NMAP Part- 2

Firewall invasion (Decoys, MTU & Fragmentation)

There are two techniques to evading the firewalls

First way is to work with techniques like spoofing using decoys changing the minimum transmission unit
Second is to using the decoys fragmenting packets which really does not work

Simply using decoys and showing that the ip scan is from another ip address and this can work on the internet or the local area network and spoof an ip address that belongs to an admin or a network admin

decoy scan is simply running a syn scan and service version and a fast scan
nmap -sS -sV -F -D

when we are in local network use the ip address we are willing to spoof and if we are in internet use the RND option you can check the ip which is whitelisted in the server or for the website and use that to evade the firewall

if we get RST back it means the port is open

nmap -sS -sV -F -D RND:3 10.0.2.7

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -F -D RND:3 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-21 18:39 EST
Nmap scan report for 10.0.2.7
Host is up (0.018s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login
514/tcp  open  tcpwrapped
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.85 seconds
```

Scanning with mtu (min transmission units) that is either 8,16,32,64 checking whether the packet is fragmented or not

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -F --mtu 24 --send-eth -D RND:3 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-21 18:44 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 44.44% done; ETC: 18:44 (0:00:08 remaining)
Nmap scan report for 10.0.2.7
Host is up (0.0061s latency).
Not shown: 82 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.60 seconds
```

Nmap Scripting Engine (NSE)

Nmap Scripting engine is an extremely versatile and useful tool and that is the core part of the nmap and allows users to write your own scripts and automate various types of scan and allows also to share simple scripts to automate a wide variety of networking tasks now Imp aspects of the nmap scripting engine

1. Nmap installation comes pre-loaded or pre-configured or pre=packaged with end with nmap scripts and we can find the scripts under ls -al /usr/share/nmap/scripts/

```
┌──(root㉿kali)-[/home/kali]
└─# ls -al /usr/share/nmap/scripts
total 4988
drwxr-xr-x 2 root root 32768 May 27  2024 .
drwxr-xr-x 4 root root  4096 May 27  2024 ..
-rw-r--r-- 1 root root  3901 Mar 13  2024 acarsd-info.nse
-rw-r--r-- 1 root root  8749 Mar 13  2024 address-info.nse
-rw-r--r-- 1 root root  3345 Mar 13  2024 afp-brute.nse
-rw-r--r-- 1 root root  6463 Mar 13  2024 afp-ls.nse
-rw-r--r-- 1 root root  7001 Mar 13  2024 afp-path-vuln.nse
-rw-r--r-- 1 root root  5600 Mar 13  2024 afp-serverinfo.nse
-rw-r--r-- 1 root root  2621 Mar 13  2024 afp-showmount.nse
-rw-r--r-- 1 root root  2262 Mar 13  2024 ajp-auth.nse
-rw-r--r-- 1 root root  2983 Mar 13  2024 ajp-brute.nse
-rw-r--r-- 1 root root  1329 Mar 13  2024 ajp-headers.nse
-rw-r--r-- 1 root root  2590 Mar 13  2024 ajp-methods.nse
-rw-r--r-- 1 root root  3051 Mar 13  2024 ajp-request.nse
-rw-r--r-- 1 root root  6719 Mar 13  2024 allseeingeye-info.nse
-rw-r--r-- 1 root root  1678 Mar 13  2024 amqp-info.nse
-rw-r--r-- 1 root root 15024 Mar 13  2024 asn-query.nse
-rw-r--r-- 1 root root  2054 Mar 13  2024 auth-owners.nse
-rw-r--r-- 1 root root   870 Mar 13  2024 auth-spoof.nse
-rw-r--r-- 1 root root  9050 Mar 13  2024 backorifice-brute.nse
-rw-r--r-- 1 root root 10193 Mar 13  2024 backorifice-info.nse
-rw-r--r-- 1 root root 53137 Mar 13  2024 bacnet-info.nse
-rw-r--r-- 1 root root  6136 Mar 13  2024 banner.nse
-rw-r--r-- 1 root root  2012 Mar 13  2024 bitcoin-getaddr.nse
-rw-r--r-- 1 root root  1812 Mar 13  2024 bitcoin-info.nse
-rw-r--r-- 1 root root  4437 Mar 13  2024 bitcoinrpc-info.nse
-rw-r--r-- 1 root root  4079 Mar 13  2024 bittorrent-discovery.nse
-rw-r--r-- 1 root root  1344 Mar 13  2024 bjnp-discover.nse
-rw-r--r-- 1 root root  4428 Mar 13  2024 broadcast-ataoe-discover.nse
-rw-r--r-- 1 root root  2964 Mar 13  2024 broadcast-avahi-dos.nse
-rw-r--r-- 1 root root  4786 Mar 13  2024 broadcast-bjnp-discover.nse
-rw-r--r-- 1 root root  2438 Mar 13  2024 broadcast-db2-discover.nse
-rw-r--r-- 1 root root  3217 Mar 13  2024 broadcast-dhcp6-discover.nse
-rw-r--r-- 1 root root 10151 Mar 13  2024 broadcast-dhcp-discover.nse
-rw-r--r-- 1 root root  1499 Mar 13  2024 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root  3866 Mar 13  2024 broadcast-dropbox-listener.nse
-rw-r--r-- 1 root root 12202 Mar 13  2024 broadcast-eigrp-discovery.nse
-rw-r--r-- 1 root root  3472 Mar 13  2024 broadcast-hid-discoveryd.nse
-rw-r--r-- 1 root root 14655 Mar 13  2024 broadcast-igmp-discovery.nse
-rw-r--r-- 1 root root  3184 Mar 13  2024 broadcast-jenkins-discover.nse
-rw-r--r-- 1 root root 10449 Mar 13  2024 broadcast-listener.nse
-rw-r--r-- 1 root root  3813 Mar 13  2024 broadcast-ms-sql-discover.nse
-rw-r--r-- 1 root root  1909 Mar 13  2024 broadcast-netbios-master-browser.nse
-rw-r--r-- 1 root root  2330 Mar 13  2024 broadcast-networker-discover.nse
-rw-r--r-- 1 root root  2005 Mar 13  2024 broadcast-novell-locate.nse
-rw-r--r-- 1 root root 16838 Mar 13  2024 broadcast-ospf2-discover.nse
-rw-r--r-- 1 root root  1966 Mar 13  2024 broadcast-pc-anywhere.nse
```

