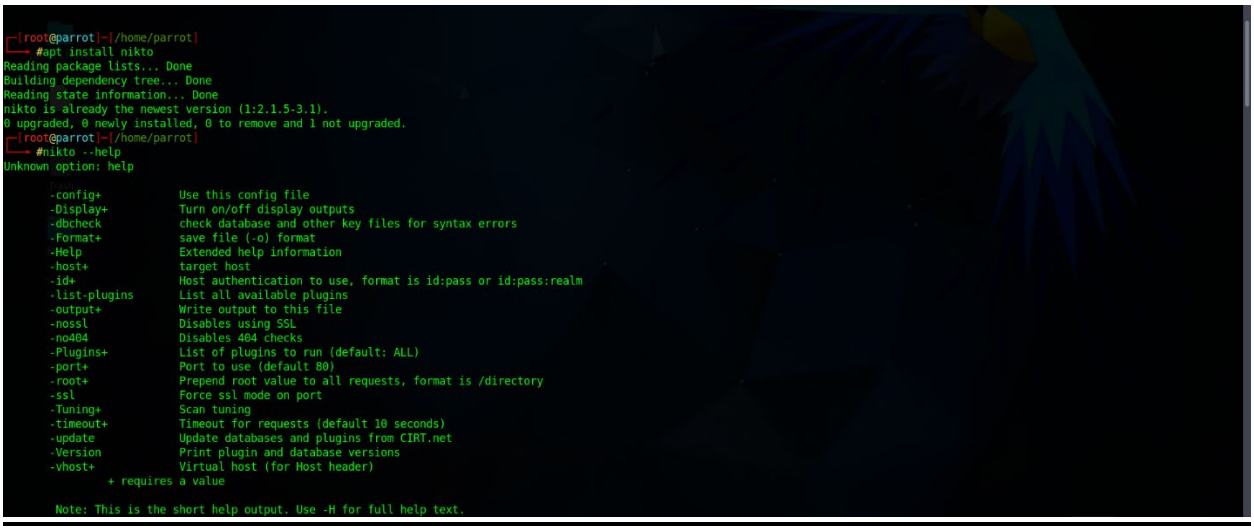
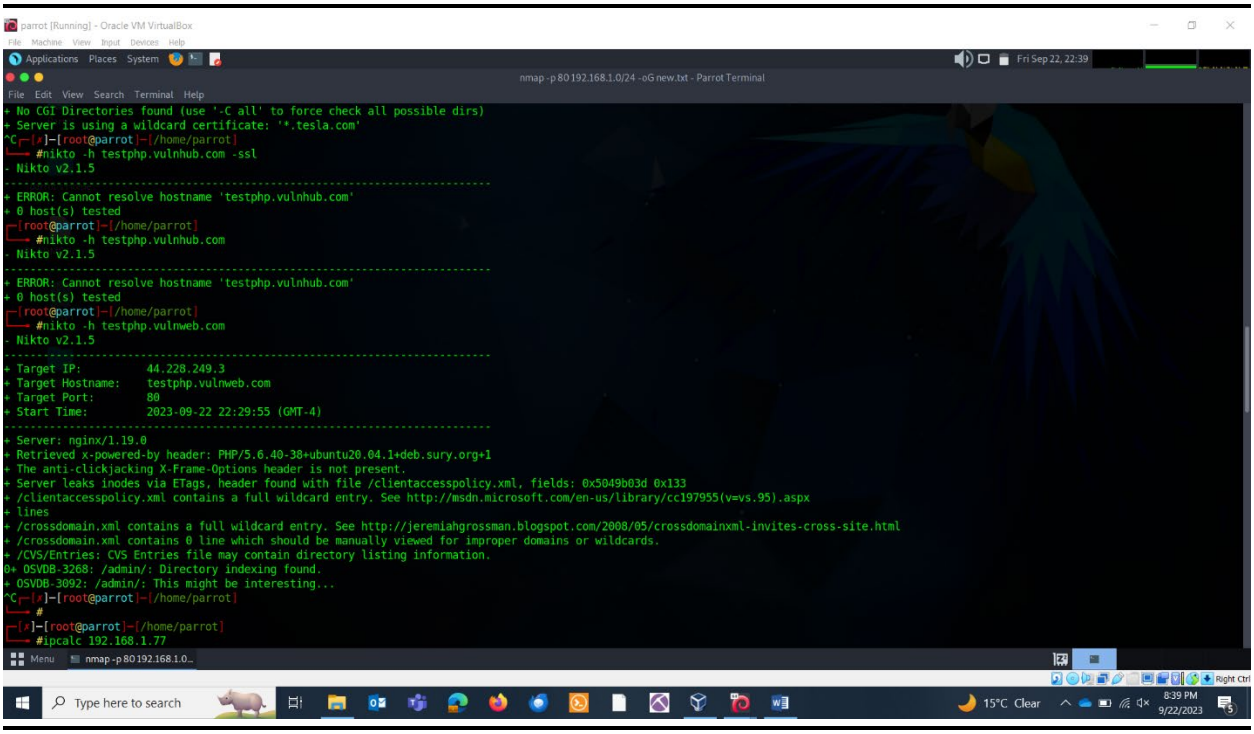
