Evasion Report for 10.3.2.1

Generated: 2025-09-03 23:04:13

Port Summary

Port	Final State	Notes

| 22 | filtered | |

| 53 | filtered | |

| 80 | filtered | |

| 139 | filtered | |

| 443 | filtered | |

| 445 | filtered | |

| 3389 | filtered | |

| 50000 | unknown | |

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 10.3.2.1 -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: filtered=7

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 21:48 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp filtered ssh 53/tcp filtered domain 80/tcp filtered http 139/tcp filtered netbios-ssn 443/tcp filtered https 445/tcp filtered microsoft-ds 3389/tcp filtered ms-wbt-server Nmap done: 1 IP address (1 host up) scanned in 3.19 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 10.3.2.1 -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: filtered=7

Output (stdout)
``` Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 21:48 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp filtered ssh 53/tcp filtered domain 80/tcp filtered http 139/tcp filtered netbios-ssn 443/tcp

filtered https 445/tcp filtered microsoft-ds 3389/tcp filtered ms-wbt-server Nmap done: 1 IP address (1 host up) scanned in 3.93 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 10.3.2.1 -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 10.3.2.1 -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 10.3.2.1 -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: open|filtered=7

Output (stdout)
``` Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 21:48 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp open|filtered 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 open|filtered ms-wbt-server 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.

### 6. NULL stealth scan

- **Tool**: nmap
- **Command**: `nmap 10.3.2.1 -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: open|filtered=7

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 21:48 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp open|filtered 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 open|filtered ms-wbt-server 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.

7. XMAS stealth scan

- **Tool**: nmap
- **Command**: `nmap 10.3.2.1 -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: open|filtered=7

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 21:48 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp open|filtered 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 open|filtered ms-wbt-server Nmap done: 1 IP address (1 host up) scanned in 4.20 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 10.3.2.1 -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: filtered=7

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 21:48 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp filtered ssh 53/tcp filtered domain 80/tcp filtered http 139/tcp filtered netbios-ssn 443/tcp filtered https 445/tcp filtered microsoft-ds 3389/tcp filtered ms-wbt-server Nmap done: 1 IP address (1 host up) scanned in 4502.69 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 @10.3.2.1 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 10.3.2.1#53: timed out ;; communications error to 10.3.2.1#53: timed out ;; communications error to 10.3.2.1#53: timed out ; <<>> DiG 9.20.9-1-Debian <<>> @10.3.2.1 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 10.3.2.1 50000`
- **Why this step**: Validate port accessibility using DNS-like source port to confirm Nmap findings.
- **Status**: Failed (rc=1)
- **What happened**: Netcat timed out (likely filtered)

Output (stderr)
``` Ncat: Version 7.95 (https://nmap.org/ncat) Ncat: TIMEOUT. ```

- **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 10.3.2.1`
- **Why this step**: Demonstrate scanning via proxies to bypass IP-based blocks/EDR egress rules.
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: filtered=2

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 23:03 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 80/tcp filtered http 443/tcp filtered https Nmap done: 1 IP address (1 host up) scanned in 3.08 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. SYN from source port 53 on filtered ports

- **Tool**: nmap
- **Command**: `sudo -n nmap 10.3.2.1 -p 22,53,80,139,443,445,3389 -sS -Pn -n --disable-arp-ping --packet-trace --source-port 53`
- **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.

13. FIN stealth scan (focused)

- **Tool**: nmap
- **Command**: `nmap 10.3.2.1 -n -Pn -p 22,53,80,139,443,445,3389,50000 -sF --max-retries 1 --scan-delay 200ms`
```

- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: open|filtered=8

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 23:03 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp open|filtered 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 open|filtered ms-wbt-server 50000/tcp open|filtered ibm-db2 Nmap done: 1 IP address (1 host up) scanned in 5.79 seconds ```

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

14. NULL stealth scan (focused)

- **Tool**: nmap
- **Command**: `nmap 10.3.2.1 -n -Pn -p 22,53,80,139,443,445,3389,50000 -sN --max-retries 1 --scan-delay 200ms`
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: open|filtered=8

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 23:04 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp open|filtered 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 open|filtered ms-wbt-server 50000/tcp open|filtered ibm-db2 Nmap done: 1 IP address (1 host up) scanned in 5.74 seconds ```

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

15. XMAS stealth scan (focused)

- **Tool**: nmap
- **Command**: `nmap 10.3.2.1 -n -Pn -p 22,53,80,139,443,445,3389,50000 -sX --max-retries 1 --scan-delay 200ms`
- **Status**: Success (rc=0)
- **What happened**: Nmap parsed states: open|filtered=8

Output (stdout)
``` Starting Nmap 7.95 (https://nmap.org) at 2025-09-03 23:04 +01 Nmap scan report for 10.3.2.1 Host is up. PORT STATE SERVICE 22/tcp open|filtered ssh 53/tcp open|filtered 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 open|filtered ms-wbt-server 50000/tcp open|filtered ibm-db2 Nmap done: 1 IP address (1 host up) scanned in 5.80 seconds ```

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.