Sri Lanka Institute of Information Technology

Penetration Testing Report

Individual Assignment

IE3022 – Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT20620066	Weththasinghe M N G

Date of Submission
29/10/2022

Contents

Introduction

In an ideal world, software and systems would have been created from the ground up to be free of harmful security defects. Pen testing provides information on the success of that goal. Pen testing can benefit a company,

- Identify system weaknesses
- Evaluate the reliability of the controls
- Encourage adherence to data privacy and security laws (e.g., PCI DSS, HIPAA, GDPR)
- Provide management with qualitative and quantitative evidence of the existing security posture and budget priorities.

<u>The pen testing technique consists of five parts.</u>

1. Preparation and reconnaissance

The first stage entails defining a test's scope and goals, as well as the systems to be covered and the testing methodologies to be employed. Obtaining intelligence (e.g., networking and domain names, mail server) to better explain how a target operates and potential weaknesses.

2. Examining

This is usually done with:

Static analysis is the process of inspecting an application's code to estimate how it will behave while operating. These tools can scan the full code in a single process.

Dynamic analysis is the process of inspecting an application's code while it is executing.

3. Obtaining Entry

To uncover holes in a target, this step involves web application attacks such as cross-site scripting, SQL injection, and backdoors.

4. Keeping access

The purpose of this stage is to determine whether the vulnerabilities can be abused to maintain a firm hold in the compromised system long enough to allow a bad actor to get in-depth access.

5. Evaluation

The penetration test results are then collected into a report that includes particular flaws that were exploited, access to sensitive information, and the duration of time the pen tester was able to stay unnoticed in the system.

Scenario

Netflix is a streaming service that requires a subscription and enables users to watch movies and TV shows without ads on any internet-connected device. A network will be subjected to penetration testing by the pen testing team. The red, blue, and purple teams are the three groups that contributed to this project. The red team's objective is to evaluate the network's current ability to withstand attacks. The blue team will indeed assess the red team's work to spot any flaws. The purple team will assess the blue team's recommendations to fix the flaws that the red team found.

The goal of this study was to find and fix the various problems with netflix networking systems. The study's conclusions were used to create a plan to increase the security of the networks operations.

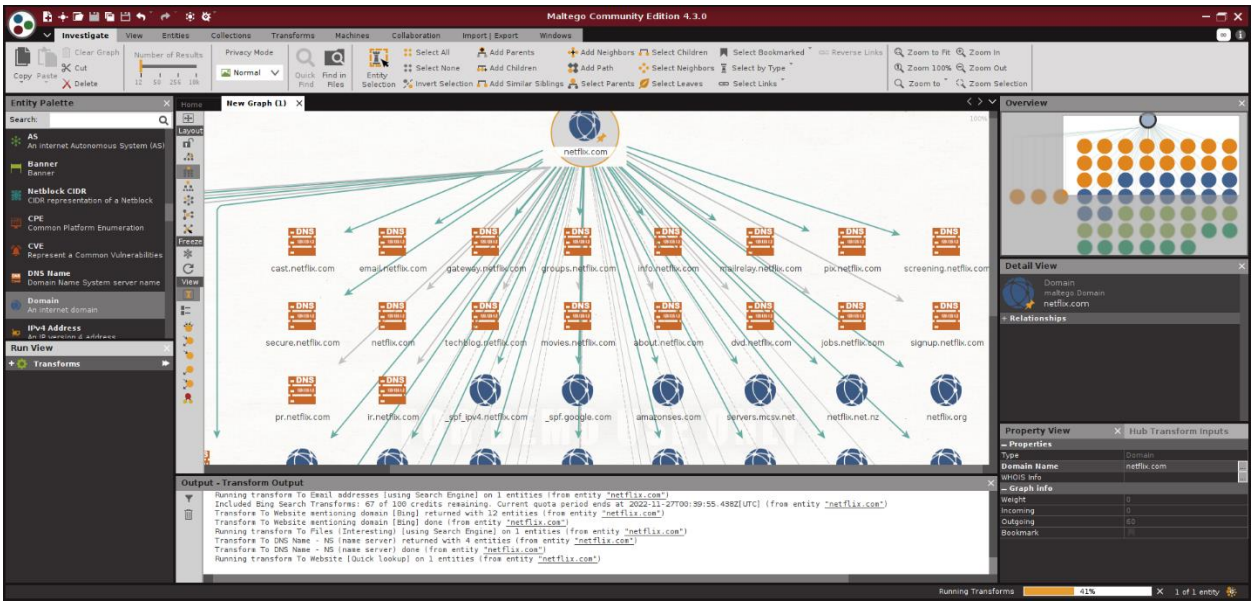
Tools Used for the Vulnerability Assessment

- Maltego tool
- Recon-ng
- The Harvester
- Nmap
- Angry IP Scanner
- Legion
- Nbtscan
- Host
- Nslookup
- Dig Command
- Metasploit Framework