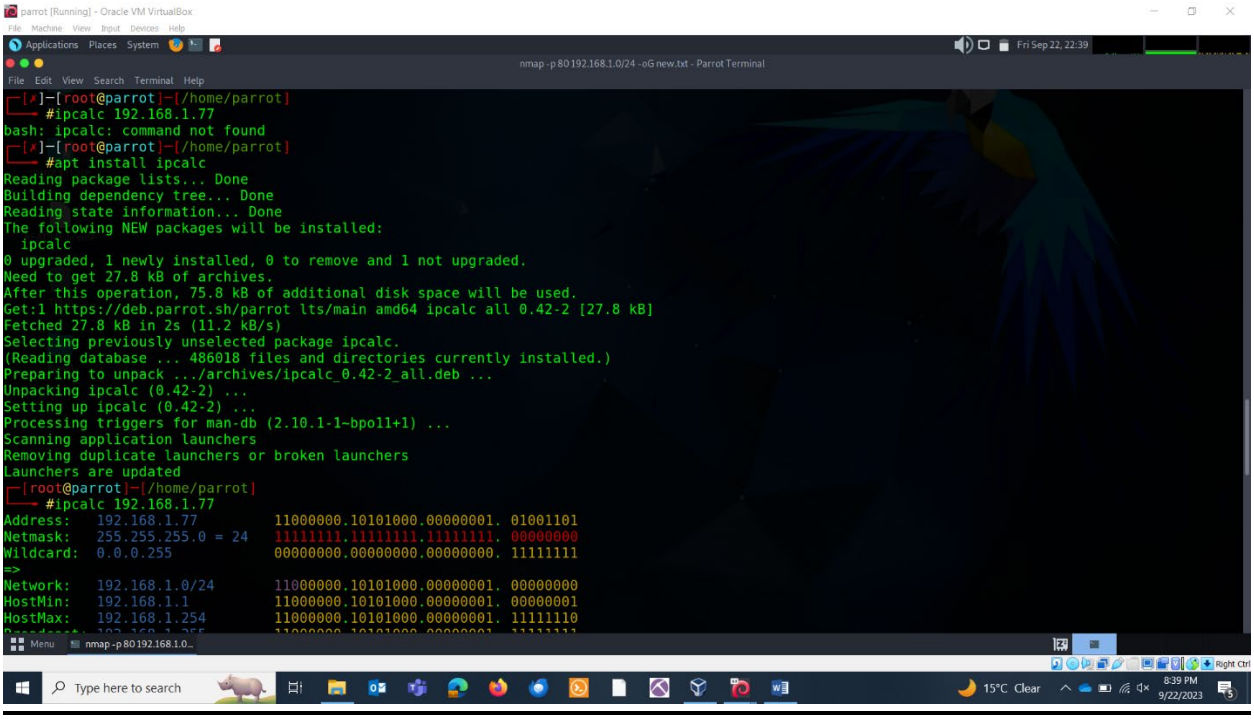
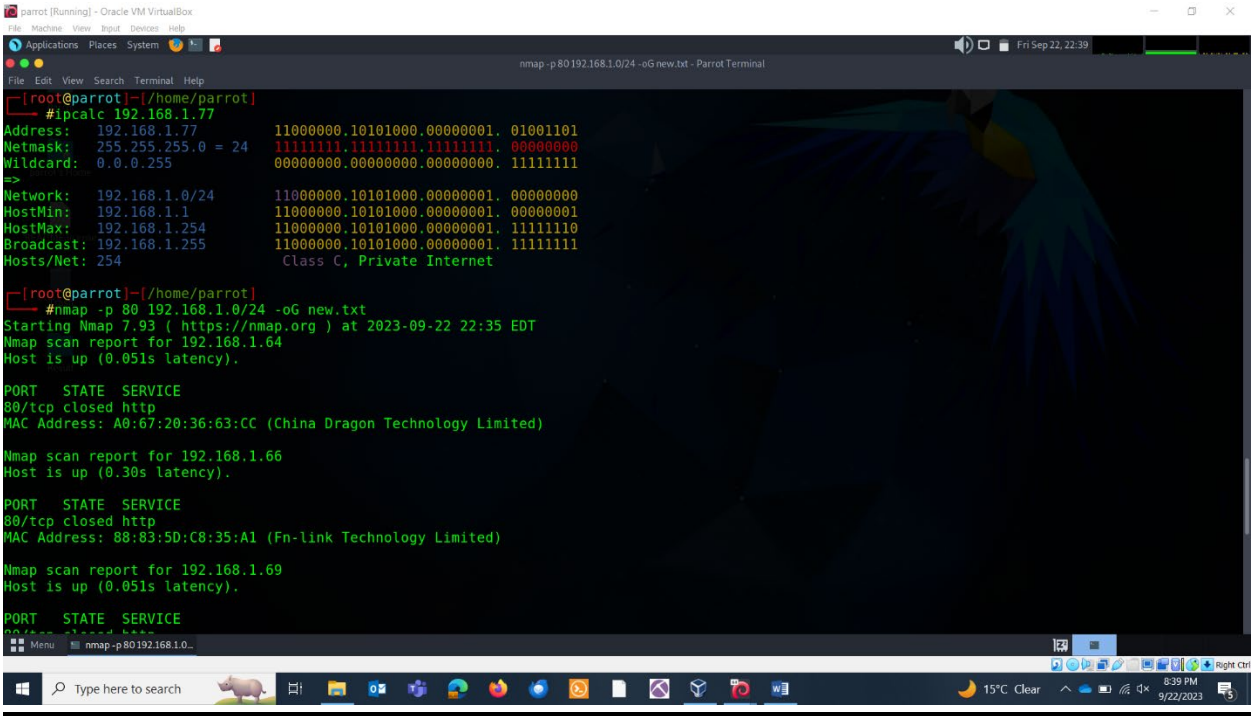
NIKTO