2. For example let us say we are checking for a particular protocol let us say for http we can use the command ls -al /usr/share/nmap/scripts | grep -e "http-enum"

```
┌──(root㉿kali)-[/home/kali]
└─# ls -al /usr/share/nmap/scripts | grep -e "http"
-rw-r--r-- 1 root root  2153 Mar 13  2024 http-adobe-coldfusion-apsa1301.nse
-rw-r--r-- 1 root root  5149 Mar 13  2024 http-affiliate-id.nse
-rw-r--r-- 1 root root  1950 Mar 13  2024 http-apache-negotiation.nse
-rw-r--r-- 1 root root  4499 Mar 13  2024 http-apache-server-status.nse
-rw-r--r-- 1 root root  1805 Mar 13  2024 http-aspnet-debug.nse
-rw-r--r-- 1 root root  3959 Mar 13  2024 http-auth-finder.nse
-rw-r--r-- 1 root root  3187 Mar 13  2024 http-auth.nse
-rw-r--r-- 1 root root  2865 Mar 13  2024 http-avaya-ipoffice-users.nse
-rw-r--r-- 1 root root  4372 Mar 13  2024 http-awstatstotals-exec.nse
-rw-r--r-- 1 root root  6872 Mar 13  2024 http-axis2-dir-traversal.nse
-rw-r--r-- 1 root root  5484 Mar 13  2024 http-backup-finder.nse
-rw-r--r-- 1 root root  6387 Mar 13  2024 http-barracuda-dir-traversal.nse
-rw-r--r-- 1 root root  2038 Mar 13  2024 http-bigip-cookie.nse
-rw-r--r-- 1 root root  4920 Mar 13  2024 http-brute.nse
-rw-r--r-- 1 root root  4436 Mar 13  2024 http-cakephp-version.nse
-rw-r--r-- 1 root root  4927 Mar 13  2024 http-chrono.nse
-rw-r--r-- 1 root root  1695 Mar 13  2024 http-cisco-anyconnect.nse
-rw-r--r-- 1 root root  5520 Mar 13  2024 http-coldfusion-subzero.nse
-rw-r--r-- 1 root root  4150 Mar 13  2024 http-comments-displayer.nse
-rw-r--r-- 1 root root  7251 Mar 13  2024 http-config-backup.nse
-rw-r--r-- 1 root root  5139 Mar 13  2024 http-cookie-flags.nse
-rw-r--r-- 1 root root  2577 Mar 13  2024 http-cors.nse
-rw-r--r-- 1 root root 13803 Mar 13  2024 http-cross-domain-policy.nse
-rw-r--r-- 1 root root  5418 Mar 13  2024 http-csrf.nse
-rw-r--r-- 1 root root  1718 Mar 13  2024 http-date.nse
-rw-r--r-- 1 root root 17392 Mar 13  2024 http-default-accounts.nse
-rw-r--r-- 1 root root  4288 Mar 13  2024 http-devframework.nse
-rw-r--r-- 1 root root  2529 Mar 13  2024 http-dlink-backdoor.nse
-rw-r--r-- 1 root root  4452 Mar 13  2024 http-dombased-xss.nse
-rw-r--r-- 1 root root 13893 Mar 13  2024 http-domino-enum-passwords.nse
-rw-r--r-- 1 root root  6931 Mar 13  2024 http-drupal-enum.nse
-rw-r--r-- 1 root root  2256 Mar 13  2024 http-drupal-enum-users.nse
-rw-r--r-- 1 root root 20667 Mar 13  2024 http-enum.nse
-rw-r--r-- 1 root root  3347 Mar 13  2024 http-errors.nse
-rw-r--r-- 1 root root 20413 Mar 13  2024 http-exif-spider.nse
-rw-r--r-- 1 root root  5199 Mar 13  2024 http-favicon.nse
-rw-r--r-- 1 root root  4451 Mar 13  2024 http-feed.nse
-rw-r--r-- 1 root root  9076 Mar 13  2024 http-fetch.nse
-rw-r--r-- 1 root root 11327 Mar 13  2024 http-fileupload-exploiter.nse
-rw-r--r-- 1 root root 21101 Mar 13  2024 http-form-brute.nse
-rw-r--r-- 1 root root  7934 Mar 13  2024 http-form-fuzzer.nse
-rw-r--r-- 1 root root  2739 Mar 13  2024 http-frontpage-login.nse
-rw-r--r-- 1 root root  2164 Mar 13  2024 http-generator.nse
-rw-r--r-- 1 root root 12100 Mar 13  2024 http-git.nse
-rw-r--r-- 1 root root  3195 Mar 13  2024 http-gitweb-projects-enum.nse
-rw-r--r-- 1 root root  3381 Mar 13  2024 http-google-malware.nse
-rw-r--r-- 1 root root 11692 Mar 13  2024 http-grep.nse
-rw-r--r-- 1 root root  1797 Mar 13  2024 http-headers.nse
-rw-r--r-- 1 root root  3383 Mar 13  2024 http-hp-ilo-info.nse
```