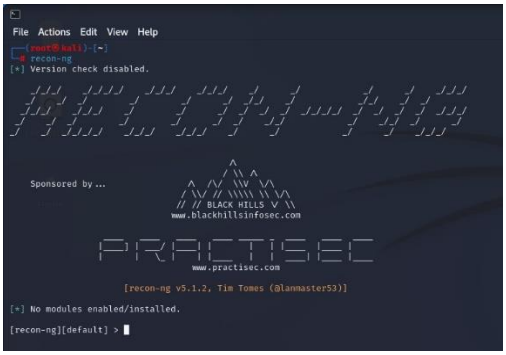
Web Reconnaissance Scan on Netflix.com

Maltego tool

Information gathering



Recon-ng



Install module

```
root@kali: ~
File  Actions  Edit  View  Help

[recon-ng][default] > marketplace install hackertarget
[+] Module installed: recon/domains-hosts/hackertarget
[+] Reloading modules ...
[!] 'namechk_api' key not set. namechk module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. geocode module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. reverse_geocode module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_tls_subjects module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_tls_subjects module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_org module will likely fail at runtime. See 'keys add'.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
[!] 'bing_api' key not set. bing_domain_api module will likely fail at runtime. See 'keys add'.
[!] 'binaryedge_api' key not set. binaryedge module will likely fail at runtime. See 'keys add'.
[!] 'spyse_api' key not set. spyse_subdomains module will likely fail at runtime. See 'keys add'.
[!] 'builtwith_api' key not set. builtwith module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_hostname module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_domain module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_api' key not set. ipstack module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_ip module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_hostname module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_hostname module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_ip module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'ipinfodb_api' key not set. ipinfodb module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_query module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_query module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-credentials/pwnedlist/account_creds' disabled. Dependency required: ''pyaes''.
[!] 'pwnedlist_api' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_api' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_api' key not set. leaks_dump module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. leaks_dump module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_users module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_contacts module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censys_netblock_company module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_net module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censys_netblock module will likely fail at runtime. See 'keys add'.
```

Load module

```
root@kali: ~
File  Actions  Edit  View  Help
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|reposito
ries|vulnerabilities>
```

Get source and Run the module

```
root@kali: ~
File  Actions  Edit  View  Help
[recon-ng][default][hackertarget] > options set SOURCE netflix.com
SOURCE => netflix.com
[recon-ng][default][hackertarget] > run

NETFLIX.COM
[*] Country: None
[*] Host: netflix.com
[*] Ip_Address: 3.211.157.115
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: ldmg101.netflix.com
[*] Ip_Address: 69.53.231.134
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: iad1-ddi01.netflix.com
[*] Ip_Address: 10.46.128.23
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: sv1-ddi01.netflix.com
[*] Ip_Address: 10.31.128.26
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: sv5-ddi01.netflix.com
[*] Ip_Address: 10.45.128.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------
[*] Country: None
[*] Host: sv1-ddi02.netflix.com
[*] Ip_Address: 10.31.128.27
[*] Latitude: None
[*] Longitude: None
```

```
File  Actions  Edit  View  Help
[*] Ip_Address: 207.45.73.145
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: contact.netflix.com
[*] Ip_Address: 52.31.48.193
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: api-nodequark.test.netflix.com
[*] Ip_Address: 100.65.89.57
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: sharkboot.test.netflix.com
[*] Ip_Address: 54.167.128.47
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: meechumlocalproxy.test.netflix.com
[*] Ip_Address: 127.0.0.1
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: crftest.netflix.com
[*] Ip_Address: 54.183.7.194
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------

_______
SUMMARY
-------
[*] 320 total (320 new) hosts found.
[recon-ng][default][hackertarget] >
```

```
root@kali: ~
File  Actions  Edit  View  Help
[recon-ng][default][hackertarget] > options set SOURCE netflix.com
SOURCE => netflix.com
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name   Current Value  Required  Description
  ----   -------------  --------  -----------
  SOURCE  netflix.com    yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][hackertarget] > input

  +-------------+
  | Module Inputs |
  +-------------+
  | netflix.com   |
  +-------------+

[recon-ng][default][hackertarget] > run

_________
NETFLIX.COM
---------
[*] Country: None
[*] Host: netflix.com
[*] Ip_Address: 54.160.93.182
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: ldmg101.netflix.com
[*] Ip_Address: 69.53.231.134
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
```

The Harvester

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# theHarvester

*******************************************************************
*                                                                 *
*   ___  _____  __   __    ___  ___  ___  ___  ___  ___  ___  ___ *
*  | _ \|_ _|_ \ \ / /__ | _ \ / _ \| _ \ / _ \| _ \ / _ \| _ \ | *
*  |  _/ | | | | \ V / _ \|  _/| (_) |  _/| (_) |  _/| (_) |  _/ | *
*  \ __|_| |_| |_|\_/ \_/ |_|   \ / \ __||__/\ __||__/\ __||__/|_| *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t DNS_TLD] [-r] [-n] [-c] [-f FILENAME] [-b SOURCE]
theHarvester: error: the following arguments are required: -d/--domain

┌──(root㉿kali)-[~]
└─#
```

Search for emails, IPs, and Hosts through the google search engine.

```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# theHarvester -d netflix.com -l 300 -b google

*******************************************************************
*                                                                 *
*   ___  _____  __   __    ___  ___  ___  ___  ___  ___  ___  ___ *
*  | _ \|_ _|_ \ \ / /__ | _ \ / _ \| _ \ / _ \| _ \ / _ \| _ \ | *
*  |  _/ | | | | \ V / _ \|  _/| (_) |  _/| (_) |  _/| (_) |  _/ | *
*  \ __|_| |_| |_|\_/ \_/ |_|   \ / \ __||__/\ __||__/\ __||__/|_| *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: netflix.com

