

Name : Hamza Bacha

Nmap Scanning

Step 1: Verify Host is Up

Command : ping -c 4 192.168.75.132

Purpose: Confirm the target is reachable

```
(kali㉿kali)-[~] $ ping -c 4 192.168.75.132
PING 192.168.75.132 (192.168.75.132) 56(84) bytes of data.
64 bytes from 192.168.75.132: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.75.132: icmp_seq=2 ttl=64 time=0.346 ms
64 bytes from 192.168.75.132: icmp_seq=3 ttl=64 time=0.292 ms
64 bytes from 192.168.75.132: icmp_seq=4 ttl=64 time=0.322 ms
```

Step 2: Basic Host Discovery

Command: nmap -sn 192.168.75.132

What it does: Ping scan to check if host is alive

```
(kali㉿kali)-[~] $ nmap -sn 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:41 EST
Nmap scan report for 192.168.75.132
Host is up (0.0011s latency).
MAC Address: 00:0C:29:B7:91:0E (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Step 3: Quick Scan (Top 1000 Ports)

Command : nmap 192.168.75.132

```
└─(kali㉿kali)-[~]
└─$ nmap 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:41 EST
Nmap scan report for 192.168.75.132
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:B7:91:0E (VMware)
```

Step 4: Full Port Scan

Command : nmap -p- 192.168.75.132

What it does: Scans all 65,535 ports .

```
(kali㉿kali)-[~]
└─$ nmap -p- 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:42 EST
Nmap scan report for 192.168.75.132
Host is up (0.00097s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsvr
48015/tcp open  unknown
48888/tcp open  unknown
53132/tcp open  unknown
58991/tcp open  unknown
MAC Address: 00:0C:29:B7:91:0E (VMware)
```

Step 5: Service Version Detection

Command : nmap -sV 192.168.75.132

Purpose: Identifies what services are running and their versions

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:42 EST
Nmap scan report for 192.168.75.132
Host is up (0.0011s latency).
Not shown: 977 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)
512/tcp   open  exec   netkit-rsh rexecd
513/tcp   open  login   OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
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)
6667/tcp  open  irc   UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:B7:91:0E (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 11.90 seconds
```

Step 6: OS Detection

Command : sudo nmap -O 192.168.75.132

Purpose: Attempts to identify the operating system

```
(kali㉿kali)-[~] ~ login.html: Possible admin folder
└─$ sudo nmap -O 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:42 EST
Nmap scan report for 192.168.75.132
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:B7:91:0E (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

Step 7: Aggressive Scan (Combines Multiple Options)

Command : sudo nmap -A 192.168.75.132

Includes: OS detection, version detection, script scanning, traceroute

```
(Kali㉿kali)-[~] $ sudo nmap -A 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:43 EST
Nmap scan report for 192.168.75.132
Host is up (0.00045s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.75.128
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| ssl-date: 2025-12-11T17:43:49+00:00; +7s from scanner time.
|_ssl2v:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|_SSL2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto service
|   100000  2          111/tcp   rpcbind
|   100000  2          111/udp   rpcbind
|   100003  2,3,4     2049/tcp  nfs
|   100003  2,3,4     2049/udp  nfs
|   100005  1,2,3     46775/udp mountd
|   100005  1,2,3     48015/tcp mountd
|   100021  1,3,4     50982/udp nlockngr
|   100021  1,3,4     53132/tcp nlockngr
|   100024  1          56120/udp status
|_ 100024  1          58991/tcp status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs        2-4 (RPC #100003)
2121/tcp  open  ftp        ProFTPD 1.3.1
```

```

512/tcp open  exec    metasploit 1.8n-rexecd
513/tcp open  login   Possible admin folder
514/tcp open  tcpwrapped
1099/tcp open  java-rmi  GNU Classpath grmiregistry
1524/tcp open  bindshell  Metasploitable root shell /loder
2049/tcp open  nfs      login   2-4 (RPC #100003) /admin folder
2121/tcp open  ftp     ProFTPD 1.3.1
3306/tcp open  mysql   MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10 in login.jsp. Possible admin folder
|   Version: 5.0.51a-3ubuntu5 Possible admin folder
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, SwitchToSSLAfterHandshake, ConnectWithDatabase, SupportsCompression, SupportsFileDownload / FCKeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   Status: Autocommit
|   Salt: p9i6#ebC1gnqoZTwxd
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-12-11T17:43:49+00:00; +7s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/ryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
5900/tcp open  vnc     VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3  ERROR: Script execution failed (use -d to debug)
|   Security types:
|     VNC Authentication (2)  <----> scanned in 325.24 seconds
6000/tcp open  X11    (access denied)
6667/tcp open  irc     UnrealIRCd
| irc-info:
|   users: 1