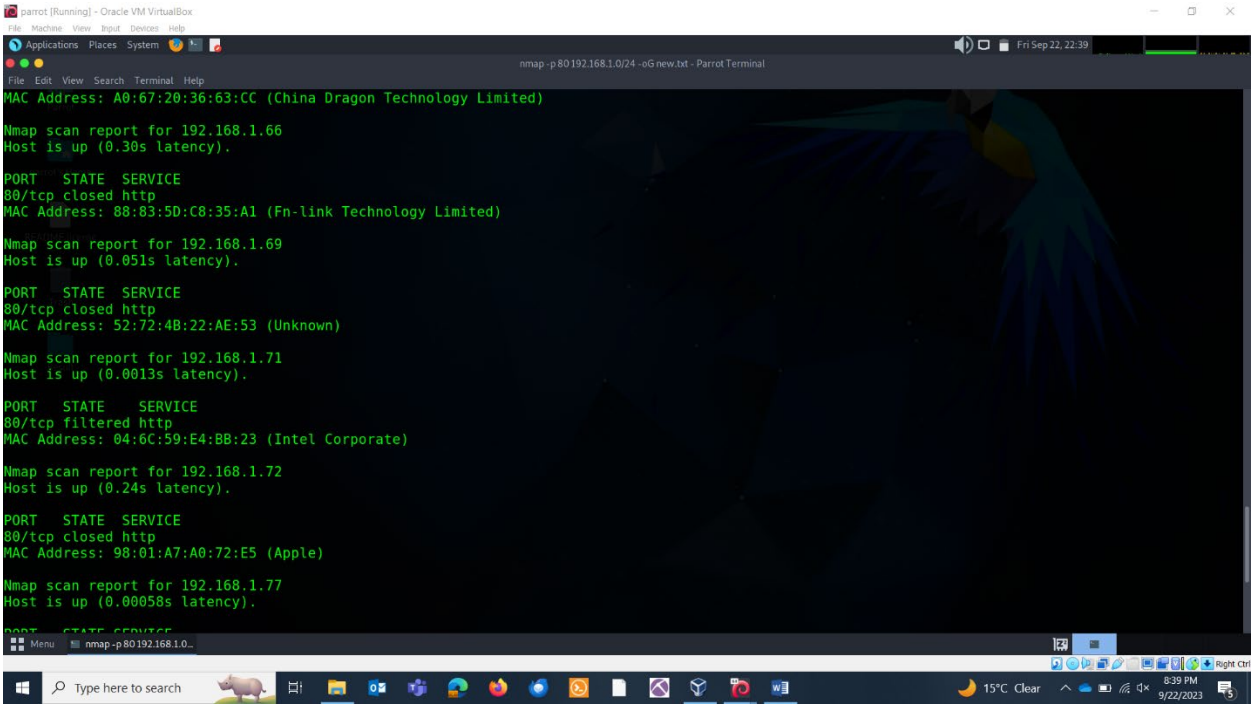

┌[root@parrot]-[/home/parrot]
└──→ #apt install nikto
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nikto is already the newest version (1:2.1.5-3.1).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
┌[root@parrot]-[/home/parrot]
└──→ #nikto --help
Unknown option: help
-config+ Use this config file
-Display+ Turn on/off display outputs
-dbcheck check database and other key files for syntax errors
-Format+ save file (-o) format
-Help Extended help information
-host+ target host
-id+ Host authentication to use, format is id:pass or id:pass:realm
-list-plugins List all available plugins
-output+ Write output to this file
-nossl Disables using SSL
-no404 Disables 404 checks
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-root+ Prepend root value to all requests, format is /directory
-ssl Force ssl mode on port
-Tuning+ Scan tuning
-timeout+ Timeout for requests (default 10 seconds)
-update Update databases and plugins from CIRT.net
-Version Print plugin and database versions
-vhost+ Virtual host (for Host header)
+ requires a value
Note: This is the short help output. Use -H for full help text.

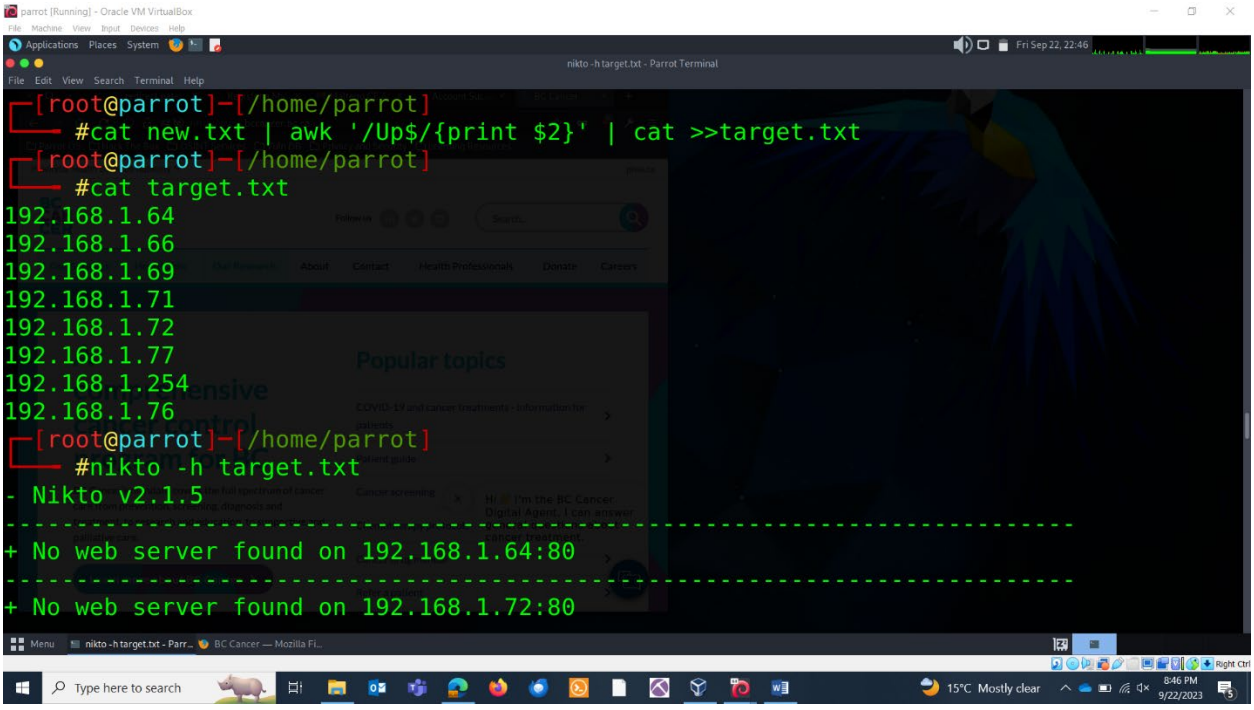
```
┌──[root@parrot]─[/home/parrot]
└─── #nikto -h tesla.com
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          104.89.118.48
+ Target Hostname:    tesla.com
+ Target Port:        80
+ Start Time:         2023-09-22 22:22:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-reference-error' found, with contents: 18.24b41160.1695435721.13acb0bd
+ Uncommon header 'permissions-policy' found, with contents: interest-cohort=()
^C┌──[✗]─[root@parrot]─[/home/parrot]
└─── #nikto -h tesla.com -ssl
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          104.89.118.48
+ Target Hostname:    tesla.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject: /C=US/ST=Texas/L=Austin/O=TESLA, INC./CN=*.tesla.com
                   Ciphers: TLS_AES_256_GCM_SHA384
                   Issuer:  /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=GeoTrust RSA CA 2018
+ Start Time:         2023-09-22 22:22:43 (GMT-4)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'strict-transport-security' found, with contents: max-age=15768000
+ Uncommon header 'x-reference-error' found, with contents: 18.66f06e68.1695435764.22456517
+ Uncommon header 'permissions-policy' found, with contents: interest-cohort=()
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server is using a wildcard certificate: '*.tesla.com'
^C┌──[✗]─[root@parrot]─[/home/parrot]
└─── #nikto -h testphp.vulnhub.com -ssl
- Nikto v2.1.5
```