        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
[*] Searching Google.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 4
---------------------
dvd.netflix.com:207.45.72.201
help.netflix.com:54.214.31.161, 44.226.248.54, 34.217.252.38
jobs.netflix.com:44.237.19.9, 34.210.239.21, 44.237.236.235, 52.88.30.115, 52.37.162.159, 35.83.27.204, 54.148.41.72
, 54.68.68.175
www.netflix.com:44.242.60.85, 44.237.234.25, 44.234.232.238
```

Get all information about the Netflix.com

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# theHarvester -d netflix.com -l 300 -b all

*******************************************************************
*                                                                 *
* | |_| |_   __    /\  /\__ _ _ __   ___ __ _ _ __ ___ _ __ ___ |
* | __| __| / _ \  / /_/ / _` | '_ \ / _ \ V / _` | '_ ` _ \ '__| *
* | |_| |_ | (_) |/ __  / (_| | | | |  __/\ / (_| | | | | | |    *
*  \__|\__|\___/ \/ /_/ \__,_|_| |_|\___|\_/ \__,_|_| |_| |_|_|    *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: netflix.com

[!] Missing API key for Hunter.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for binaryedge.
[!] Missing API key for Intelx.
[!] Missing API key for PentestTools.
[!] Missing API key for RocketReach.
[!] Missing API key for Securitytrail.
[!] Missing API key for Spyse.
[!] Missing API key for Github.
[!] Missing API key for zoomeye.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for fullhunt.
[*] Searching Anubis.
[*] Searching Urlscan.
[*] Searching CRTsh.
[*] Searching Duckduckgo.
Google is blocking your ip and the workaround, returning
        Searching 0 results.
        Searching 100 results.
Google is blocking your ip and the workaround, returning
```

```
File  Actions  Edit  View  Help
Google is blocking your ip and the workaround, returning
        Searching 200 results.
Google is blocking your ip and the workaround, returning
        Searching 300 results.
[*] Searching Google.
[*] Searching Hackertarget.
[*] Searching Dnsdumpster.
[*] Searching Baidu.
        Searching results.
[*] Searching Virustotal.
Google is blocking your ip and the workaround, returning
        Searching 100 results.
[*] Searching Qwant.
[*] Searching Omnisint.
[*] Searching Otx.
Google is blocking your ip and the workaround, returning
        Searching 200 results.
Google is blocking your ip and the workaround, returning
Google is blocking your ip and the workaround, returning
        Searching 300 results.
[*] Searching Linkedin.
        Searching 100 results.
        Searching results.
[*] Searching Certspotter.
        Searching 200 results.
An exception has occurred: Response payload is not completed
[*] Searching Rapiddns.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https:/
/api.h45ht.or.id/v1/subdomain-enumeration?domain=netflix.com')
Google is blocking your ip and the workaround, returning
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0x7fda4d0fdec
0> [Name or service not known]
        Searching 300 results.
[*] Searching Linkedin.
[*] Searching Sublist3r.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[
SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.thre
atcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
        Searching 0 results.
[*] Searching Bing.
Google is blocking your ip and the workaround, returning
        Searching 0 results.
[*] Searching Trello.
[*] Searching Threatminer.

[*] ASNS found: 9
--------------------
AS13335
AS14618
AS15169
```

```
File  Actions  Edit  View  Help

[*] Emails found: 1
--------------------
netflixoss@netflix.com

[*] Hosts found: 2991
---------------------
1.dig.netflix.com
1.dig.netflix.com:176.96.182.1
2014stockenroll.netflix.com
360.netflix.com
360.netflix.com:34.252.74.1, 52.31.48.193, 46.137.171.215
360classic.netflix.com
aa.netflix.com
ablaze-beta.prod.netflix.com:100.82.155.48, 100.85.46.65, 100.85.120.110
ablaze.prod.netflix.com:100.82.155.48, 100.85.46.65, 100.85.120.110
ablaze.prod.netflix.com
```

```
[*] No Twitter users found.

[*] No LinkedIn users found.

[*] LinkedIn Links found: 0
--------------------------

[*] No Trello URLs found.

[*] IPs found: 411
------------------
```

Scan the IP Address on Metasploitable

Nmap

Check the connectivity using ‘ping’.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1e:a6:03
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1e:a603/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1252 (1.2 KB)  TX bytes:3638 (3.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 3062 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
From 192.168.56.100 icmp_seq=3 Destination Host Unreachable
64 bytes from 192.168.56.103: icmp_seq=4 ttl=63 time=0.800 ms
64 bytes from 192.168.56.103: icmp_seq=5 ttl=63 time=0.796 ms
64 bytes from 192.168.56.103: icmp_seq=6 ttl=63 time=0.849 ms
64 bytes from 192.168.56.103: icmp_seq=7 ttl=63 time=0.760 ms
64 bytes from 192.168.56.103: icmp_seq=8 ttl=63 time=0.763 ms
64 bytes from 192.168.56.103: icmp_seq=9 ttl=63 time=0.710 ms
64 bytes from 192.168.56.103: icmp_seq=10 ttl=63 time=0.751 ms
64 bytes from 192.168.56.103: icmp_seq=11 ttl=63 time=0.749 ms
64 bytes from 192.168.56.103: icmp_seq=12 ttl=63 time=0.839 ms
64 bytes from 192.168.56.103: icmp_seq=13 ttl=63 time=0.631 ms
64 bytes from 192.168.56.103: icmp_seq=14 ttl=63 time=0.670 ms
64 bytes from 192.168.56.103: icmp_seq=15 ttl=63 time=0.743 ms
64 bytes from 192.168.56.103: icmp_seq=16 ttl=63 time=0.759 ms
64 bytes from 192.168.56.103: icmp_seq=17 ttl=63 time=0.703 ms
64 bytes from 192.168.56.103: icmp_seq=18 ttl=63 time=1.33 ms
64 bytes from 192.168.56.103: icmp_seq=19 ttl=63 time=1.05 ms
64 bytes from 192.168.56.103: icmp_seq=20 ttl=63 time=0.877 ms
64 bytes from 192.168.56.103: icmp_seq=21 ttl=63 time=0.734 ms
64 bytes from 192.168.56.103: icmp_seq=22 ttl=63 time=1.12 ms
64 bytes from 192.168.56.103: icmp_seq=23 ttl=63 time=0.874 ms
64 bytes from 192.168.56.103: icmp_seq=24 ttl=63 time=0.968 ms
64 bytes from 192.168.56.103: icmp_seq=25 ttl=63 time=0.726 ms
64 bytes from 192.168.56.103: icmp_seq=26 ttl=63 time=0.693 ms
64 bytes from 192.168.56.103: icmp_seq=27 ttl=63 time=3.04 ms
64 bytes from 192.168.56.103: icmp_seq=28 ttl=63 time=1.07 ms
64 bytes from 192.168.56.103: icmp_seq=29 ttl=63 time=1.03 ms
64 bytes from 192.168.56.103: icmp_seq=30 ttl=63 time=1.03 ms
```

Scan the open ports.