|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http   Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
MAC Address: 00:0C:29:B7:91:0E (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33 Possible admin folder
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery: login.jsp: Possible admin folder
|   OS: Unix (Samba 3.0.20-Debian) Possible admin folder
|   Computer name: metasploitable
|   NetBIOS computer name: metasploitable
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   FQDN: metasploitable.localdomain editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|_ System time: 2025-12-11T12:43:39+05:00
|_smb2-time: Protocol negotiation failed (SMB2) / Remote File upload
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h15m06s, deviation: 2h30m00s, median: 6s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)

TRACEROUTE nmap-sync-dos: ERROR: Script execution failed (use -d to debug)
HOP RTT      ADDRESS
1  0.45 ms 192.168.75.132  (1 host up) scanned in 325.24 seconds

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.10 seconds

```

Step 8: Specific Port Scan

Command : nmap -p 21,22,23,80,443,3306,3389 192.168.75.132

Purpose: Targets common service ports

```
(kali㉿kali)-[~]
└─$ nmap -p 21,22,23,80,443,3306,3389 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:43 EST
Nmap scan report for 192.168.75.132
Host is up (0.00027s latency).

PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
23/tcp    open   telnet
80/tcp    open   http
443/tcp   closed https
3306/tcp  open   mysql
3389/tcp  closed ms-wbt-server
MAC Address: 00:0C:29:B7:91:0E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Step 9: Vulnerability Scanning with NSE Scripts

Command : nmap --script vuln 192.168.75.132

Specific vulnerability scripts:

```
(kali㉿kali)-[~]
└$ nmap --script vuln 192.168.75.132
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:45 EST
Nmap scan report for 192.168.75.132
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|  ftp-vsftpd-backdoor:
|    VULNERABLE:
|      vsFTPD version 2.3.4 backdoor
|        State: VULNERABLE (Exploitable)
|        IDs:  BID:48539  CVE:CVE-2011-2523
|          vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|          Disclosure date: 2011-07-03
|        Exploit results:
|          Shell command: id
|          Results: uid=0(root) gid=0(root)
|        References:
|          https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|          http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|          https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|          https://www.securityfocus.com/bid/48539
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
|  smtp-vuln-cve2010-4344:
|    The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|
| Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|   State: VULNERABLE
|     Transport Layer Security (TLS) services that use anonymous
|     Diffie-Hellman key exchange only provide protection against passive
|     eavesdropping, and are vulnerable to active man-in-the-middle attacks
|     which could completely compromise the confidentiality and integrity
|     of any data exchanged over the resulting session.
| Check results:
|   ANONYMOUS DH GROUP 1
|     Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|     Modulus Type: Safe prime
|     Modulus Source: postfix builtin
|     Modulus Length: 1024
|     Generator Length: 8
|     Public Key Length: 1024
|   References:
|     https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|   State: VULNERABLE
|   IDs:  BID:74733  CVE:CVE-2015-4000
|     The Transport Layer Security (TLS) protocol contains a flaw that is
|     triggered when handling Diffie-Hellman key exchanges defined with
|     the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|     to downgrade the security of a TLS session to 512-bit export-grade
|     cryptography, which is significantly weaker, allowing the attacker
|     to more easily break the encryption and monitor or tamper with
|     the encrypted stream.
|   Disclosure date: 2015-5-19
|   Check results:
```

```
| ANONYMOUS DH GROUP 1
|   Cipher Suite: TLS_DH_anon_WITH_AES_128_CBC_SHA
|   Modulus Type: Safe prime
|   Modulus Source: postfix builtin
|   Modulus Length: 1024
|   Generator Length: 8
|   Public Key Length: 1024
| References:
|     https://www.ietf.org/rfc/rfc2246.txt
|
| Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
| State: VULNERABLE
| IDs: BID:74733 CVE:CVE-2015-4000
|   The Transport Layer Security (TLS) protocol contains a flaw that is
|   triggered when handling Diffie-Hellman key exchanges defined with
|   the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|   to downgrade the security of a TLS session to 512-bit export-grade
|   cryptography, which is significantly weaker, allowing the attacker
|   to more easily break the encryption and monitor or tamper with
|   the encrypted stream.
| Disclosure date: 2015-5-19
|
| http-vuln-cve2017-100100: ERROR: Script execution failed (use -d to debug)
| http-sql-injection:
| Possible sql for queries:
|   http://192.168.75.132:80/dav/?C=S%3B0%3DA%27%200R%20sqlspider
|   http://192.168.75.132:80/dav/?C=D%3B0%3DA%27%200R%20sqlspider
|   http://192.168.75.132:80/dav/?C=N%3B0%3DD%27%200R%20sqlspider
|   http://192.168.75.132:80/dav/?C=M%3B0%3DA%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=login.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=home.php&do=toggle-security%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=framing.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/?page=text-file-viewer.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/?page=user-info.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/?page=view-someones-blog.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/?page=show-log.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=captured-data.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=browser-info.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/?page=add-to-your-blog.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=secret-administrative-pages.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=add-to-your-blog.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=dns-lookup.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=installation.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=register.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=notes.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=user-info.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=php-errors.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=usage-instructions.php%27%200R%20sqlspider
|   http://192.168.75.132:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%200R%20sqlspider
```

```
| http-slowloris-check:  
| VULNERABLE:  
| Slowloris DOS attack  
| State: LIKELY VULNERABLE  
| IDs: CVE:CVE-2007-6750  
| Slowloris tries to keep many connections to the target web server open and hold  
| them open as long as possible. It accomplishes this by opening connections to  
| the target web server and sending a partial request. By doing so, it starves  
| the http server's resources causing Denial Of Service.  
|  
| Disclosure date: 2009-09-17  
| References:  
|   http://ha.ckers.org/slowloris/  
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
| http-dombased-xss: Couldn't find any DOM based XSS.  
| http-enum:  
|   /tikiwiki/: Tikiwiki  
|   /test/: Test page  
|   /phpinfo.php: Possible information file  
|   /phpMyAdmin/: phpMyAdmin  
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'  
|   /icons/: Potentially interesting folder w/ directory listing  
|   /index/: Potentially interesting folder  
111/tcp  open  rpcbind  
139/tcp  open  netbios-ssn  
445/tcp  open  microsoft-ds  
512/tcp  open  exec  
513/tcp  open  login  
514/tcp  open  shell  
1099/tcp open  rmiregistry  
| rmi-vuln-classloader:
```