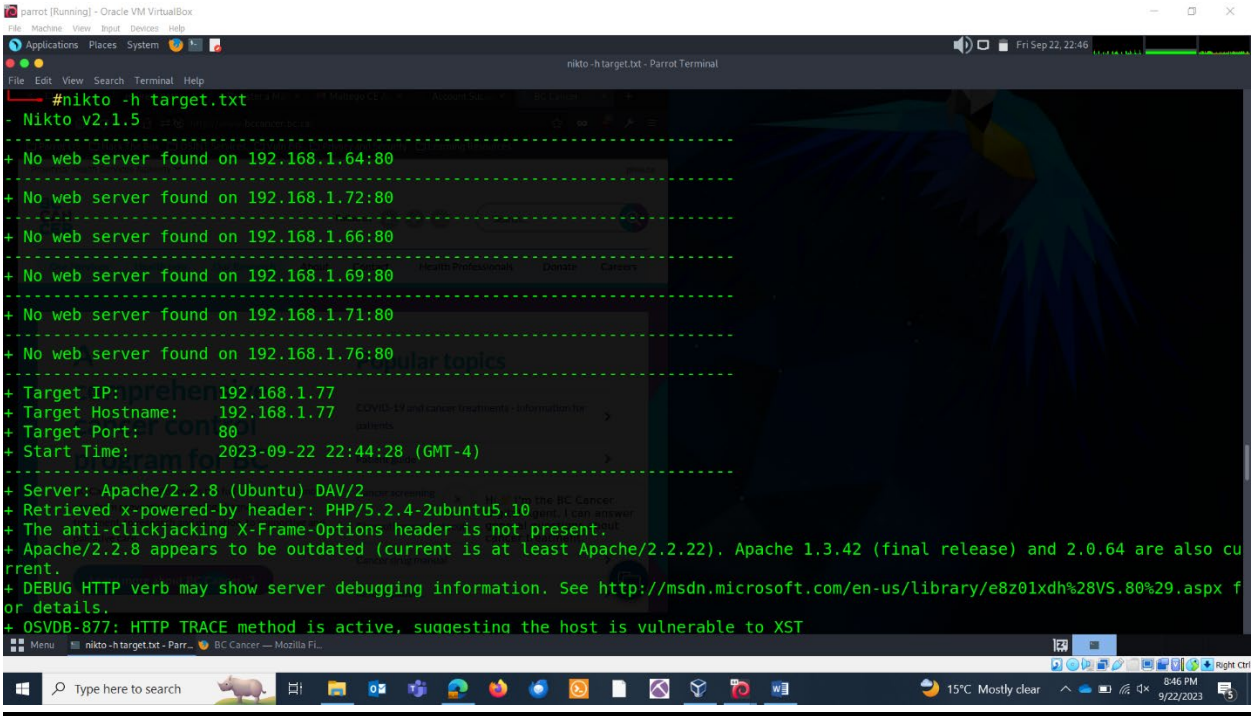


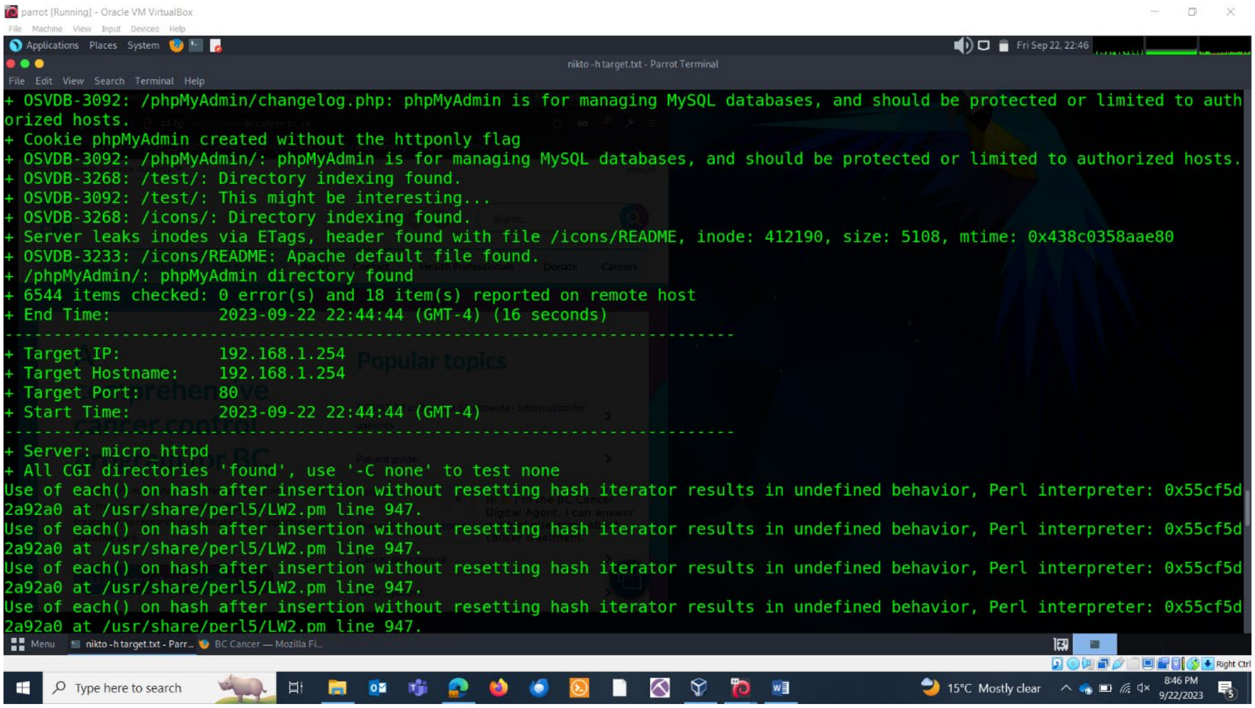

parrot [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Fri Sep 22, 22:39
nmap -p 80 192.168.1.0/24 -oG new.txt - Parrot Terminal
File Edit View Search Terminal Help
┌─[✗]─[root@parrot]─[/home/parrot]
└──╼ #ipcalc 192.168.1.77
bash: ipcalc: command not found
┌─[✗]─[root@parrot]─[/home/parrot]
└──╼ #apt install ipcalc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
ipcalc
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 27.8 kB of archives.
After this operation, 75.8 kB of additional disk space will be used.
Get:1 https://deb.parrot.sh/parrot lts/main amd64 ipcalc all 0.42-2 [27.8 kB]
Fetched 27.8 kB in 2s (11.2 kB/s)
Selecting previously unselected package ipcalc.
(Reading database ... 486018 files and directories currently installed.)
Preparing to unpack .../archives/ipcalc_0.42-2_all.deb ...
Unpacking ipcalc (0.42-2) ...
Setting up ipcalc (0.42-2) ...
Processing triggers for man-db (2.10.1-1~bpo11+1) ...
Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated
┌─[root@parrot]─[/home/parrot]
└──╼ #ipcalc 192.168.1.77
Address: 192.168.1.77 11000000.10101000.00000001. 01001101
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255 00000000.00000000.00000000. 11111111
=>
Network: 192.168.1.0/24 11000000.10101000.00000001. 00000000
HostMin: 192.168.1.1 11000000.10101000.00000001. 00000001
HostMax: 192.168.1.254 11000000.10101000.00000001. 11111110
Menu
nmap -p 80 192.168.1.0...
Right Ctrl
Type here to search
15°C Clear
8:39 PM
9/22/2023


parrot [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Fri Sep 22, 22:39
nmap -p 80 192.168.1.0/24 -oG new.txt - Parrot Terminal
File Edit View Search Terminal Help
┌─[root@parrot]─[/home/parrot]
└──╼ #ipcalc 192.168.1.77
Address: 192.168.1.77 11000000.10101000.00000001. 01001101
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255 00000000.00000000.00000000. 11111111
=>
Network: 192.168.1.0/24 11000000.10101000.00000001. 00000000
HostMin: 192.168.1.1 11000000.10101000.00000001. 00000001
HostMax: 192.168.1.254 11000000.10101000.00000001. 11111110
Broadcast: 192.168.1.255 11000000.10101000.00000001. 11111111
Hosts/Net: 254 Class C, Private Internet
┌─[root@parrot]─[/home/parrot]
└──╼ #nmap -p 80 192.168.1.0/24 -oG new.txt
Starting Nmap 7.93 (https://nmap.org) at 2023-09-22 22:35 EDT
Nmap scan report for 192.168.1.64
Host is up (0.051s latency).
PORT STATE SERVICE
80/tcp closed http
MAC Address: A0:67:20:36:63:CC (China Dragon Technology Limited)
Nmap scan report for 192.168.1.66
Host is up (0.30s latency).
PORT STATE SERVICE
80/tcp closed http
MAC Address: 88:83:5D:C8:35:A1 (Fn-link Technology Limited)
Nmap scan report for 192.168.1.69
Host is up (0.051s latency).
PORT STATE SERVICE
Menu
nmap -p 80 192.168.1.0...
Right Ctrl
Type here to search
15°C Clear
8:39 PM
9/22/2023

