

1. Overview

This room focuses on advanced Nmap scanning techniques. You will learn about different types of scans, service and OS detection, firewall evasion, and the use of the Nmap Scripting Engine (NSE).

2. Environment Setup

- Platform: TryHackMe
- Tools: Nmap, Linux Terminal (Kali/AttackBox)
- Target: Deployed machine from the TryHackMe room (IP: 10.10.139.119)

3. Tasks Summary

Task 1: Basic Scan

Command: `nmap 10.10.139.119`

Description: Finds open ports on the target.

Task 2: Service Detection

Command: `nmap -sV 10.10.139.119`

Description: Identifies services and versions running on the open ports.

Task 3: Aggressive Scan

Command: `nmap -A 10.10.139.119`

Description: Performs OS detection, version detection, script scanning, and traceroute.

Task 4: HTTP Title Script

Command: `nmap --script=http-title -p 80 10.10.139.119`

Description: Retrieves the web page title running on port 80.

Task 5: Vulnerability Scan

Command: `nmap --script=vuln 10.10.139.119`

Description: Runs Nmap scripts that check for known vulnerabilities.

4. Key Findings

- SSH and HTTP ports are open.
- Apache HTTP server and OpenSSH detected.
- Web server page title found using the `http-title` script.
- No major vulnerabilities detected from the scan.
- Target operating system appears to be Linux-based.

