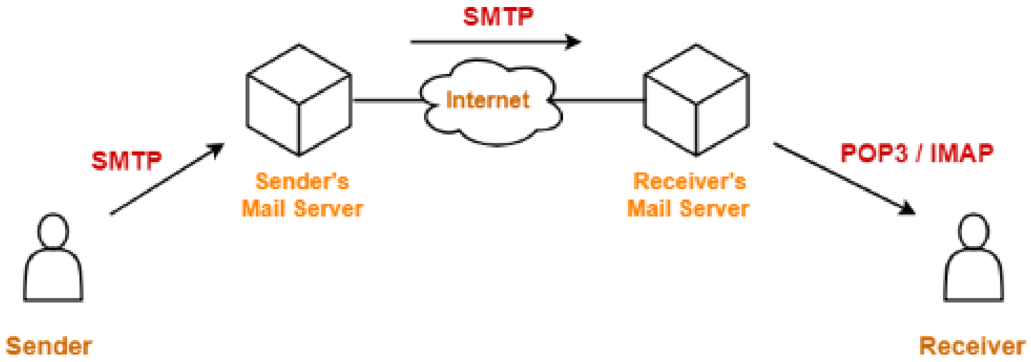
EXPLOITING SERVER VULNERABILITIES

1)SMTP

SMTP (Simple Mail Transfer Protocol) is a widely used protocol for sending email messages over the Internet. In Kali Linux, just like in any other Linux distribution, you can use SMTP to send email messages from the command line or through a scripting language like Python. SMTP is a crucial tool for various purposes, such as automated notifications, alerting, or sending reports



1. Overview

smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN and RCPT TO commands. It could be adapted to work against other vulnerable SMTP daemons, but this hasn't been done as of v1.0.

2.Installation

smtp-user-enum is just a stand alone PERL script, so installation is as simple as copying it to your path (e.g. /usr/local/bin). It has only been tested under Linux so far. It depends on the following PERL modules which you may need to install first:

- Socket
- IO::Handle
- IO::Select
- IO::Socket::INET
- Getopt::Std

If you have PERL installed, you should be able to install the modules from CPAN: # perl -MCPAN -e shell cpan> install Getopt::Std

3. Usage smtp-user-enum simply needs to be passed a list of users and at least one target running an SMTP service.

smtp-user-enum v1.0 (http://pentestmonkey.net/tools/smtp-user-enum)

Usage: smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)

```
options are:
 -m   n  Maximum number of processes (default: 5)
-M mode   Method to use for username guessing EXPN, VRFY or RCPT (default:
VRFY) -u user Check if user exists on remote system
-f addr From email address to use for "RCPT TO" guessing (default:
user@example.com)
-U file    File of usernames to check via smtp service
-t host   Server host running smtp service
-T file     File of hostnames running the smtp service
-p port   TCP port on which smtp service runs (default: 25)
-d Debugging output
-t n Wait a maximum of n seconds for reply (default: 5)
-v Verbose
-h This help message
```

4. Some Examples

For all of the examples below we need a list of potential usernames. The following output demonstrates the format for this list:

```
$ head users.txt
 Root
 Bin
 Daemon
 Adm
 lp
Sync
 Shutdown
 Halt
 mail
News
```

4.1 Using the SMTP VRFY Command

The output below shows how the SMTP server responds differently to VRFY requests for valid and invalid users. It is recommended that a manual check like the following is carried out before running smtp-user-enum. Obviously the tool won’t work if the server doesn’t respond differently to requests for valid and invalid users.

```
$ telnet 10.0.0.1 25
Trying 10.0.0.1... Connected to 10.0.0.1.
 Escape character is ’^]’.
220 myhost ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
```

```
250 myhost Hello [10.0.0.99], pleased to meet you VRFY root
250 Super-User <root@myhost>
VRFY blah 550 blah... User unknown
```