Step 9: UDP Scan

Command: sudo nmap -sU 192.168.75.132

Purpose: Scans for UDP services (DNS, DHCP, SNMP, etc.)

```
└─(kali㉿kali)-[~]  
$ sudo nmap -sU 192.168.75.132  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-11 12:44 EST  
Stats: 0:05:45 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan  
UDP Scan Timing: About 40.10% done; ETC: 12:58 (0:08:35 remaining)  
Stats: 0:05:46 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan  
UDP Scan Timing: About 40.22% done; ETC: 12:58 (0:08:34 remaining)  
Stats: 0:05:47 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan  
UDP Scan Timing: About 40.22% done; ETC: 12:58 (0:08:36 remaining)  
Stats: 0:06:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan  
UDP Scan Timing: About 41.98% done; ETC: 12:58 (0:08:24 remaining)  
└─(kali㉿kali)-[~]
```

Scapy Packet Analysis

Step 1: Open Scapy Interactive Mode

Command : sudo scapy

```
└─(kali㉿kali)-[~]
$ sudo scapy
[sudo] password for kali:
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

          aSPY//YASa
      apyyyyCY/////////YCa
      sY/////YSpcs  scpCY//Pp
  ayp ayyyyyyySCP//Pp      syY//C
AYAsAYYYYYYYY///Ps      cY//S
    pCCCCY//p      cSSps y//Y
    SPPPP//a      pP///AC//Y
      A//A      cyP///C
      p///Ac      SC///a
      P///YCpc      A//A
  scccccp///pSP///p      p//Y
  sY/////////y  caa      S//P
  cayCyayP//Ya      pY/Ya
  sY/PsY///YCc      aC//Yp
  sc  sccacY//PCyapaYCP//YSS
  spCPY////YPSps
  ccaacs

Welcome to Scapy
Version 2.6.1
https://github.com/secdev/scapy
Have fun!
Wanna support scapy? Star us on
GitHub! -- Satoshi Nakamoto
using IPython 8.30.0

>>> ls
<function scapy.packet.ls(obj=None, case_sensitive=False, verbose=False)>
```