If for http-enum script then

```
┌──(root㉿kali)-[/home/kali]
└─# ls -al /usr/share/nmap/scripts | grep -e "http-enum"
-rw-r--r-- 1 root root 20667 Mar 13  2024 http-enum.nse

┌──(root㉿kali)-[/home/kali]
└─#
```

Nmap NSE-Syntax

Updating the script database is important for efficiency
sudo nmap --script-updatedb

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script-updatedb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-24 09:08 EST
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.83 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

sending a ping scan to the target system and check whether it is up or not is very important and a service version detection on it
-sn and -sV

we can use the grep command to short the nmap

ls -al /usr/share/nmap/scripts/ | grep -e "ftp"

syntax is :
nmap -p "port_number" --script "script_name1","script_name2" "target_ip_address"

Banner Grabbing

Banner Grabbing is the process of essentially identifying the service version currently running on a particular getting the banner of the service of the piece of software or the service version that is running

There is a nmap script for banner

nmap -p22,80 --script banner "target_ip"

```
└─# nmap -p 22,80 --script banner 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-24 09:36 EST
Nmap scan report for 10.0.2.7
Host is up (0.0014s latency).

PORT   STATE SERVICE
22/tcp open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
80/tcp open  http
MAC Address: 08:00:27:69:F2:E9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.53 seconds
```