To use smtp-user-enum to enumerate valid usernames using the VRFY command, first prepare a list of usernames (users.txt) and run the tool as follows: $ smtp-user-enum.pl -M VRFY -U users.txt -t 10.0.0.1 Starting smtp-user-enum v1.0 (http://pentestmonkey.net/tools/smtp-user-enum)

```
----------------------------------------------------------
| Scan Information |
----------------------------------------------------------
Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 47
Target TCP port .......... 25
Query timeout ............ 5 secs
Relay Server ............. Not used
######## Scan started at Sun AUG 27 18:01:50 2023 #########
root@10.0.0.1: Exists
bin@10.0.0.1: Exists
daemon@10.0.0.1: Exists
lp@10.0.0.1: Exists
adm@10.0.0.1: Exists
uucp@10.0.0.1: Exists
postmaster@10.0.0.1: Exists
nobody@10.0.0.1: Exists
ftp@10.0.0.1: Exists


######## Scan completed at AUG 27 18:01:50 2023#########
9 results.
47 queries in 1 seconds (47.0 queries / sec)
```

It’s worth noting that postmaster is not actually a valid OS-level user account
- it’s a mail alias.

4.2 Using the SMTP EXPN Command

The output below shows how the SMTP server responds differently to EXPN requests for valid and invalid users.

```
$ telnet 10.0.0.1 25
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is ’^]’.
220 myhost ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 myhost Hello [10.0.0.99], pleased to meet you
EXPN root
250 Super-User <root@myhost>
EXPN blah
550 blah... User unknown
```

To use smtp-user-enum to enumerate valid usernames using the VRFY command, first prepare a list of usernames (users.txt) and run the tool as follows (unsurprisingly, we get the same results as above):

```
$ smtp-user-enum.pl -M EXPN -U users.txt -t 10.0.0.1
Starting smtp-user-enum v1.0 ( http://pentestmonkey.net/tools/smtp-user-enum )
----------------------------------------------------------
| Scan Information |
----------------------------------------------------------
Mode ..................... EXPN
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 47
Target TCP port .......... 25
Query timeout ............ 5 secs
Relay Server ............. Not used
######## Scan started at Sun Jan 21 18:01:50 2007 #########
root@10.0.0.1: Exists
bin@10.0.0.1: Exists
daemon@10.0.0.1: Exists
lp@10.0.0.1: Exists
adm@10.0.0.1: Exists
uucp@10.0.0.1: Exists
postmaster@10.0.0.1: Exists
nobody@10.0.0.1: Exists
ftp@10.0.0.1: Exists
######## Scan completed at Sun Jan 21 18:01:50 2007 #########
9 results.
47 queries in 1 seconds (47.0 queries / sec)
```

4.3 Using the SMTP RCPT TO Command

The output below shows how the SMTP server responds differently to RCPT TO requests for valid and invalid users. This is often to the most useful technique as VRFY and EXPN are often disabled to prevent username enumeration.

```
$ telnet 10.0.0.1 25
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is ’^]’.
220 myhost ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 myhost Hello [10.0.0.99], pleased to meet you
MAIL FROM:root
250 root... Sender ok
RCPT TO:root
250 root... Recipient ok
RCPT TO: blah
550 blah... User unknown
```

