|  |  |  |
| --- | --- | --- |
| 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 |
| 5900/tcp | open | vnc |
| 6000/tcp | open | X11 |
| 6667/tcp | open | irc |
| 8009/tcp | open | ajp13 |
| 8180/tcp | open | unknown |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

root@kali:~# nmap -v 192.168.198.130

Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 11:55 EDT

Initiating ARP Ping Scan at 11:55

Scanning 192.168.198.130 [1 port]

Completed ARP Ping Scan at 11:55, 0.41s elapsed (1 total hosts)

Nmap scan report for 192.168.198.130 [host down]

Read data files from: /usr/bin/../share/nmap

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 0.68 seconds

Raw packets sent: 2 (56B) | Rcvd: 0 (0B)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

root@kali:~# nmap -sA -v -A 192.168.198.130

Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 12:17 EDT

NSE: Loaded 148 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 12:17

Completed NSE at 12:17, 0.00s elapsed

Initiating NSE at 12:17

Completed NSE at 12:17, 0.00s elapsed

Initiating ARP Ping Scan at 12:17

Scanning 192.168.198.130 [1 port]

Completed ARP Ping Scan at 12:17, 0.41s elapsed (1 total hosts)

Nmap scan report for 192.168.198.130 [host down]

NSE: Script Post-scanning.

Initiating NSE at 12:17

Completed NSE at 12:17, 0.00s elapsed

Initiating NSE at 12:17

Completed NSE at 12:17, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 2.83 seconds

Raw packets sent: 2 (56B) | Rcvd: 0 (0B)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

nmap -A 192.168.198.132

Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 12:34 EDT

Nmap scan report for 192.168.198.132

Host is up (0.00080s latency).

Not shown: 981 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.198.129

| 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

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:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

|\_ssl-date: 2019-04-21T16:34:02+00:00; -1m11s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_DES\_64\_CBC\_WITH\_MD5

|\_ SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

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 50812/tcp mountd

| 100005 1,2,3 52163/udp mountd

| 100021 1,3,4 36781/udp nlockmgr

| 100021 1,3,4 45935/tcp nlockmgr

| 100024 1 37739/tcp status

|\_ 100024 1 40451/udp 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 OpenBSD or Solaris rlogind

514/tcp open tcpwrapped

1099/tcp open java-rmi Java RMI Registry

1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

2121/tcp open ftp ProFTPD 1.3.1

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|\_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

| irc-info:

| users: 1

| servers: 1

| lusers: 1

| lservers: 0

| server: irc.Metasploitable.LAN

| version: Unreal3.2.8.1. irc.Metasploitable.LAN

| uptime: 0 days, 1:51:30

| source ident: nmap

| source host: D831683B.768961CD.FFFA6D49.IP

|\_ error: Closing Link: vbhbvxuwm[192.168.198.129] (Quit: vbhbvxuwm)

MAC Address: 00:0C:29:B5:A5:7C (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

Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 1h58m49s, deviation: 2h49m43s, median: -1m11s

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| NetBIOS computer name:

| Workgroup: WORKGROUP\x00

|\_ System time: 2019-04-21T12:34:01-04:00

|\_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE

HOP RTT ADDRESS

1 0.80 ms 192.168.198.132

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 22.12 seconds

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| ftp | ftp-anon.nse  ftp-bounce.nse  ftp-brute.nse  ftp-libopie.nse  ftp-proftpd-backdoor.nse  ftp-syst.nse  ftp-vsftpd-backdoor.nse  ftp-vuln-cve2010-4221.nse  tftp-enum.nse |
| ssh | ssh-auth-methods.nse  ssh-brute.nse  ssh-hostkey.nse  ssh-publickey-acceptance.nse  ssh-run.nse  ssh2-enum-algos.nse  sshv1.nse |
| telnet | telnet-brute.nse  telnet-encryption.nse  telnet-ntlm-info.nse |
| smtp | smtp-brute.nse  smtp-commands.nse  smtp-enum-users.nse  smtp-ntlm-info.nse  smtp-open-relay.nse  smtp-strangeport.nse  smtp-vuln-cve2010-4344.nse  smtp-vuln-cve2011-1720.nse  smtp-vuln-cve2011-1764.nse |
| domain | http-cross-domain-policy.nse  smb-enum-domains.nse  whois-domain.nse |
| http | /usr/share/golismero/wordlist/fingerprint/httprecon/httprecon.nse  http-adobe-coldfusion-apsa1301.nse  http-affiliate-id.nse  http-apache-negotiation.nse  http-apache-server-status.nse  http-aspnet-debug.nse  http-auth-finder.nse  http-auth.nse  http-avaya-ipoffice-users.nse  http-awstatstotals-exec.nse  http-axis2-dir-traversal.nse  http-backup-finder.nse  http-barracuda-dir-traversal.nse  http-bigip-cookie.nse  http-brute.nse  http-cakephp-version.nse  http-chrono.nse  http-cisco-anyconnect.nse  http-coldfusion-subzero.nse  http-comments-displayer.nse  http-config-backup.nse  http-cookie-flags.nse  http-cors.nse  http-cross-domain-policy.nse  http-csrf.nse  http-date.nse  http-default-accounts.nse  http-devframework.nse  http-dlink-backdoor.nse  http-dombased-xss.nse  http-domino-enum-passwords.nse  http-drupal-enum-users.nse  http-drupal-enum.nse  http-enum.nse  http-errors.nse  http-exif-spider.nse  http-favicon.nse  http-feed.nse  http-fetch.nse  http-fileupload-exploiter.nse  http-form-brute.nse  http-form-fuzzer.nse  http-frontpage-login.nse  http-generator.nse  http-git.nse  http-gitweb-projects-enum.nse  http-google-malware.nse  http-grep.nse  http-headers.nse  http-huawei-hg5xx-vuln.nse  http-icloud-findmyiphone.nse  http-icloud-sendmsg.nse  http-iis-short-name-brute.nse  http-iis-webdav-vuln.nse  http-internal-ip-disclosure.nse  http-joomla-brute.nse  http-jsonp-detection.nse  http-litespeed-sourcecode-download.nse  http-ls.nse  http-majordomo2-dir-traversal.nse  http-malware-host.nse  http-mcmp.nse  http-method-tamper.nse  http-methods.nse  http-mobileversion-checker.nse  http-ntlm-info.nse  http-open-proxy.nse  http-open-redirect.nse  http-passwd.nse  http-php-version.nse  http-phpmyadmin-dir-traversal.nse  http-phpself-xss.nse  http-proxy-brute.nse  http-put.nse  http-qnap-nas-info.nse  http-referer-checker.nse  http-rfi-spider.nse  http-robots.txt.nse  http-robtex-reverse-ip.nse  http-robtex-shared-ns.nse  http-security-headers.nse  http-server-header.nse  http-shellshock.nse  http-sitemap-generator.nse  http-slowloris-check.nse  http-slowloris.nse  http-sql-injection.nse  http-stored-xss.nse  http-svn-enum.nse  http-svn-info.nse  http-title.nse  http-tplink-dir-traversal.nse  http-trace.nse  http-traceroute.nse  http-trane-info.nse  http-unsafe-output-escaping.nse  http-useragent-tester.nse  http-userdir-enum.nse  http-vhosts.nse  http-virustotal.nse  http-vlcstreamer-ls.nse  http-vmware-path-vuln.nse  http-vuln-cve2006-3392.nse  http-vuln-cve2009-3960.nse  http-vuln-cve2010-0738.nse  http-vuln-cve2010-2861.nse  http-vuln-cve2011-3192.nse  http-vuln-cve2011-3368.nse  http-vuln-cve2012-1823.nse  http-vuln-cve2013-0156.nse  http-vuln-cve2013-6786.nse  http-vuln-cve2013-7091.nse  http-vuln-cve2014-2126.nse  http-vuln-cve2014-2127.nse  http-vuln-cve2014-2128.nse  http-vuln-cve2014-2129.nse  http-vuln-cve2014-3704.nse  http-vuln-cve2014-8877.nse  http-vuln-cve2015-1427.nse  http-vuln-cve2015-1635.nse  http-vuln-cve2017-1001000.nse  http-vuln-cve2017-5638.nse  http-vuln-cve2017-5689.nse  http-vuln-cve2017-8917.nse  http-vuln-misfortune-cookie.nse  http-vuln-wnr1000-creds.nse  http-waf-detect.nse  http-waf-fingerprint.nse  http-webdav-scan.nse  http-wordpress-brute.nse  http-wordpress-enum.nse  http-wordpress-users.nse  http-xssed.nse  ip-https-discover.nse  membase-http-info.nse  riak-http-info.nse |
| rpcbind |  |
| netbios-ssn | broadcast-netbios-master-browser.nse |
| microsoft-ds |  |
| exec | clamav-exec.nse  http-awstatstotals-exec.nse  jdwp-exec.nse  mmouse-exec.nse  qconn-exec.nse  rexec-brute.nse  smb-psexec.nse |
| login | http-frontpage-login.nse  rlogin-brute.nse  snmp-hh3c-logins.nse |
| shell | http-shellshock.nse  ms-sql-xp-cmdshell.nse |
| rmiregistry |  |
| ingreslock |  |
| nfs | nfs-ls.nse  nfs-showmount.nse  nfs-statfs.nse |
| ccproxy-ftp |  |
| vnc | realvnc-auth-bypass.nse  vnc-brute.nse  vnc-info.nse  vnc-title.nse |
| X11 | x11-access.nse |
| irc | irc-botnet-channels.nse  irc-brute.nse  irc-info.nse  irc-sasl-brute.nse  irc-unrealircd-backdoor.nse |
| ajp13 |  |
| unknown |  |

root@kali:~# nmap -p 21 --script ftp-anon 192.168.198.132

Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 13:30 EDT

Nmap scan report for 192.168.198.132

Host is up (0.00029s latency).

PORT STATE SERVICE

21/tcp open ftp

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

MAC Address: 00:0C:29:B5:A5:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds

root@kali:~# nmap -p 80 --script http-brute 192.168.198.132

Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 13:32 EDT

Nmap scan report for 192.168.198.132

Host is up (0.00027s latency).

PORT STATE SERVICE

80/tcp open http

| http-brute:

|\_ Path "/" does not require authentication

MAC Address: 00:0C:29:B5:A5:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds

root@kali:~# nmap -p 80 --script http-brute vk.com

Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 13:32 EDT

Nmap scan report for vk.com (87.240.190.67)

Host is up (0.087s latency).

Other addresses for vk.com (not scanned): 93.186.225.197 87.240.129.133 87.240.182.224

rDNS record for 87.240.190.67: srv67-190-240-87.vk.com

PORT STATE SERVICE

80/tcp open http

| http-brute:

|\_ Path "/" does not require authentication

Nmap done: 1 IP address (1 host up) scanned in 0.92 seconds

root@kali:~# nmap -p 80 --script http-trace 192.168.198.132

Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-21 13:35 EDT

Nmap scan report for 192.168.198.132

Host is up (0.00029s latency).

PORT STATE SERVICE

80/tcp open http

|\_http-trace: TRACE is enabled

MAC Address: 00:0C:29:B5:A5:7C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.72 seconds