```
File  Actions  Edit  View  Help
└─$ nmap 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 03:14 EDT
Nmap scan report for 192.168.56.103 (192.168.56.103)
Host is up (0.013s latency).
Not shown: 977 filtered tcp ports (no-response)
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
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds

┌──(kali㉿kali)-[~]
└─$
```

Scan version information of services type.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 03:16 EDT
Nmap scan report for 192.168.56.103 (192.168.56.103)
Host is up (0.010s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.16 seconds

┌──(kali㉿kali)-[~]
└─$
```

Find version of operationg system

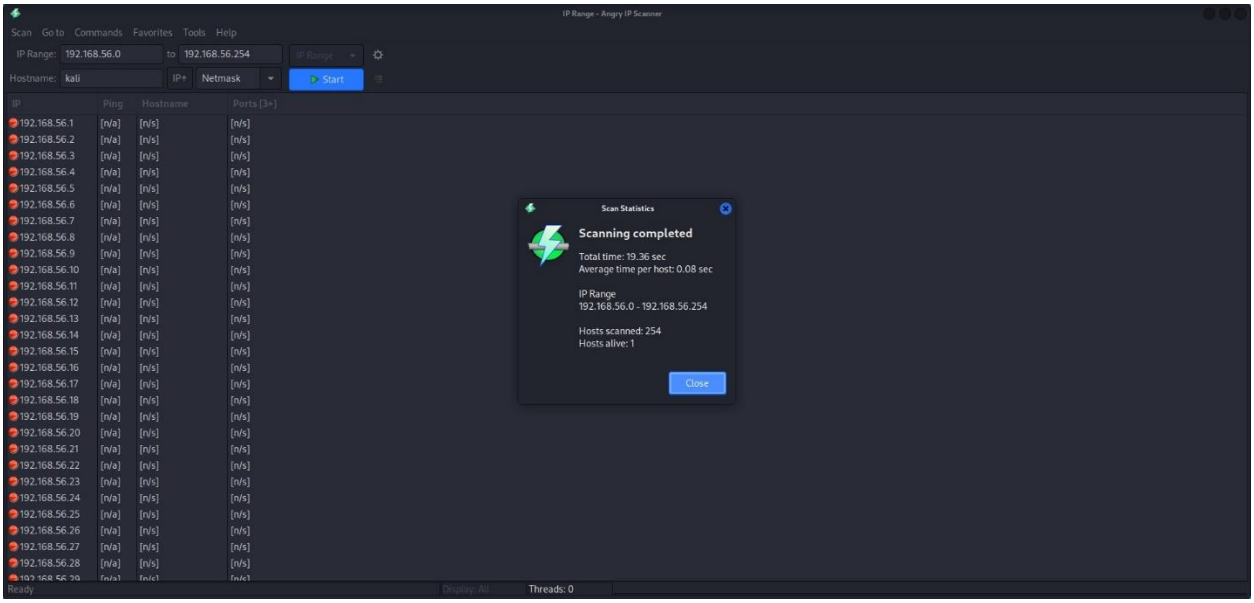
```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# nmap -O 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 03:39 EDT
Nmap scan report for 192.168.56.103 (192.168.56.103)
Host is up (0.0028s latency).
Not shown: 977 filtered tcp ports (no-response)
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
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gatewa
y (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.37 seconds

┌──(root㉿kali)-[~]
└─#
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.56.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 03:40 EDT
Nmap scan report for 192.168.56.103 (192.168.56.103)
Host is up (0.00037s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.101
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_ssl-date: 2022-10-30T07:41:55+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
```