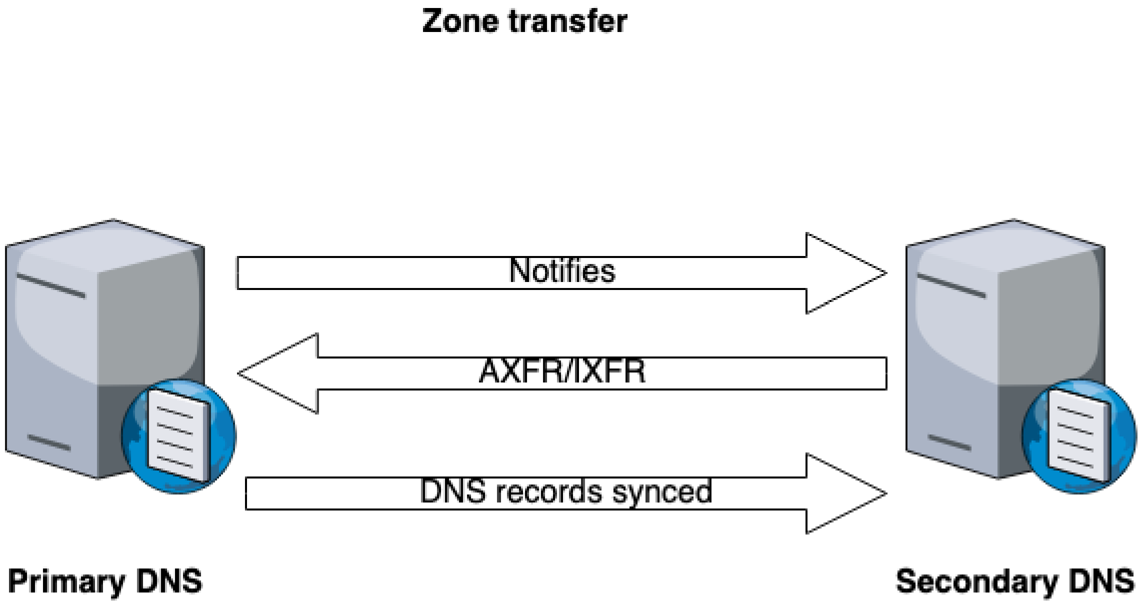
To use smtp-user-enum to enumerate valid usernames using the RCPT TO command, first prepare a list of usernames (users.txt) and run the tool as follows (again, the results are the same as above):

```
$ smtp-user-enum.pl -M RCPT -U users.txt -t 10.0.0.1
Starting smtp-user-enum v1.0 ( http://pentestmonkey.net/tools/smtp-user-enum )
----------------------------------------------------------
| Scan Information |
----------------------------------------------------------
Mode ..................... RCPT
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 47
Target TCP port .......... 25
Query timeout ............ 5 secs
Relay Server ............. Not used
######## Scan started at Sun Jan 21 18:01:50 2007 #########
root@10.0.0.1: Exists
bin@10.0.0.1: Exists
daemon@10.0.0.1: Exists
lp@10.0.0.1: Exists
adm@10.0.0.1: Exists
```

```
uucp@10.0.0.1: Exists
postmaster@10.0.0.1: Exists
nobody@10.0.0.1: Exists
ftp@10.0.0.1: Exists
######## Scan completed at Sun Jan 21 18:01:50 2007 #########
9 results.
47 queries in 1 seconds (47.0 queries / sec)
```

2)Zone Transfers

Zone transfer, in the context of cybersecurity and Domain Name System (DNS), refers to the process of replicating DNS data (zone data) from a primary DNS server to one or more secondary DNS servers. This mechanism helps distribute the responsibility for resolving domain names across multiple servers, ensuring redundancy and fault tolerance. However, if not configured securely, zone transfers can become a significant security risk.



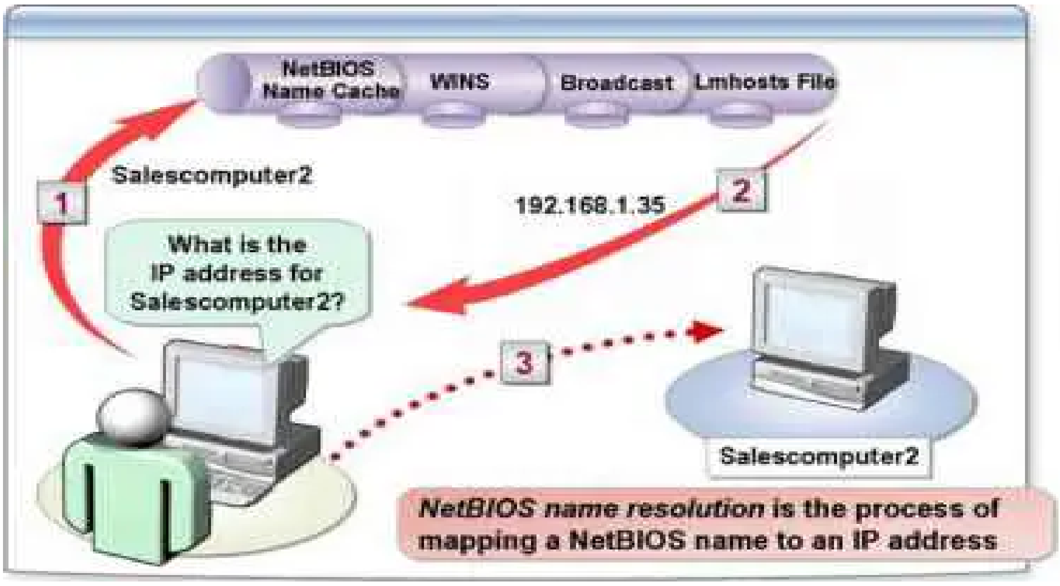