DNS Enumeration

There are several ways to attack the dns which is active tech and passive tech But we will focus more in active with using zone transfer

```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[/home/kali]
└─# ls -al  /usr/share/nmap/scripts/ | grep -e "dns"
-rw-r--r-- 1 root root  1499 Mar 13  2024 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root  5329 Mar 13  2024 dns-blacklist.nse
-rw-r--r-- 1 root root 10100 Mar 13  2024 dns-brute.nse
-rw-r--r-- 1 root root  6639 Mar 13  2024 dns-cache-snoop.nse
-rw-r--r-- 1 root root 15152 Mar 13  2024 dns-check-zone.nse
-rw-r--r-- 1 root root 14826 Mar 13  2024 dns-client-subnet-scan.nse
-rw-r--r-- 1 root root 10168 Mar 13  2024 dns-fuzz.nse
-rw-r--r-- 1 root root  3803 Mar 13  2024 dns-ip6-arpa-scan.nse
-rw-r--r-- 1 root root 12702 Mar 13  2024 dns-nsec3-enum.nse
-rw-r--r-- 1 root root 10580 Mar 13  2024 dns-nsec-enum.nse
-rw-r--r-- 1 root root  3441 Mar 13  2024 dns-nsid.nse
-rw-r--r-- 1 root root  4364 Mar 13  2024 dns-random-srcport.nse
-rw-r--r-- 1 root root  4363 Mar 13  2024 dns-random-txid.nse
-rw-r--r-- 1 root root  1456 Mar 13  2024 dns-recursion.nse
-rw-r--r-- 1 root root  2195 Mar 13  2024 dns-service-discovery.nse
-rw-r--r-- 1 root root  5679 Mar 13  2024 dns-srv-enum.nse
-rw-r--r-- 1 root root  5765 Mar 13  2024 dns-update.nse
-rw-r--r-- 1 root root  2123 Mar 13  2024 dns-zeustracker.nse
-rw-r--r-- 1 root root 26574 Mar 13  2024 dns-zone-transfer.nse
-rw-r--r-- 1 root root  3910 Mar 13  2024 fcrdns.nse

┌──(root㉿kali)-[/home/kali]
└─#
```

Zone transfer is the technology where we can transfer the dns records from one server to other