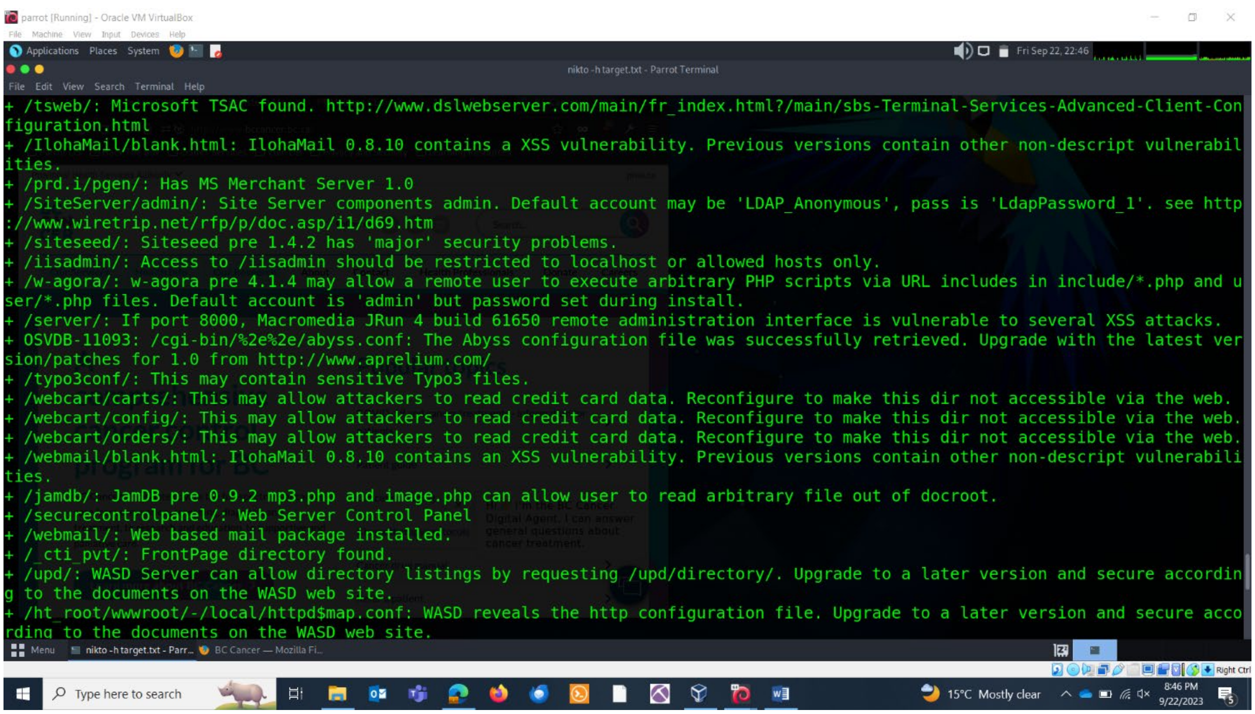

parrot [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Fri Sep 22, 22:39
nmap -p 80 192.168.1.0/24 -oG new.txt - Parrot Terminal
File Edit View Search Terminal Help
MAC Address: A0:67:20:36:63:CC (China Dragon Technology Limited)
Nmap scan report for 192.168.1.66
Host is up (0.30s latency).
PORT STATE SERVICE
80/tcp closed http
MAC Address: 88:83:5D:C8:35:A1 (Fn-link Technology Limited)
Nmap scan report for 192.168.1.69
Host is up (0.051s latency).
PORT STATE SERVICE
80/tcp closed http
MAC Address: 52:72:4B:22:AE:53 (Unknown)
Nmap scan report for 192.168.1.71
Host is up (0.0013s latency).
PORT STATE SERVICE
80/tcp filtered http
MAC Address: 04:6C:59:E4:BB:23 (Intel Corporate)
Nmap scan report for 192.168.1.72
Host is up (0.24s latency).
PORT STATE SERVICE
80/tcp closed http
MAC Address: 98:01:A7:A0:72:E5 (Apple)
Nmap scan report for 192.168.1.77
Host is up (0.00058s latency).
Menu
nmap -p 80 192.168.1.0...
Right Ctrl
Type here to search
15°C Clear
8:39 PM
9/22/2023


parrot [Running] - Oracle VM VirtualBox
Applications Places System
Fri Sep 22, 22:46
nikto -h target.txt - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/parrot]
#cat new.txt | awk '/Up$/{print $2}' | cat >>target.txt
[root@parrot]-[/home/parrot]
#cat target.txt
192.168.1.64
192.168.1.66
192.168.1.69
192.168.1.71
192.168.1.72
192.168.1.77
192.168.1.254
192.168.1.76
[root@parrot]-[/home/parrot]
#nikto -h target.txt
- Nikto v2.1.5
+ No web server found on 192.168.1.64:80
+ No web server found on 192.168.1.72:80
Menu
nikto -h target.txt - Parr...
BC Cancer — Mozilla Fi...
Type here to search
15°C Mostly clear
8:46 PM
9/22/2023