DNS zone transfers are a tool for domain name administrators to replicate their DNS databases across their organisation's DNS servers. The problem that arises is that this can reveal a great deal of information about an organisation's infrastructure. For this reason, typically, DNS servers are configured to not allow a zone transfer. To attempt a zone transfer using dnsrecon, we would use the -a flag (AXFR), or you can use the -t flag with type axfr. The axfr type is the query type that denotes DNS zone transfer. The command to run a zone transfer would look like the following:

```
dnsrecon -d google.com -a
```

```
root@kali:-# dns recon -d google.com -a
[*] Performing General Enumeration of Domain: google.com
[*] Checking for Zone Transfer for google.com name servers
[*] Resolving SOA Record
SOA ns3.google.com 216.239.36.10 Resolving NS Records NS Servers found:
NS ns4.google.com 216.239.38.10 NS ns1.google.com 216.239.32.10
NS ns2.google.com 216.239.34.10
NS ns3.google.com 216.239.36.10
Removing any duplicate NS server IP Addresses...

[*] Trying NS server 216.239.36.10
216.239.36.10 Has port 53 TCP Open Zone Transfer Failed!
No answer or RRset not for qname

[*] Trying NS server 216.239.34.10
[*] 216.239.34.10 Has port 53 TCP Open [-] Zone Transfer Failed!
No answer or RRset not for qname
[*]

[*] Trying NS server 216.239.32.10
216.239.32.10 Has port 53 TCP Open
Zone Transfer Failed!

No answer or RRset not for qname

Trying NS server 216.239.38.10 216.239.38.10 Has port 53 TCP Open Zone
Transfer Failed!
No answer or RRset not for qname
Checking for Zone Transfer for google.com name servers Resolving SOA Record
SOA ns3.google.com 216.239.36.10 Resolving NS Records
NS Servers found:
NS ns4.google.com 216.239.38.10
NS ns1.google.com 216.239.32.10
NS ns2.google.com 216.239.34.10
```