Part 2: Basic Packet Creation

Exercise 1: Create a Simple IP Packet

Command :packet = IP(dst="192.168.75.132")

packet.show()

```
>>> packet = IP(dst="192.168.75.132")
>>> packet.show()
###[ ID ]###[
version  = 4
ihl     = None
tos     = 0x0
len     = None
id      = 1
flags   =
frag   = 0
ttl    = 64
proto  = hopopt
chksum = None
src    = 192.168.75.128
dst    = 192.168.75.132
options \
```

Exercise 2: Create ICMP Packet (Ping)

Command : ping = IP(dst="192.168.75.132")/ICMP()

ping.show()

Explanation:

- IP() = Internet Protocol layer
- ICMP() = Ping protocol
- / = Stack layers together

```
>>> ping = IP(dst="192.168.75.132")/ICMP()
>>> ping.show()
###[ IP ]###[ 
    version   = 4
    ihl      = None
    tos      = 0x0
    len     = None
    id       = 1
    flags    = 
    frag     = 0
    ttl      = 64
    proto    = icmp
    chksum   = None
    src      = 192.168.75.128
    dst      = 192.168.75.132
    \options  \
###[ ICMP ]###[ 
    type     = echo-request
    code     = 0
    checksum = None
    id       = 0x0
    seq     = 0x0
    unused   = b''
```

Exercise 3: Send the Ping

send(ping)

What happens: Packet is sent (you won't see response)

```
>>> send(ping)
.
Sent 1 packets.
```

Exercise 4: Send and Receive Response

Command : response = sr1(ping)

response.show()

What happens:

- `sr1()` = Send and Receive 1 packet
 - You'll see the reply from 192.168.75.132

Simple ARP (Address Resolution Protocol)

Exercise 5: Create ARP Request

Command : arp = ARP(pdst="192.168.75.132")

arp.show()

op= who-has (asking for MAC address)

```
>>> arp = ARP(pdst="192.168.75.132")
>>> arp.show()
###[ ARP ]###[  
    hwtype      = Ethernet (10Mb)  
    ptype       = IPv4  
    hwlen       = None  
    plen        = None  
    op          = who-has  
    hwsrc       = 00:0c:29:24:15:5c  
    psrc        = 192.168.75.128  
    hwdst       = 00:00:00:00:00:00  
    pdst        = 192.168.75.132
```

Exercise 6: Send ARP Request

Command : answered, unanswered = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/arp, timeout=2)

```
answered.show()
```

what happened :

you will see;

IP: 192.168.75.132

MAC: 00:0c:29:b7:91:0e

```
>>> answered, unanswered = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/arp, timeout=2)
Begin emission
Finished sending 1 packets
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> answered.show()
0000 Ether / ARP who has 192.168.75.132 says 192.168.75.128 ==> Ether / ARP is at 00:0c:29:b7:91:0e says 192.168.75.132 / Padding
```

Simple Packet Sniffing

Exercise 7: Sniff 5 Packets

Command : packets = sniff(count=5)

packets.show()

What happens: Captures 5 packets from your network

```
>>> packets = sniff(count=5)

^C>>> packets.show()
0000 Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option - Source Link-Layer Address 00:50:56:c0:00:08
```

Exercise 8: Sniff and Display Each Packet

Command : packets = sniff(count=5)

for pkt in packets:

print(pkt.summary())

you'll see:

Ether / IP / TCP 192.168.75.1:12345 > 192.168.75.132:80

Ether / IP / TCP 192.168.75.132:80 > 192.168.75.1:12345

```
>>> packets = sniff(count=5)
>>> for pkt in packets: print(pkt.summary())
Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option - Source Link-Layer Address 00:50:56:c0:00:08
Ether / IP / UDP / NBT Datagram / SMB_Header / Tran b'\\MAILSLOT\\BROWSE' LocalMasterAnnouncement for b'METASPLOITABLE'
Ether / IP / UDP / NBT Datagram / SMB_Header / Tran b'\\MAILSLOT\\BROWSE' DomainAnnouncement
Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option - Source Link-Layer Address 00:50:56:c0:00:08
Ether / IP / UDP / mDNS_Ans b'DESKTOP-P4GB80R._dosvc._tcp.local.'
```