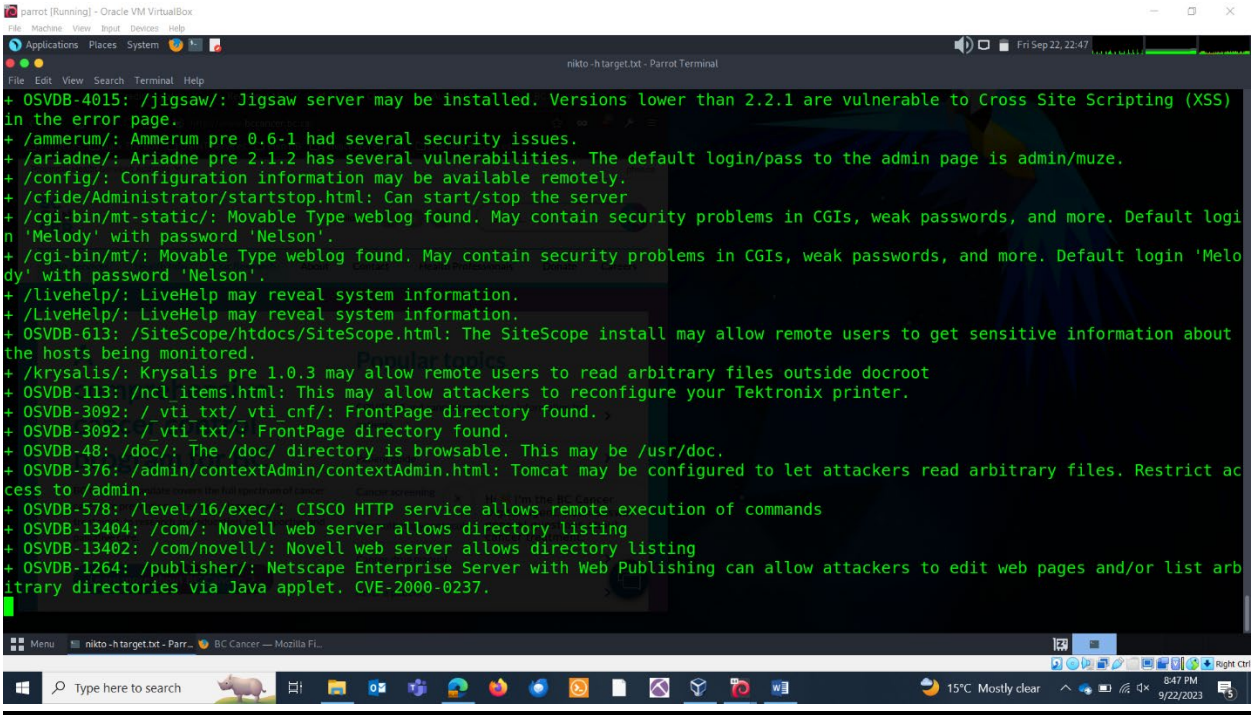

parrot [Running] - Oracle VM VirtualBox
Applications Places System
Fri Sep 22, 22:46
nikto -h target.txt - Parrot Terminal
File Edit View Search Terminal Help
#nikto -h target.txt
- Nikto v2.1.5
+ No web server found on 192.168.1.64:80
+ No web server found on 192.168.1.72:80
+ No web server found on 192.168.1.66:80
+ No web server found on 192.168.1.69:80
+ No web server found on 192.168.1.71:80
+ No web server found on 192.168.1.76:80
+ Target IP: 192.168.1.77
+ Target Hostname: 192.168.1.77
+ Target Port: 80
+ Start Time: 2023-09-22 22:44:28 (GMT-4)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also cu
rrent.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx f
or details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
Menu
nikto -h target.txt - Parr...
BC Cancer — Mozilla Fi...
Type here to search
15°C Mostly clear
8:46 PM
9/22/2023

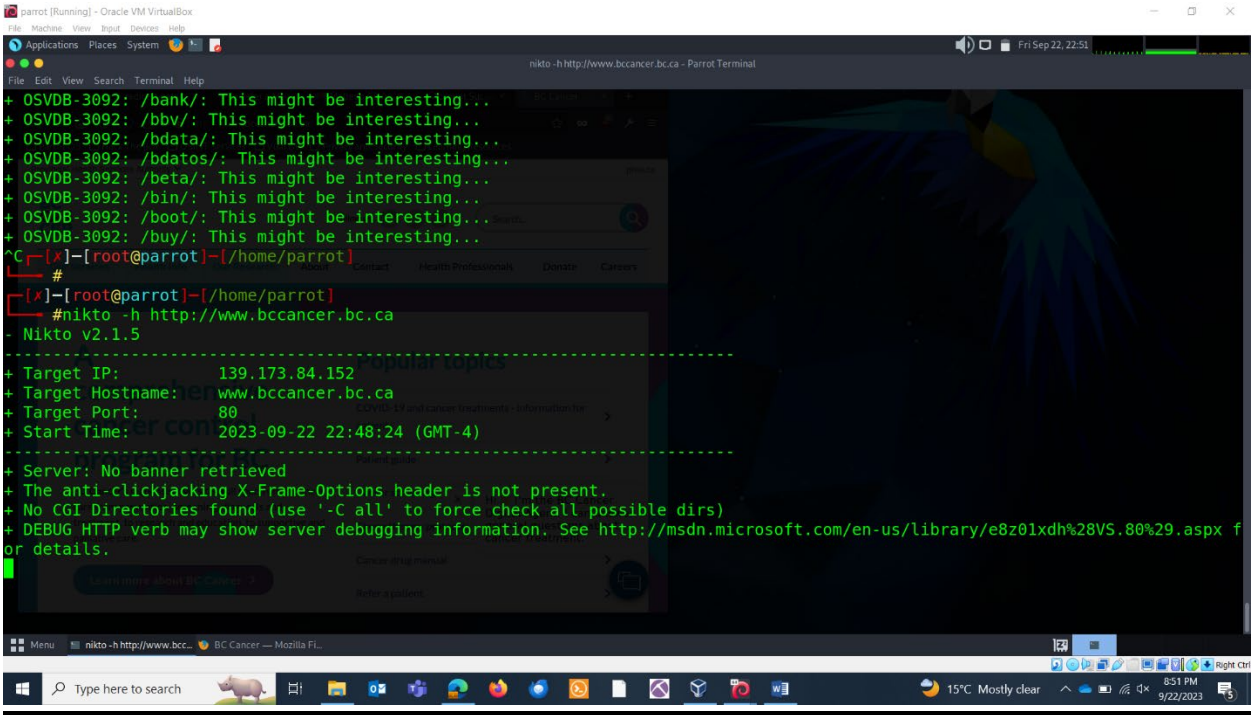


```
parrot [Running] - Oracle VM VirtualBox
nikto -h target.txt - Parrot Terminal
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Cookie phpMyAdmin created without the httponly flag
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, inode: 412190, size: 5108, mtime: 0x438c0358aae80
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2023-09-22 22:44:44 (GMT-4) (16 seconds)
---------------------------------------------------------------------------
+ Target IP:          192.168.1.254
+ Target Hostname:    192.168.1.254
+ Target Port:        80
+ Start Time:         2023-09-22 22:44:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: micro_httpd
+ All CGI directories 'found', use '-C none' to test none
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x55cf5d2a92a0 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: 0x55cf5d2a92a0 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: 0x55cf5d2a92a0 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: 0x55cf5d2a92a0 at /usr/share/perl5/LW2.pm line 947.
```



```
parrot [Running] - Oracle VM VirtualBox
nikto -h target.txt - Parrot Terminal