3)NetBIOS

NetBIOS provides communication services on local networks. It uses a software protocol called NetBIOS Frames that allows applications and computers on a local area network to communicate with network hardware and to transmit data across the network.NetBIOS, an abbreviation for Network Basic Input/Output System, is a networking industry standard. It was created in 1983 by Sytek and is often used with the NetBIOS over TCP/IP protocol. However, it's also used in Token Ring networks, as well as by Microsoft Windows.


NetBIOS Name Cache
WINS
Broadcast
Lmhosts File
Salescomputer2
1
What is the IP address for Salescomputer2?
192.168.1.35
2
3
Salescomputer2
NetBIOS name resolution is the process of mapping a NetBIOS name to an IP address

nbtscan

NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address (such as Ethernet).

This program is useful for security checks, network discovery and forensics investigations.

Installed size: 57 KB
How to install: sudo apt install nbtscan

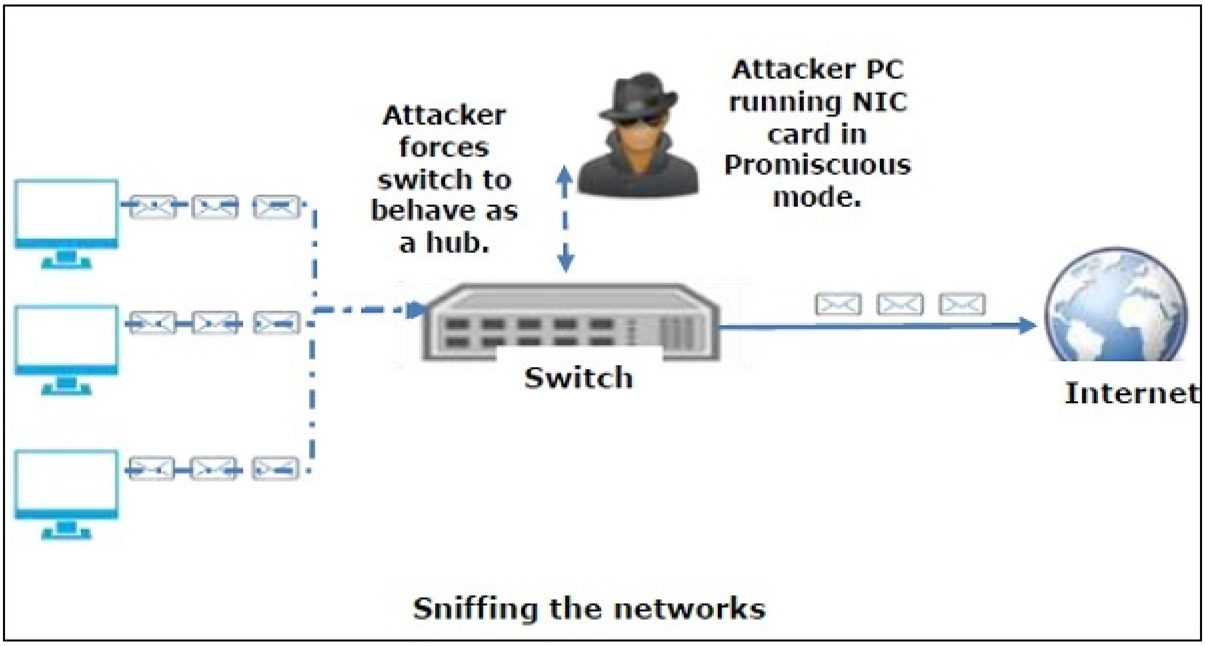
```
root@kali:~# nbtscan --help

NBTscan version 1.7.2.
This is a free software and it comes with absolutely no warranty.
```

```
You can use, distribute and modify it under terms of GNU GPL 2+.


Usage:
nbtscan [-v] [-d] [-e] [-l] [-t timeout] [-b bandwidth] [-r] [-q] [-s separator] [-m retransmits]
(-f filename)|(<scan_range>)
        -v              verbose output. Print all names received
                        from each host
        -d              dump packets. Print whole packet contents.
        -e              Format output in /etc/hosts format.
        -l              Format output in lmhosts format.
                        Cannot be used with -v, -s or -h options.
        -t timeout      wait timeout milliseconds for response.
                        Default 1000.
        -b bandwidth    Output throttling. Slow down output
                        so that it uses no more that bandwidth bps.
                        Useful on slow links, so that ougoing queries
                        don't get dropped.
        -r              use local port 137 for scans. Win95 boxes
                        respond to this only.
                        You need to be root to use this option on Unix.
        -q              Suppress banners and error messages,
        -s separator    Script-friendly output. Don't print
                        column and record headers, separate fields with separator.
        -h              Print human-readable names for services.
                        Can only be used with -v option.
        -m retransmits          Number of retransmits. Default 0.
        -f filename     Take IP addresses to scan from file filename.
                        -f - makes nbtscan take IP addresses from stdin.
        <scan_range>            what to scan. Can either be single IP
                        like 192.168.1.1 or
                        range of addresses in one of two forms:
                        xxx.xxx.xxx.xxx/xx or xxx.xxx.xxx.xxx-xxx.
Examples:
        nbtscan -r 192.168.1.0/24
                Scans the whole C-class network.
        nbtscan 192.168.1.25-137
                Scans a range from 192.168.1.25 to 192.168.1.137
        nbtscan -v -s : 192.168.1.0/24
                Scans C-class network. Prints results in script-friendly
                format using colon as field separator.
                Produces output like that:
```

```
          192.168.0.1:NT_SERVER:00U
          192.168.0.1:MY_DOMAIN:00G
          192.168.0.1:ADMINISTRATOR:03U
          192.168.0.2:OTHER_BOX:00U
          ...
nbtscan -f iplist
          Scans IP addresses specified in file iplist.
```