Run aggressive scan to find all the details of a target

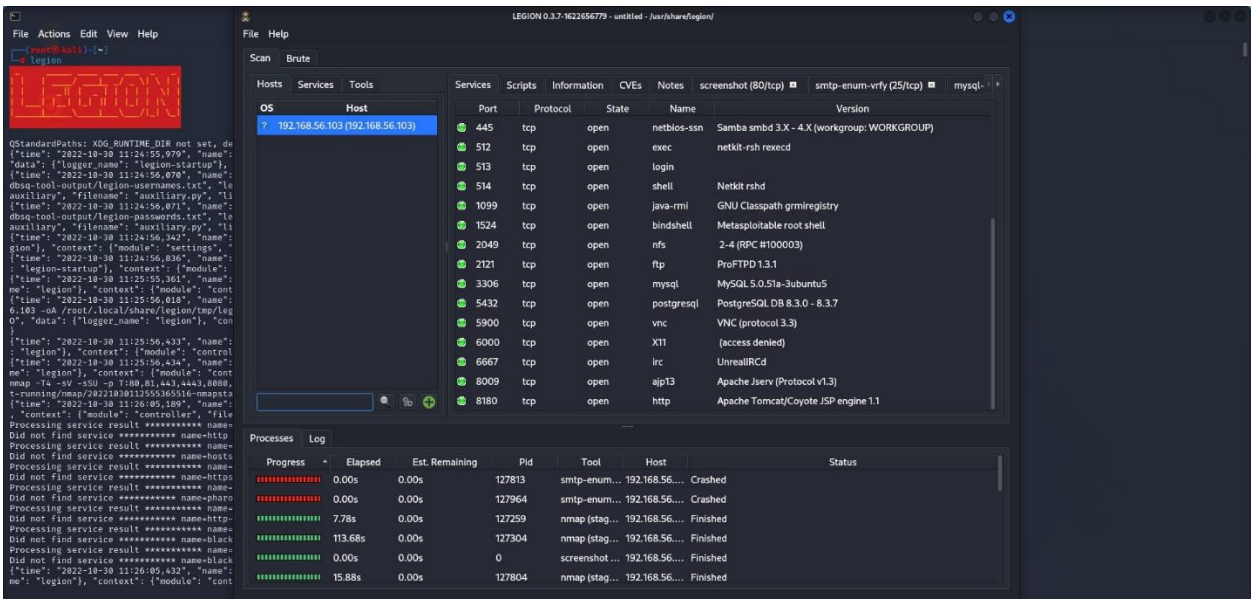
Angry IP Scanner

Perform a scan on IP range 192.168.56.0 - 255