+ /tsweb/: Microsoft TSAC found. http://www.dslwebserver.com/main/fr_index.html?/main/sbs-Terminal-Services-Advanced-Client-Configuration.html
+ /IlohaMail/blank.html: IlohaMail 0.8.10 contains a XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /prd.i/pgen/: Has MS Merchant Server 1.0
+ /SiteServer/admin/: Site Server components admin. Default account may be 'LDAP_Anonymous', pass is 'LdapPassword_1'. see http://www.wiretrip.net/rfp/p/doc.asp/i1/d69.htm
+ /siteseed/: Siteseed pre 1.4.2 has 'major' security problems.
+ /iisadmin/: Access to /iisadmin should be restricted to localhost or allowed hosts only.
+ /w-agora/: w-agora pre 4.1.4 may allow a remote user to execute arbitrary PHP scripts via URL includes in include/*.php and user/*.php files. Default account is 'admin' but password set during install.
+ /server/: If port 8000, Macromedia JRun 4 build 61650 remote administration interface is vulnerable to several XSS attacks.
+ OSVDB-11093: /cgi-bin/%2e%2e/abyss.conf: The Abyss configuration file was successfully retrieved. Upgrade with the latest version/patches for 1.0 from http://www.aprelium.com/.
+ /typo3conf/: This may contain sensitive Typo3 files.
+ /webcart/carts/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
+ /webcart/config/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
+ /webcart/orders/: This may allow attackers to read credit card data. Reconfigure to make this dir not accessible via the web.
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /jamdb/: JamDB pre 0.9.2 mp3.php and image.php can allow user to read arbitrary file out of docroot.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ /_cti_pvt/: FrontPage directory found.
+ /upd/: WASD Server can allow directory listings by requesting /upd/directory/. Upgrade to a later version and secure according to the documents on the WASD web site.
+ /ht_root/wwwroot/-/local/httpd$map.conf: WASD reveals the http configuration file. Upgrade to a later version and secure according to the documents on the WASD web site.
```