4)Sniffing

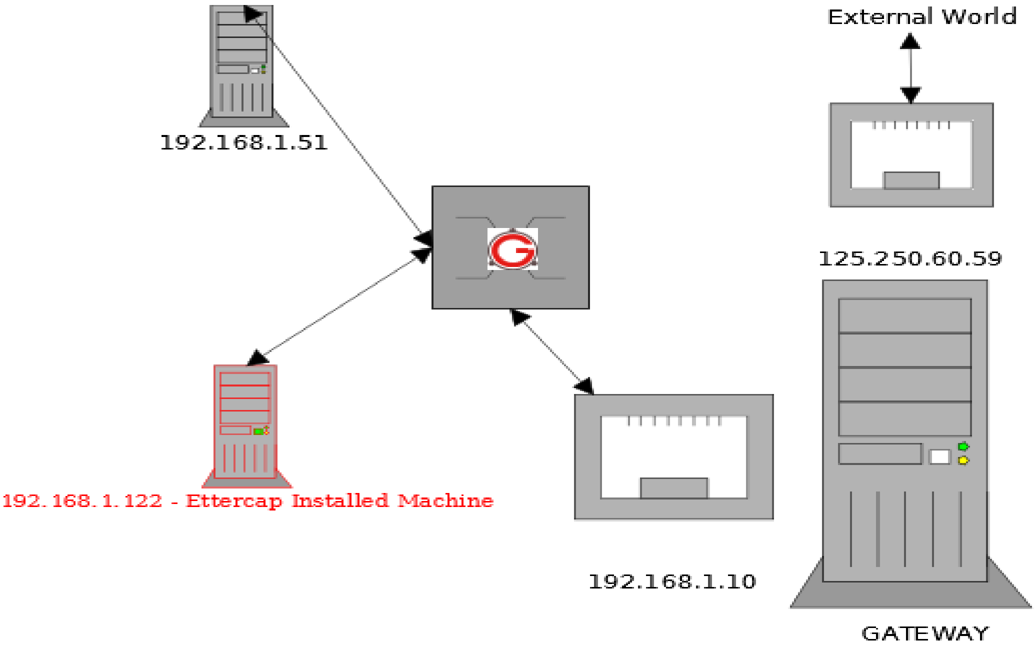
Sniffing is the process in which all the data packets passing in the network are monitored. Sniffers are usually used by network administrators to monitor and troubleshoot the network traffic. Whereas attackers use Sniffers to monitor and capture data packets to steal sensitive information containing password and user accounts. Sniffers can be hardware or software installed on the system.


Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet

Sniffing the networks

a)Ettercap

Ettercap is an open-source tool that can be used to support man-in-the-middle attacks on networks. Ettercap can capture packets and then write them back onto the network. Ettercap enables the diversion and alteration of data virtually in real-time. Ettercap can also be used for the protocol analysis necessary to analyse network traffic.