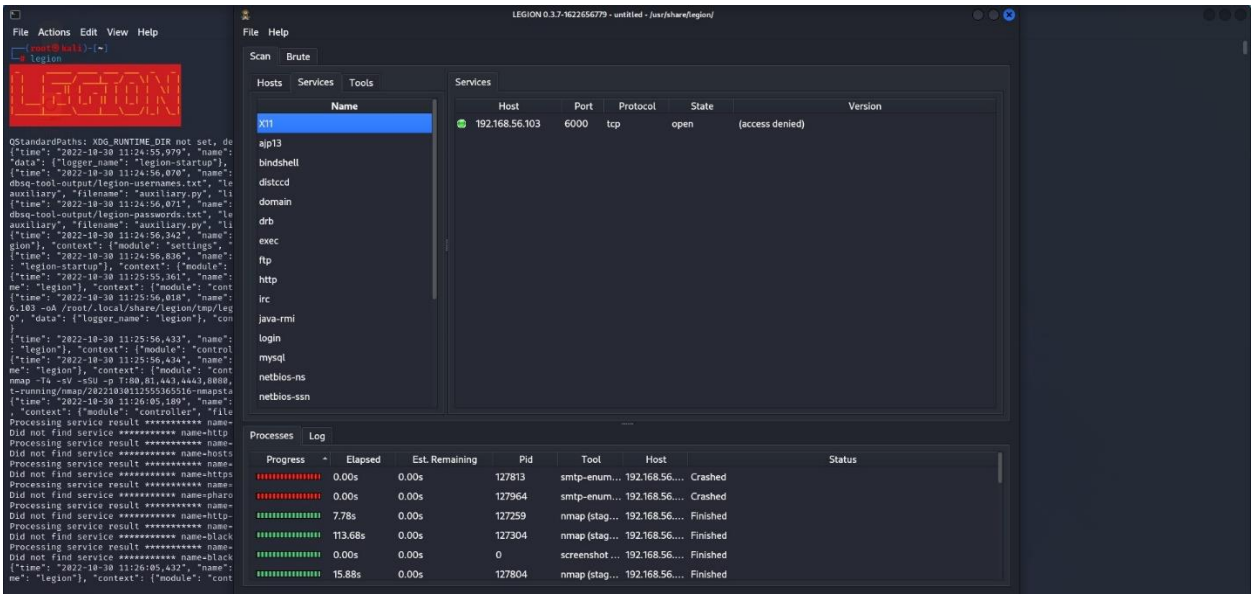


Enumeration scans

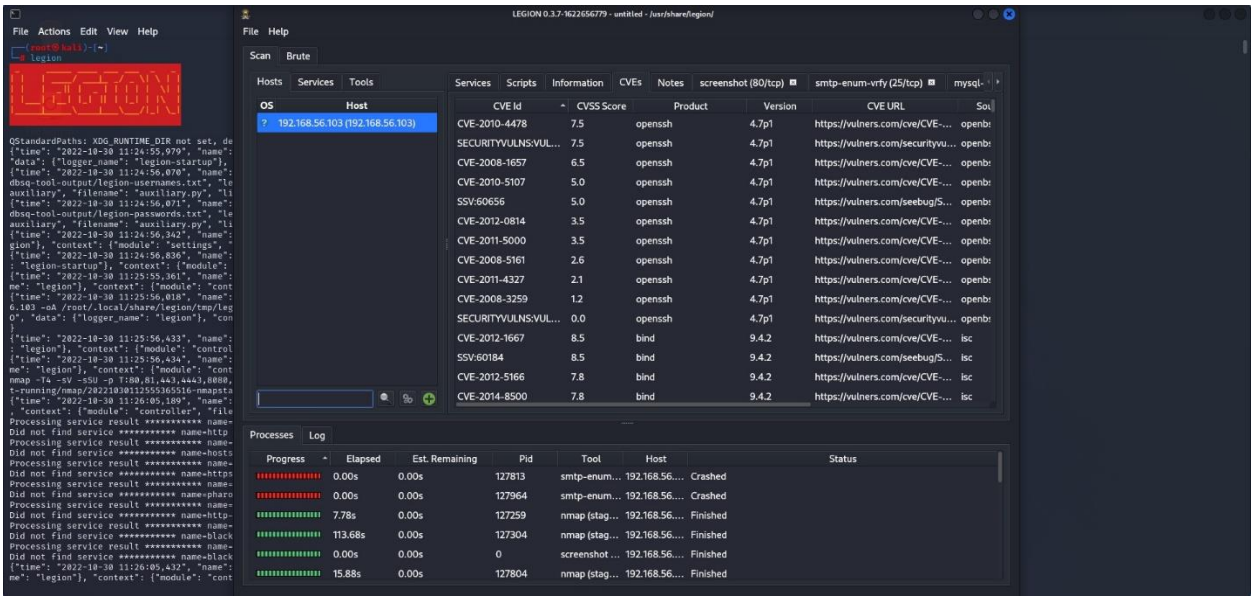
Legion



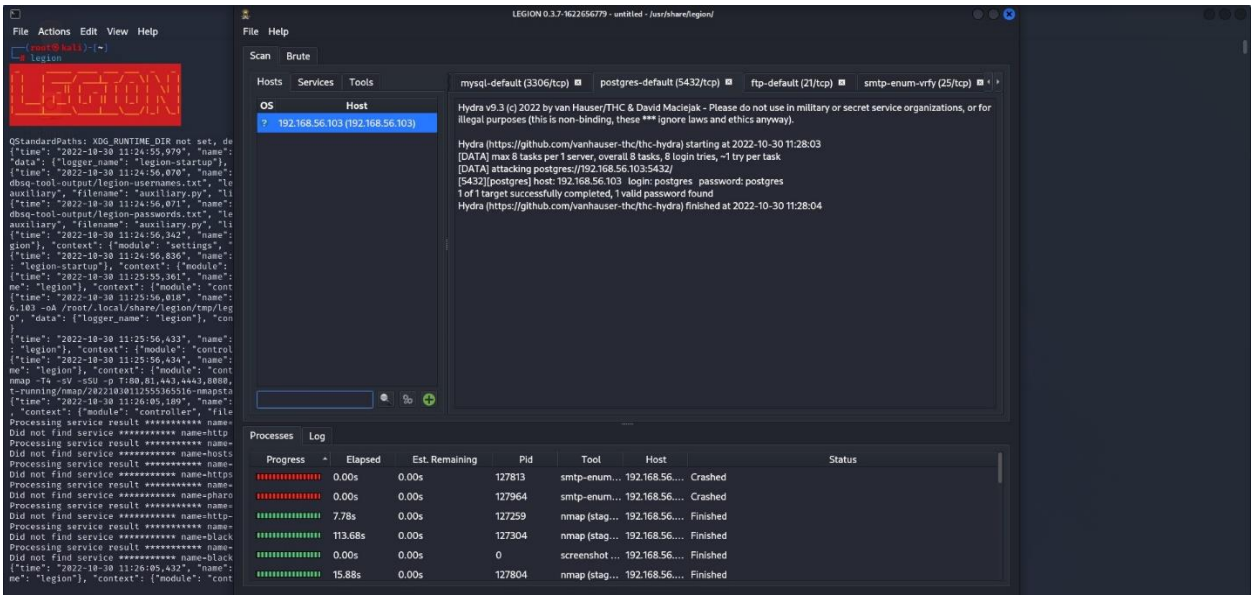
Services



CVEs (Common vulnerabilities)

