow timing `-T0`/`-T1`, `--scan-delay` to reduce detection.

IDS/IPS detection strategy

- Vary sources (multiple VPS), observe blocks; use decoys or idle scans.
- Throttle probes, randomize order, and split port ranges.

Proxying

- `proxychains nmap -sT -Pn -p 80,443 <target>` to route via SOCKS/HTTP proxies.

Validation via Netcat

- `ncat -nv --source-port 53 <target> <port>` to confirm server behavior.