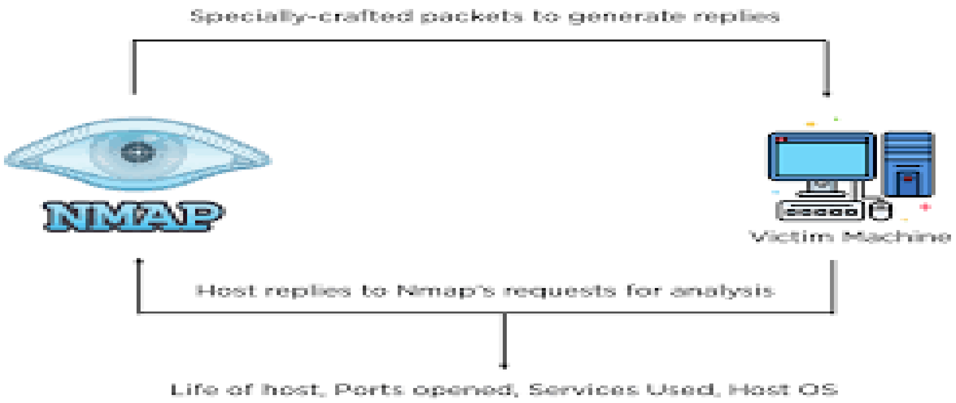


```
root@kali:~# ettercap -h

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team


Usage: ettercap [OPTIONS] [TARGET1] [TARGET2]

TARGET is in the format MAC/IP/IPv6/PORTs (see the man for further detail)

Sniffing and Attack options:
  -M, --mitm <METHOD:ARGS>     perform a mitm attack
  -o, --only-mitm              don't sniff, only perform the mitm attack
  -b, --broadcast              sniff packets destined to broadcast
  -B, --bridge <IFACE>         use bridged sniff (needs 2 ifaces)
  -p, --nopromisc              do not put the iface in promisc mode
  -S, --nosslmitm              do not forge SSL certificates
  -u, --unoffensive            do not forward packets
  -r, --read <file>            read data from pcapfile <file>
  -f, --pcapfilter <string>    set the pcap filter <string>
  -R, --reversed               use reversed TARGET matching
  -t, --proto <proto>          sniff only this proto (default is all)
      --certificate <file>     certificate file to use for SSL MiTM
      --private-key <file>     private key file to use for SSL MiTM

User Interface Type:
  -T, --text                   use text only GUI
       -q, --quiet                  do not display packet contents
```

```
     -s, --script <CMD>          issue these commands to the GUI
  -C, --curses                use curses GUI
  -D, --daemon                daemonize ettercap (no GUI)
  -G, --gtk                   use GTK+ GUI

Logging options:
  -w, --write <file>          write sniffed data to pcapfile <file>
  -L, --log <logfile>         log all the traffic to this <logfile>
  -l, --log-info <logfile>    log only passive infos to this <logfile>
  -m, --log-msg <logfile>     log all the messages to this <logfile>
  -c, --compress              use gzip compression on log files

Visualization options:
  -d, --dns                   resolves ip addresses into hostnames
  -V, --visual <format>       set the visualization format
  -e, --regex <regex>         visualize only packets matching this regex
  -E, --ext-headers           print extended header for every pck
  -Q, --superquiet            do not display user and password

LUA options:
     --lua-script <script1>,[<script2>,...]     comma-separted list of LUA scripts
        --lua-args n1=v1,[n2=v2,...]                  comma-separated arguments to LUA
script(s)

General options:
  -i, --iface <iface>         use this network interface
  -I, --liface                show all the network interfaces
  -Y, --secondary <ifaces>    list of secondary network interfaces
  -n, --netmask <netmask>     force this <netmask> on iface
  -A, --address <address>     force this local <address> on iface
  -P, --plugin <plugin>       launch this <plugin> - multiple occurance allowed
     --plugin-list <plugin1>,[<plugin2>,...]       comma-separated list of plugins
  -F, --filter <file>         load the filter <file> (content filter)
  -z, --silent                do not perform the initial ARP scan
  -6, --ip6scan               send ICMPv6 probes to discover IPv6 nodes on the link
  -j, --load-hosts <file>     load the hosts list from <file>
  -k, --save-hosts <file>     save the hosts list to <file>
  -W, --wifi-key <wkey>       use this key to decrypt wifi packets (wep or wpa)
  -a, --config <config>       use the alternative config file <config>

Standard options:
  -v, --version               prints the version and exit
  -h, --help                  this help screen
```

b)Nmap

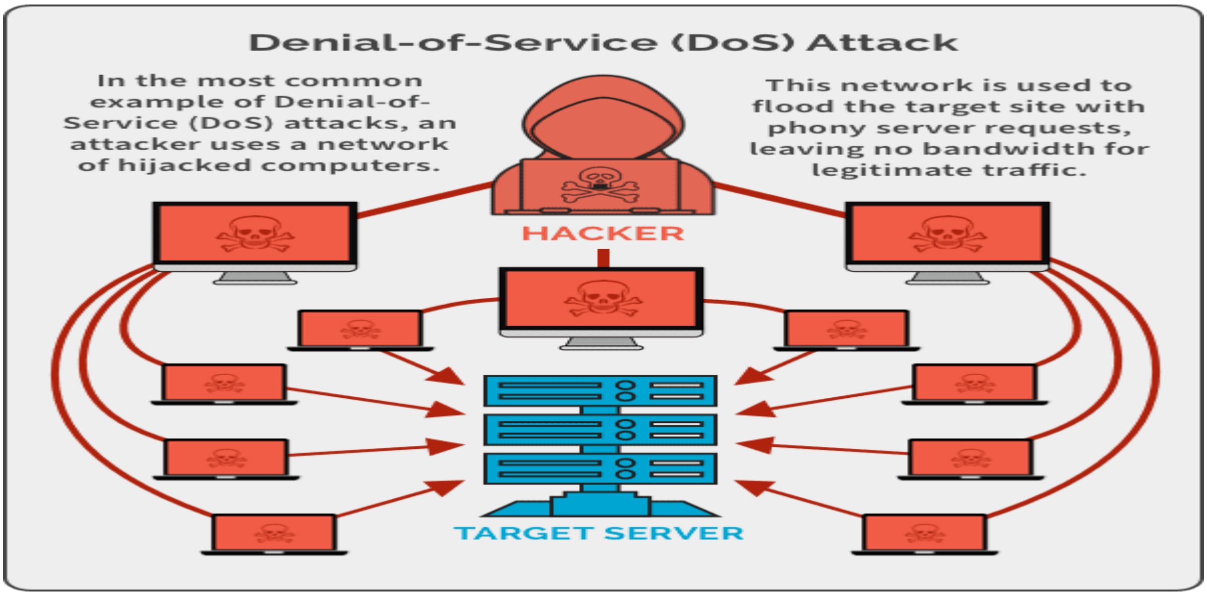
Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.