SCREENSHOTS:

```
(kali@kali)~$ cd /usr/share/nmap/scripts
(kali@kali)~/usr/share/nmap/scripts$ ls
acarsd-info.nse      hostmap-crtsh.nse      ip-geolocation-map-bing.nse  rsa-vuln-roca.nse
address-info.nse    hostmap-robotx.nse     ip-geolocation-map-google.nse  rsync-brute.nse
afp-brute.nse        http-adobe-coldfusion-apsal301.nse  ip-geolocation-map-kml.nse    rsync-list-modules.nse
afp-ls.nse           http-affiliate-id.nse   ip-geolocation-maxmind.nse    rtsp-methods.nse
afp-path-vuln.nse    http-apache-negotiation.nse  ip-https-discover.nse        rtsp-url-brute.nse
afp-serverinfo.nse   http-apache-server-status.nse  ipidseq.nse                  rusers.nse
afp-showmount.nse    http-asnnet-debug.nse     ipmi-brute.nse               s7-info.nse
ajp-auth.nse         http-auth-finder.nse      ipmi-cipher-zero.nse        samba-vuln-cve-2012-1182.nse
ajp-brute.nse        http-auth.nse            ipmi-version.nse             script.db
ajp-headers.nse      http-avaya-ipoffice-users.nse  ipv6-multicast-mld-list.nse  servicetags.nse
ajp-methods.nse      http-awstatstotals-exec.nse  ipv6-node-info.nse          shodan-api.nse
ajp-request.nse      http-axis2-dir-traversal.nse  ipv6-ra-flood.nse           sip-brute.nse
allseeingeye-info.nse  http-backup-finder.nse      irc-hotnet-channels.nse     sip-call-spoof.nse
amqp-info.nse         http-barracuda-dir-traversal.nse  irc-brute.nse               sip-enum-users.nse
asn-query.nse         http-bigip-cookie.nse       irc-info.nse                 sip-methods.nse
auth-owners.nse      http-brute.nse             irc-sasl-brute.nse          skypev2-version.nse
auth-spoof.nse       http-cakephp-version.nse     irc-unrealircd-backdoor.nse  smb2-capabilities.nse
backorifice-brute.nse http-chrono.nse             iscsi-brute.nse             smb2-security-mode.nse
backorifice-info.nse http-cisco-anyconnect.nse    iscsi-info.nse              smb2-time.nse
bacnet-info.nse      http-coldfusion-subzero.nse  isns-info.nse               smb2-vuln-uptime.nse
banner.nse           http-comments-displayer.nse  jdwp-exec.nse               smb-brute.nse
bitcoin-getaddr.nse  http-config-backup.nse      jdwp-info.nse               smb-double-pulsar-backdoor.nse
bitcoin-info.nse     http-cors.nse               jdwp-inject.nse             smb-enum-domains.nse
bitcoindrpc-info.nse http-date.nse               jdwp-version.nse            smb-enum-groups.nse
bittorrent-discovery.nse http-cross-domain-policy.nse  knx-gateway-discover.nse     smb-enum-processes.nse
bjnp-discover.nse   http-csrf.nse              knx-gateway-info.nse        smb-enum-services.nse
broadcast-ataoe-discover.nse http-default-accounts.nse  krb5-enum-users.nse         smb-enum-sessions.nse
broadcast-avahi-dos.nse http-devframework.nse      ldap-brute.nse              smb-enum-shares.nse
broadcast-bjnp-discover.nse http-dlink-backdoor.nse    ldap-novell-getpass.nse     smb-enum-users.nse
broadcast-db2-discover.nse http-dmbased-xss.nse       ldap-rootse.nse             smb-flood.nse
broadcast-dhcp6-discover.nse http-domino-enum-passwords.nse  ldap-search.nse            smb-ls.nse
broadcast-dhcp-discover.nse http-drupal-enum.nse        lexmark-config.nse          smb-mbenum.nse
broadcast-dns-service-discovery.nse http-drupal-enum-users.nse  llmnr-resolve.nse          smb-os-discovery.nse
broadcast-dropbox-listener.nse http-enum.nse              llttd-discovery.nse         smb-print-text.nse
broadcast-eigrp-discovery.nse                                     lu-enum.nse                 smb-protocols.nse

(kali@kali)~/usr/share/nmap/scripts$ sudo nmap -Pn -sX -vv -p 1-999 10.10.139.119
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 11:52 EDT
Initiating Parallel DNS resolution of 1 host. at 11:52
Completed Parallel DNS resolution of 1 host. at 11:52, 0.00s elapsed
Initiating XMAS Scan at 11:52
Scanning 10.10.139.119 [999 ports]
XMAS Scan Timing: About 15.52% done; ETC: 11:55 (0:02:49 remaining)
XMAS Scan Timing: About 29.88% done; ETC: 11:55 (0:02:23 remaining)
XMAS Scan Timing: About 44.89% done; ETC: 11:55 (0:01:52 remaining)
XMAS Scan Timing: About 59.91% done; ETC: 11:55 (0:01:21 remaining)
XMAS Scan Timing: About 74.92% done; ETC: 11:55 (0:00:51 remaining)
Completed XMAS Scan at 11:55, 201.26s elapsed (999 total ports)
Nmap scan report for 10.10.139.119
Host is up, received user-set.
Scanned at 2025-08-08 11:52:26 EDT for 202s
All 999 scanned ports on 10.10.139.119 are in ignored states.
Not shown: 999 open|filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.35 seconds
Raw packets sent: 1998 (79.920KB) | Rcvd: 0 (0B)

(kali@kali)~/usr/share/nmap/scripts$
```

```
kali@kali: /usr/share/nmap/scripts
$ cd /usr/share/nmap/scripts
(kali@kali)-[/usr/share/nmap/scripts]
$ ls
acarsd-info.nse      hostmap-crtsh.nse      ip-geolocation-map-bing.nse  rsa-vuln-roca.nse
address-info.nse     hostmap-robtx.nse      ip-geolocation-map-google.nse  rsync-brute.nse
afp-brute.nse         http-adobe-coldfusion-apsa1301.nse  ip-geolocation-map-kml.nse    rsync-list-modules.nse
afp-ls.nse            http-affiliate-id.nse   ip-geolocation-maxmind.nse     rtsp-methods.nse
afp-path-vuln.nse     http-apache-negotiation.nse  ip-https-discover.nse         rtsp-url-brute.nse
afp-serverinfo.nse    http-apache-server-status.nse  ipidseq.nse                    rusers.nse
afp-showmount.nse     http-asnmap-debug.nse      ipmi-brute.nse                 s7-info.nse
afp-auth.nse          http-auth-finder.nse       ipmi-cipher-zero.nse          samba-vuln-cve-2012-1182.nse
ajp-brute.nse         http-auth.nse            ipmi-version.nse               script.db
ajp-headers.nse       http-avaya-ipoffice-users.nse  ipv6-multicast-mld-list.nse    servicetags.nse