we can use the ZoneTransfer.me domain for testing dns attacks

like DNS we can also check for different scripts

we can check for http,ftp,smb etc

```
┌──(root㉿kali)-[/home/kali]
└─# ls -al  /usr/share/nmap/scripts/ | grep -e "vul"
-rw-r--r-- 1 root root  7001 Mar 13  2024 afp-path-vuln.nse
-rw-r--r-- 1 root root  5923 Mar 13  2024 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  6973 Mar 13  2024 http-huawei-hg5xx-vuln.nse
-rw-r--r-- 1 root root  7921 Mar 13  2024 http-iis-webdav-vuln.nse
-rw-r--r-- 1 root root  4111 Mar 13  2024 http-vmware-path-vuln.nse
-rw-r--r-- 1 root root  3273 Mar 13  2024 http-vuln-cve2006-3392.nse
-rw-r--r-- 1 root root  6610 Mar 13  2024 http-vuln-cve2009-3960.nse
-rw-r--r-- 1 root root  2957 Mar 13  2024 http-vuln-cve2010-0738.nse
-rw-r--r-- 1 root root  5607 Mar 13  2024 http-vuln-cve2010-2861.nse
-rw-r--r-- 1 root root  4527 Mar 13  2024 http-vuln-cve2011-3192.nse
-rw-r--r-- 1 root root  5851 Mar 13  2024 http-vuln-cve2011-3368.nse
-rw-r--r-- 1 root root  4403 Mar 13  2024 http-vuln-cve2012-1823.nse
-rw-r--r-- 1 root root  4831 Mar 13  2024 http-vuln-cve2013-0156.nse
-rw-r--r-- 1 root root  2853 Mar 13  2024 http-vuln-cve2013-6786.nse
-rw-r--r-- 1 root root  5009 Mar 13  2024 http-vuln-cve2013-7091.nse
-rw-r--r-- 1 root root  2945 Mar 13  2024 http-vuln-cve2014-2126.nse
-rw-r--r-- 1 root root  3334 Mar 13  2024 http-vuln-cve2014-2127.nse
-rw-r--r-- 1 root root  3193 Mar 13  2024 http-vuln-cve2014-2128.nse
-rw-r--r-- 1 root root  2979 Mar 13  2024 http-vuln-cve2014-2129.nse
-rw-r--r-- 1 root root 14018 Mar 13  2024 http-vuln-cve2014-3704.nse
-rw-r--r-- 1 root root  4523 Mar 13  2024 http-vuln-cve2014-8877.nse
-rw-r--r-- 1 root root  7774 Mar 13  2024 http-vuln-cve2015-1427.nse
-rw-r--r-- 1 root root  3443 Mar 13  2024 http-vuln-cve2015-1635.nse
-rw-r--r-- 1 root root  4372 Mar 13  2024 http-vuln-cve2017-1001000.nse
-rw-r--r-- 1 root root  2594 Mar 13  2024 http-vuln-cve2017-5638.nse
-rw-r--r-- 1 root root  5480 Mar 13  2024 http-vuln-cve2017-5689.nse
-rw-r--r-- 1 root root  5187 Mar 13  2024 http-vuln-cve2017-8917.nse
-rw-r--r-- 1 root root  2699 Mar 13  2024 http-vuln-misfortune-cookie.nse
-rw-r--r-- 1 root root  4225 Mar 13  2024 http-vuln-wnr1000-creds.nse
-rw-r--r-- 1 root root  6977 Mar 13  2024 mysql-vuln-cve2012-2122.nse
-rw-r--r-- 1 root root  9425 Mar 13  2024 rdp-vuln-ms12-020.nse
-rw-r--r-- 1 root root  4011 Mar 13  2024 rmi-vuln-classloader.nse
-rw-r--r-- 1 root root  6528 Mar 13  2024 rsa-vuln-roca.nse
-rw-r--r-- 1 root root  4148 Mar 13  2024 samba-vuln-cve-2012-1182.nse
-rw-r--r-- 1 root root  5269 Mar 13  2024 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root  7524 Mar 13  2024 smb-vuln-conficker.nse
-rw-r--r-- 1 root root  6402 Mar 13  2024 smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 23154 Mar 13  2024 smb-vuln-cve-2017-7494.nse
-rw-r--r-- 1 root root  6545 Mar 13  2024 smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root  5386 Mar 13  2024 smb-vuln-ms07-029.nse
-rw-r--r-- 1 root root  5688 Mar 13  2024 smb-vuln-ms08-067.nse
-rw-r--r-- 1 root root  5647 Mar 13  2024 smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root  7214 Mar 13  2024 smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root  7344 Mar 13  2024 smb-vuln-ms17-010.nse