Specially-crafted packets to generate replies
NMAP
Victim Machine
Host replies to Nmap's requests for analysis
Life of host, Ports opened, Services Used, Host OS

```
root@kali:~# nmap -v -A -sV 192.168.1.1

Starting Nmap 6.45 ( http://nmap.org ) at 2014-05-13 18:40 MDT
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 18:40
Scanning 192.168.1.1 [1 port]
Completed ARP Ping Scan at 18:40, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:40
Completed Parallel DNS resolution of 1 host. at 18:40, 0.00s elapsed
Initiating SYN Stealth Scan at 18:40
Scanning router.localdomain (192.168.1.1) [1000 ports]
Discovered open port 53/tcp on 192.168.1.1
Discovered open port 22/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 3001/tcp on 192.168.1.1
```

5)DoS

A DoS (denial-of-service) attack is a cyberattack that makes a computer or other device unavailable to its intended users. This is usually accomplished by overwhelming the targeted machine with requests until normal traffic can no longer be processed. With a DoS attack, a single computer launches the attack.



Denial-of-Service (DoS) Attack

In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.

This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.

dos2unix

This package contains utilities dos2unix, unix2dos, mac2unix, unix2mac to convert the line endings of text files between UNIX (LF), DOS (CRLF) and Mac (CR) formats.

Text files under Windows and DOS typically have two ASCII characters at the end of each line: CR (carriage return) followed by LF (line feed). Older Macs used just CR, while UNIX uses just LF. While most modern editors can read all these formats, there may still be a need to convert files between them.

This is the classic utility developed in 1989.

Installed size: `1.80 MB`

How to install: `sudo apt install dos2unix`

```
root@kali:~# dos2unix -h
Usage: dos2unix [options] [file ...] [-n infile outfile ...]
 --allow-chown        allow file ownership change
 -ascii               convert only line breaks (default)
 -iso                 conversion between DOS and ISO-8859-1 character set
   -1252              use Windows code page 1252 (Western European)
```

```
  -437             use DOS code page 437 (US) (default)
  -850             use DOS code page 850 (Western European)
  -860             use DOS code page 860 (Portuguese)
  -863             use DOS code page 863 (French Canadian)
  -865             use DOS code page 865 (Nordic)
-7                 convert 8 bit characters to 7 bit space
-b, --keep-bom        keep Byte Order Mark
-c, --convmode        conversion mode
  convmode           ascii, 7bit, iso, mac, default to ascii
-e, --add-eol         add a line break to the last line if there isn't one
-f, --force           force conversion of binary files
-h, --help            display this help text
-i, --info[=FLAGS]    display file information
  file ...           files to analyze
-k, --keepdate        keep output file date
-L, --license         display software license
-l, --newline         add additional newline
-m, --add-bom         add Byte Order Mark (default UTF-8)
-n, --newfile         write to new file
  infile             original file in new-file mode
  outfile            output file in new-file mode
--no-allow-chown      don't allow file ownership change (default)
--no-add-eol          don't add a line break to the last line if there isn't one (default)
-O, --to-stdout       write to standard output
-o, --oldfile         write to old file (default)
  file ...           files to convert in old-file mode
-q, --quiet           quiet mode, suppress all warnings
-r, --remove-bom      remove Byte Order Mark (default)
-s, --safe            skip binary files (default)
-u,  --keep-utf16     keep UTF-16 encoding
-ul, --assume-utf16le assume that the input format is UTF-16LE
-ub, --assume-utf16be assume that the input format is UTF-16BE
-v,  --verbose        verbose operation
-F, --follow-symlink  follow symbolic links and convert the targets
-R, --replace-symlink replace symbolic links with converted files
                      (original target files remain unchanged)
-S, --skip-symlink    keep symbolic links and targets unchanged (default)
-V, --version         display version number
```