parrot [Running] - Oracle VM VirtualBox
Applications Places System
Fri Sep 22, 22:47
nikto -h target.txt - Parrot Terminal
File Edit View Search Terminal Help
+ OSVDB-4015: /jigsaw/: Jigsaw server may be installed. Versions lower than 2.2.1 are vulnerable to Cross Site Scripting (XSS) in the error page.
+ /ammerum/: Ammerum pre 0.6-1 had several security issues.
+ /ariadne/: Ariadne pre 2.1.2 has several vulnerabilities. The default login/pass to the admin page is admin/muze.
+ /config/: Configuration information may be available remotely.
+ /cfide/Administrator/startstop.html: Can start/stop the server
+ /cgi-bin/mt-static/: Movable Type weblog found. May contain security problems in CGIs, weak passwords, and more. Default login 'Melody' with password 'Nelson'.
+ /cgi-bin/mt/: Movable Type weblog found. May contain security problems in CGIs, weak passwords, and more. Default login 'Melody' with password 'Nelson'.
+ /livehelp/: LiveHelp may reveal system information.
+ /LiveHelp/: LiveHelp may reveal system information.
+ OSVDB-613: /SiteScope/htdocs/SiteScope.html: The SiteScope install may allow remote users to get sensitive information about the hosts being monitored.
+ /krysalis/: Krysalis pre 1.0.3 may allow remote users to read arbitrary files outside docroot
+ OSVDB-113: /ncl_items.html: This may allow attackers to reconfigure your Tektronix printer.
+ OSVDB-3092: /_vti_txt/_vti_cnf/: FrontPage directory found.
+ OSVDB-3092: /_vti_txt/: FrontPage directory found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-376: /admin/contextAdmin/contextAdmin.html: Tomcat may be configured to let attackers read arbitrary files. Restrict access to /admin.
+ OSVDB-578: /level/16/exec/: CISCO HTTP service allows remote execution of commands
+ OSVDB-13404: /com/: Novell web server allows directory listing
+ OSVDB-13402: /com/novell/: Novell web server allows directory listing
+ OSVDB-1264: /publisher/: Netscape Enterprise Server with Web Publishing can allow attackers to edit web pages and/or list arbitrary directories via Java applet. CVE-2000-0237.
Menu
nikto -h target.txt - Parr...
BC Cancer — Mozilla Fi...
Type here to search
15°C Mostly clear
8:47 PM
9/22/2023


parrot [Running] - Oracle VM VirtualBox
Applications Places System
Fri Sep 22, 22:51
nikto -h http://www.bccancer.bc.ca - Parrot Terminal
File Edit View Search Terminal Help
+ OSVDB-3092: /bank/: This might be interesting...
+ OSVDB-3092: /bbv/: This might be interesting...
+ OSVDB-3092: /bdata/: This might be interesting...
+ OSVDB-3092: /bdatos/: This might be interesting...
+ OSVDB-3092: /beta/: This might be interesting...
+ OSVDB-3092: /bin/: This might be interesting...
+ OSVDB-3092: /boot/: This might be interesting...
+ OSVDB-3092: /buy/: This might be interesting...
^C┌─[x]─[root@parrot]─[/home/parrot]
└── #
┌─[x]─[root@parrot]─[/home/parrot]
└── #nikto -h http://www.bccancer.bc.ca
- Nikto v2.1.5

+ Target IP: 139.173.84.152
+ Target Hostname: www.bccancer.bc.ca
+ Target Port: 80
+ Start Time: 2023-09-22 22:48:24 (GMT-4)

+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
Menu
nikto -h http://www.bcc...
BC Cancer — Mozilla Fi...
Type here to search
15°C Mostly clear
8:51 PM
9/22/2023