ajp-methods.nse       http-awstats-totals-exec.nse  ipv6-node-info.nse            shodan-api.nse
ajp-request.nse       http-aws2-dir-traversal.nse   ipv6-ra-flood.nse             sip-brute.nse
allseeingeye-info.nse http-backup-finder.nse       irc-hotnet-channels.nse        sip-call-spoof.nse
amqp-info.nse         http-barracuda-dir-traversal.nse  irc-brute.nse                  sip-enum-users.nse
asn-query.nse         http-bigip-cookie.nse        irc-info.nse                    sip-methods.nse
auth-owners.nse       http-brute.nse              irc-sasl-brute.nse              skypev2-version.nse
auth-spoof.nse        http-cakephp-version.nse      irc-unrealircd-backdoor.nse    smb2-capabilities.nse
backorifice-brute.nse http-chrono.nse              iscsi-brute.nse                 smb2-security-mode.nse
backorifice-info.nse  http-cisco-anyconnect.nse     iscsi-info.nse                 smb2-time.nse
bacnet-info.nse       http-coldfusion-subzero.nse   isns-info.nse                  smb2-vuln-uptime.nse
banner.nse            http-comments-displayer.nse   jdwp-exec.nse                  smb-brute.nse
bitcoin-getaddr.nse   http-config-backup.nse       jdwp-info.nse                  smb-double-pulsar-backdoor.nse
bitcoin-info.nse      http-cookie-flags.nse        jdwp-inject.nse                smb-enum-domains.nse
bitcoinnrpc-info.nse  http-cors.nse                jdwp-version.nse               smb-enum-groups.nse
bittorrent-discovery.nse http-cross-domain-policy.nse  knx-gateway-discover.nse       smb-enum-processes.nse
bjnp-discover.nse     http-csrf.nse                knx-gateway-info.nse           smb-enum-services.nse
broadcast-ataoe-discover.nse http-date.nse                krb5-enum-users.nse            smb-enum-sessions.nse
broadcast-avahi-dos.nse http-default-accounts.nse    ldap-brute.nse                 smb-enum-shares.nse
broadcast-bjnp-discover.nse http-devframework.nse       ldap-novell-getpass.nse        smb-enum-users.nse
broadcast-db2-discover.nse http-dlink-backdoor.nse     ldap-rootdse.nse               smb-flood.nse
broadcast-dhcp6-discover.nse http-dombased-xss.nse       ldap-search.nse                smb-ls.nse
broadcast-dhcp-discover.nse http-domino-enum-passwords.nse  lexmark-config.nse             smb-mbenum.nse
broadcast-dns-service-discovery.nse http-drupal-enum.nse        llmnr-resolve.nse              smb-os-discovery.nse
broadcast-dropbox-listener.nse http-drupal-enum-users.nse   llttd-discovery.nse            smb-print-text.nse
broadcast-eigrp-discovery.nse http-enum.nse                lu-enum.nse                     smb-protocols.nse
```

```
kali@kali: /usr/share/nmap/scripts
$ grep 'smb' script.db
Entry { filename = "smb-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "smb-double-pulsar-backdoor.nse", categories = { "malware", "safe", "vuln", } }
Entry { filename = "smb-enum-domains.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-groups.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-processes.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-services.nse", categories = { "discovery", "intrusive", "safe", } }
Entry { filename = "smb-enum-sessions.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-shares.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-users.nse", categories = { "auth", "intrusive", } }
Entry { filename = "smb-flood.nse", categories = { "dos", "intrusive", } }
Entry { filename = "smb-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-mbenum.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-os-discovery.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb-print-text.nse", categories = { "intrusive", } }
Entry { filename = "smb-protocols.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-psexec.nse", categories = { "intrusive", } }
Entry { filename = "smb-security-mode.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb-server-stats.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-system-info.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-vuln-conficker.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve-2017-7494.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve2009-3103.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms06-025.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms07-029.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms08-067.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-054.nse", categories = { "dos", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-061.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms17-010.nse", categories = { "safe", "vuln", } }
Entry { filename = "smb-vuln-regsvcs-dos.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-webexec.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-webexec-exploit.nse", categories = { "exploit", "intrusive", } }
Entry { filename = "smb2-capabilities.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb2-security-mode.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb2-time.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb2-vuln-uptime.nse", categories = { "safe", "vuln", } }
```


1234

TryHackMe | Nmap

tryhackme.com/room/furthernmap

Search ☆ 📄 School

Learn » Nmap



Nmap

An in depth look at scanning with nmap, a powerful network scanning tool.

🟢 Easy ⌚ 50 min

Share your achievement


Start AttackBox

Help

Save Room



19636


Options






NMAP PROJECT



Room completed (100%)



Task 1  Deploy 



Task 2  Introduction



Task 3  Nmap Switches



Task 4   Overview



Task 5   TCP Connect Scans



Task 6   SYN Scans



Task 7   UDP Scans


Task 8   NULL, FIN and Xmas


Task 9   ICMP Network Scanning


Task 10   Overview

Task 11   Working with the NSE

Task 12   Searching for Scripts

Task 13  Firewall Evasion

Task 14  Practical

Task 15  Conclusion