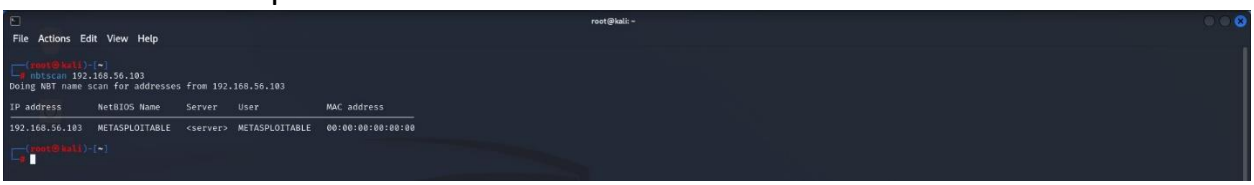


Found valid username and password



Nbtscan

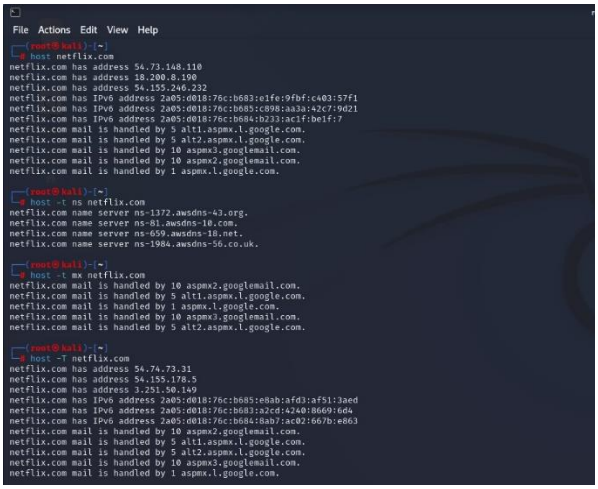
Netbios on metasploitable



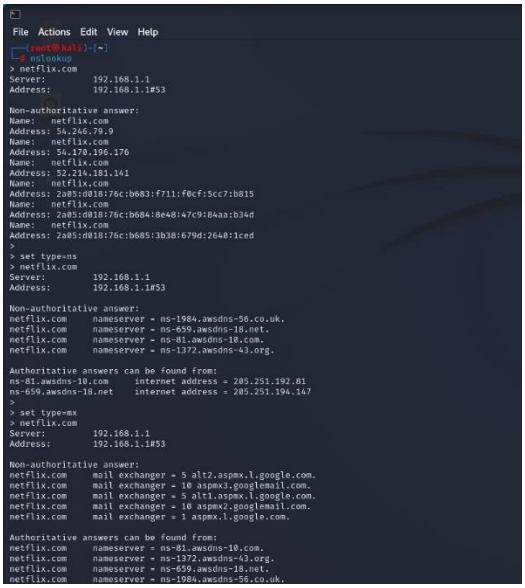
Verbose scan on metasploitable to find work group information

Host

host -t ns = name server information
host -t mx = mail server information
host -T = enables TCP/IP mode



```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# host netflix.com
netflix.com has address 54.73.148.110
netflix.com has address 18.200.8.190
netflix.com has address 54.155.246.232
netflix.com has IPv6 address 2a05:d018:76c:b683:e1fe:9fbf:c403:57f1
netflix.com has IPv6 address 2a05:d018:76c:b685:c898:aa3a:42c7:9d21
netflix.com has IPv6 address 2a05:d018:76c:b684:b233:ac1f:be1f:7
netflix.com mail is handled by 5 alt1.aspmx.l.google.com.
netflix.com mail is handled by 5 alt2.aspmx.l.google.com.
netflix.com mail is handled by 10 aspmx3.googlemail.com.
netflix.com mail is handled by 10 aspmx2.googlemail.com.
netflix.com mail is handled by 1 aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─# host -t ns netflix.com
netflix.com name server ns-1372.awsdns-43.org.
netflix.com name server ns-81.awsdns-10.com.
netflix.com name server ns-659.awsdns-18.net.
netflix.com name server ns-1984.awsdns-56.co.uk.

┌──(root㉿kali)-[~]
└─# host -t mx netflix.com
netflix.com mail is handled by 10 aspmx2.googlemail.com.
netflix.com mail is handled by 5 alt1.aspmx.l.google.com.
netflix.com mail is handled by 1 aspmx.l.google.com.
netflix.com mail is handled by 10 aspmx3.googlemail.com.
netflix.com mail is handled by 5 alt2.aspmx.l.google.com.

┌──(root㉿kali)-[~]
└─# host -T netflix.com
netflix.com has address 54.74.73.31
netflix.com has address 54.155.178.5
netflix.com has address 3.251.50.149
netflix.com has IPv6 address 2a05:d018:76c:b685:e8ab:afd3:af51:3aed
netflix.com has IPv6 address 2a05:d018:76c:b683:a2cd:42a0:8660:6d4
netflix.com has IPv6 address 2a05:d018:76c:b684:8ab7:ac02:667b:e863
netflix.com mail is handled by 10 aspmx2.googlemail.com.
netflix.com mail is handled by 5 alt1.aspmx.l.google.com.
netflix.com mail is handled by 5 alt2.aspmx.l.google.com.
netflix.com mail is handled by 10 aspmx3.googlemail.com.
netflix.com mail is handled by 1 aspmx.l.google.com.
```



```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nslookup
> netflix.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   netflix.com
Address: 54.246.79.9
Name:   netflix.com
Address: 54.170.196.176
Name:   netflix.com
Address: 52.214.181.141
Name:   netflix.com
Address: 2a05:d018:76c:b683:f711:f0cf:5cc7:b815
Name:   netflix.com
Address: 2a05:d018:76c:b684:8e48:47c9:84aa:b34d
Name:   netflix.com
Address: 2a05:d018:76c:b685:3b38:679d:2640:1ced
>
> set type=ns
> netflix.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
netflix.com     nameserver = ns-1984.awsdns-56.co.uk.
netflix.com     nameserver = ns-659.awsdns-18.net.
netflix.com     nameserver = ns-81.awsdns-10.com.
netflix.com     nameserver = ns-1372.awsdns-43.org.

Authoritative answers can be found from:
ns-81.awsdns-10.com     internet address = 205.251.192.81
ns-659.awsdns-18.net    internet address = 205.251.194.147
>
> set type=mx
> netflix.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
netflix.com     mail exchanger = 5 alt2.aspmx.l.google.com.
netflix.com     mail exchanger = 10 aspmx3.googlemail.com.
netflix.com     mail exchanger = 5 alt1.aspmx.l.google.com.
netflix.com     mail exchanger = 10 aspmx2.googlemail.com.
netflix.com     mail exchanger = 1 aspmx.l.google.com.

Authoritative answers can be found from:
netflix.com     nameserver = ns-81.awsdns-10.com.
netflix.com     nameserver = ns-1372.awsdns-43.org.
netflix.com     nameserver = ns-659.awsdns-18.net.
netflix.com     nameserver = ns-1984.awsdns-56.co.uk.
```