-rw-r--r-- 1 root root  4400 Mar 13  2024 smb-vuln-regsvc-dos.nse
-rw-r--r-- 1 root root  6586 Mar 13  2024 smb-vuln-webexec.nse
-rw-r--r-- 1 root root 14781 Mar 13  2024 smtp-vuln-cve2010-4344.nse
-rw-r--r-- 1 root root  7719 Mar 13  2024 smtp-vuln-cve2011-1720.nse
```

```
┌──(root㉿kali)-[/home/kali]
└─# ls -al  /usr/share/nmap/scripts/ | grep -e "http"
-rw-r--r-- 1 root root  2153 Mar 13  2024 http-adobe-coldfusion-apsa1301.nse
-rw-r--r-- 1 root root  5149 Mar 13  2024 http-affiliate-id.nse
-rw-r--r-- 1 root root  1950 Mar 13  2024 http-apache-negotiation.nse
-rw-r--r-- 1 root root  4499 Mar 13  2024 http-apache-server-status.nse
-rw-r--r-- 1 root root  1805 Mar 13  2024 http-aspnet-debug.nse
-rw-r--r-- 1 root root  3959 Mar 13  2024 http-auth-finder.nse
-rw-r--r-- 1 root root  3187 Mar 13  2024 http-auth.nse
-rw-r--r-- 1 root root  2865 Mar 13  2024 http-avaya-ipoffice-users.nse
-rw-r--r-- 1 root root  4372 Mar 13  2024 http-awstatstotals-exec.nse
-rw-r--r-- 1 root root  6872 Mar 13  2024 http-axis2-dir-traversal.nse
-rw-r--r-- 1 root root  5484 Mar 13  2024 http-backup-finder.nse
-rw-r--r-- 1 root root  6387 Mar 13  2024 http-barracuda-dir-traversal.nse
-rw-r--r-- 1 root root  2038 Mar 13  2024 http-bigip-cookie.nse
-rw-r--r-- 1 root root  4920 Mar 13  2024 http-brute.nse
-rw-r--r-- 1 root root  4436 Mar 13  2024 http-cakephp-version.nse
-rw-r--r-- 1 root root  4927 Mar 13  2024 http-chrono.nse
-rw-r--r-- 1 root root  1695 Mar 13  2024 http-cisco-anyconnect.nse
-rw-r--r-- 1 root root  5520 Mar 13  2024 http-coldfusion-subzero.nse
-rw-r--r-- 1 root root  4150 Mar 13  2024 http-comments-displayer.nse
-rw-r--r-- 1 root root  7251 Mar 13  2024 http-config-backup.nse
-rw-r--r-- 1 root root  5139 Mar 13  2024 http-cookie-flags.nse
-rw-r--r-- 1 root root  2577 Mar 13  2024 http-cors.nse
-rw-r--r-- 1 root root 13803 Mar 13  2024 http-cross-domain-policy.nse
-rw-r--r-- 1 root root  5418 Mar 13  2024 http-csrf.nse
-rw-r--r-- 1 root root  1718 Mar 13  2024 http-date.nse
-rw-r--r-- 1 root root 17392 Mar 13  2024 http-default-accounts.nse
-rw-r--r-- 1 root root  4288 Mar 13  2024 http-devframework.nse
-rw-r--r-- 1 root root  2529 Mar 13  2024 http-dlink-backdoor.nse
-rw-r--r-- 1 root root  4452 Mar 13  2024 http-dombased-xss.nse
-rw-r--r-- 1 root root 13893 Mar 13  2024 http-domino-enum-passwords.nse
-rw-r--r-- 1 root root  6931 Mar 13  2024 http-drupal-enum.nse
-rw-r--r-- 1 root root  2256 Mar 13  2024 http-drupal-enum-users.nse
-rw-r--r-- 1 root root 20667 Mar 13  2024 http-enum.nse
-rw-r--r-- 1 root root  3347 Mar 13  2024 http-errors.nse
-rw-r--r-- 1 root root 20413 Mar 13  2024 http-exif-spider.nse
-rw-r--r-- 1 root root  5199 Mar 13  2024 http-favicon.nse
-rw-r--r-- 1 root root  4451 Mar 13  2024 http-feed.nse
-rw-r--r-- 1 root root  9076 Mar 13  2024 http-fetch.nse
-rw-r--r-- 1 root root 11327 Mar 13  2024 http-fileupload-exploiter.nse
-rw-r--r-- 1 root root 21101 Mar 13  2024 http-form-brute.nse
-rw-r--r-- 1 root root  7934 Mar 13  2024 http-form-fuzzer.nse
-rw-r--r-- 1 root root  2739 Mar 13  2024 http-frontpage-login.nse
-rw-r--r-- 1 root root  2164 Mar 13  2024 http-generator.nse
-rw-r--r-- 1 root root 12100 Mar 13  2024 http-git.nse
-rw-r--r-- 1 root root  3195 Mar 13  2024 http-gitweb-projects-enum.nse
-rw-r--r-- 1 root root  3381 Mar 13  2024 http-google-malware.nse
```

```
┌──(root㉿kali)-[/home/kali]
└─# ls -al  /usr/share/nmap/scripts/ | grep -e "smb"
-rw-r--r-- 1 root root  3753 Mar 13  2024 smb2-capabilities.nse
-rw-r--r-- 1 root root  2689 Mar 13  2024 smb2-security-mode.nse
-rw-r--r-- 1 root root  1408 Mar 13  2024 smb2-time.nse
-rw-r--r-- 1 root root  5269 Mar 13  2024 smb2-vuln-uptime.nse
-rw-r--r-- 1 root root 45061 Mar 13  2024 smb-brute.nse
-rw-r--r-- 1 root root  5289 Mar 13  2024 smb-double-pulsar-backdoor.nse
-rw-r--r-- 1 root root  4840 Mar 13  2024 smb-enum-domains.nse
-rw-r--r-- 1 root root  5971 Mar 13  2024 smb-enum-groups.nse
-rw-r--r-- 1 root root  8043 Mar 13  2024 smb-enum-processes.nse
-rw-r--r-- 1 root root 27274 Mar 13  2024 smb-enum-services.nse
-rw-r--r-- 1 root root 12017 Mar 13  2024 smb-enum-sessions.nse
-rw-r--r-- 1 root root  6923 Mar 13  2024 smb-enum-shares.nse
-rw-r--r-- 1 root root 12527 Mar 13  2024 smb-enum-users.nse
-rw-r--r-- 1 root root  4418 Mar 13  2024 smb-flood.nse
-rw-r--r-- 1 root root  7471 Mar 13  2024 smb-ls.nse
-rw-r--r-- 1 root root  8758 Mar 13  2024 smb-mbenum.nse
-rw-r--r-- 1 root root  8220 Mar 13  2024 smb-os-discovery.nse
-rw-r--r-- 1 root root  4982 Mar 13  2024 smb-print-text.nse
-rw-r--r-- 1 root root  1833 Mar 13  2024 smb-protocols.nse
-rw-r--r-- 1 root root 63596 Mar 13  2024 smb-psexec.nse
-rw-r--r-- 1 root root  5190 Mar 13  2024 smb-security-mode.nse
-rw-r--r-- 1 root root  2424 Mar 13  2024 smb-server-stats.nse
-rw-r--r-- 1 root root 14159 Mar 13  2024 smb-system-info.nse
-rw-r--r-- 1 root root  7524 Mar 13  2024 smb-vuln-conficker.nse
-rw-r--r-- 1 root root  6402 Mar 13  2024 smb-vuln-cve2009-3103.nse
-rw-r--r-- 1 root root 23154 Mar 13  2024 smb-vuln-cve-2017-7494.nse
-rw-r--r-- 1 root root  6545 Mar 13  2024 smb-vuln-ms06-025.nse
-rw-r--r-- 1 root root  5386 Mar 13  2024 smb-vuln-ms07-029.nse
-rw-r--r-- 1 root root  5688 Mar 13  2024 smb-vuln-ms08-067.nse
-rw-r--r-- 1 root root  5647 Mar 13  2024 smb-vuln-ms10-054.nse
-rw-r--r-- 1 root root  7214 Mar 13  2024 smb-vuln-ms10-061.nse
-rw-r--r-- 1 root root  7344 Mar 13  2024 smb-vuln-ms17-010.nse
-rw-r--r-- 1 root root  4400 Mar 13  2024 smb-vuln-regsvc-dos.nse
-rw-r--r-- 1 root root  6586 Mar 13  2024 smb-vuln-webexec.nse
-rw-r--r-- 1 root root  5084 Mar 13  2024 smb-webexec-exploit.nse
```

```
┌──(root㉿kali)-[/home/kali]
└─# ls -al  /usr/share/nmap/scripts/ | grep -e "ftp"
-rw-r--r-- 1 root root  4530 Mar 13  2024 ftp-anon.nse
-rw-r--r-- 1 root root  3253 Mar 13  2024 ftp-bounce.nse
-rw-r--r-- 1 root root  3108 Mar 13  2024 ftp-brute.nse
-rw-r--r-- 1 root root  3272 Mar 13  2024 ftp-libopie.nse
-rw-r--r-- 1 root root  3290 Mar 13  2024 ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root  3768 Mar 13  2024 ftp-syst.nse
-rw-r--r-- 1 root root  6021 Mar 13  2024 ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root  5923 Mar 13  2024 ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root  5736 Mar 13  2024 tftp-enum.nse
-rw-r--r-- 1 root root 10034 Mar 13  2024 tftp-version.nse

┌──(root㉿kali)-[/home/kali]
└─# ls -al  /usr/share/nmap/scripts/ | grep -e "vulners"
-rw-r--r-- 1 root root  7077 Mar 13  2024 vulners.nse
```