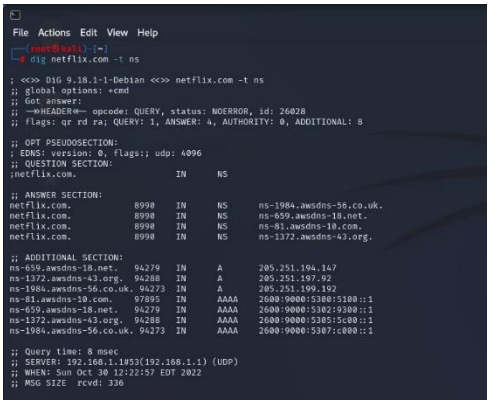
Nalookup

Nslookup :- gather information
Set type=ns :- name serverinformation
Set type=mx :- mail server information

Dig Command

Find DNS related information

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# dig netflix.com

; <<>> DiG 9.18.1-1-Debian <<>> netflix.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36428
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3b5c0f2e102935460100000035ea4b9081ac33817000670 (good)
;; QUESTION SECTION:
;netflix.com.                   IN      A

;; ANSWER SECTION:
netflix.com.            19      IN      A       54.74.73.31
netflix.com.            19      IN      A       3.251.50.149
netflix.com.            19      IN      A       54.155.178.5

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Oct 30 12:22:15 EDT 2022
;; MSG SIZE  rcvd: 116
```



```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# dig netflix.com -t ns

; <<>> DiG 9.18.1-1-Debian <<>> netflix.com -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26028
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;netflix.com.                   IN      NS

;; ANSWER SECTION:
netflix.com.            8990    IN      NS      ns-1984.awsdns-56.co.uk.
netflix.com.            8990    IN      NS      ns-659.awsdns-18.net.
netflix.com.            8990    IN      NS      ns-81.awsdns-10.com.
netflix.com.            8990    IN      NS      ns-1372.awsdns-43.org.

;; ADDITIONAL SECTION:
ns-659.awsdns-18.net.   94279   IN      A       205.251.194.147
ns-1372.awsdns-43.org.  94288   IN      A       205.251.197.92
ns-1984.awsdns-56.co.uk. 94273  IN      A       205.251.199.192
ns-81.awsdns-10.com.    97895   IN      AAAA    2600:9000:5300:5100::1
ns-659.awsdns-18.net.   94279   IN      AAAA    2600:9000:5302:9300::1
ns-1372.awsdns-43.org.  94288   IN      AAAA    2600:9000:5305:5c00::1
ns-1984.awsdns-56.co.uk. 94273  IN      AAAA    2600:9000:5307:c000::1

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Oct 30 12:22:57 EDT 2022
;; MSG SIZE  rcvd: 336
```

```
┌──(root㉿kali)-[~]
└─# dig netflix.com -t ns CNAME

; <<>> DiG 9.18.1-1-Debian <<>> netflix.com -t ns CNAME
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8411
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: bca9dca5bb81c8f701000000635ea4ca82cd1444c53b0b22 (good)
;; QUESTION SECTION:
;netflix.com.                   IN      NS

;; ANSWER SECTION:
netflix.com.            14054   IN      NS      ns-659.awsdns-18.net.
netflix.com.            14054   IN      NS      ns-1984.awsdns-56.co.uk.
netflix.com.            14054   IN      NS      ns-81.awsdns-10.com.
netflix.com.            14054   IN      NS      ns-1372.awsdns-43.org.

;; ADDITIONAL SECTION:
ns-81.awsdns-10.com.    94756   IN      A       205.251.192.81
ns-659.awsdns-18.net.   94944   IN      A       205.251.194.147

;; Query time: 12 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Oct 30 12:23:25 EDT 2022
;; MSG SIZE  rcvd: 239

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42681
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: bca9dca5bb81c8f701000000635ea4fe4415b04401d95cef (good)
;; QUESTION SECTION:
;CNAME.                         IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2022103000 1800 900 604
800 86400

;; Query time: 120 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Oct 30 12:23:25 EDT 2022
;; MSG SIZE  rcvd: 137
```

```
┌──(root㉿kali)-[~]
└─# dig netflix.com -t ns AAAA

; <<>> DiG 9.18.1-1-Debian <<>> netflix.com -t ns AAAA
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16237
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: efb9658ee5c9817f01000000635ea4da4c837ca8d45385af (good)
;; QUESTION SECTION:
;netflix.com.                   IN      NS

;; ANSWER SECTION:
netflix.com.            14038   IN      NS      ns-1372.awsdns-43.org.
netflix.com.            14038   IN      NS      ns-659.awsdns-18.net.
netflix.com.            14038   IN      NS      ns-81.awsdns-10.com.
netflix.com.            14038   IN      NS      ns-1984.awsdns-56.co.uk.

;; ADDITIONAL SECTION:
ns-81.awsdns-10.com.    94740   IN      A       205.251.192.81
ns-659.awsdns-18.net.   94928   IN      A       205.251.194.147

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Oct 30 12:23:41 EDT 2022
;; MSG SIZE  rcvd: 239

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6980
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: efb9658ee5c9817f01000000635ea50e7854d37977c36a2e (good)
;; QUESTION SECTION:
;AAAA.                          IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2022103000 1800 900 604
800 86400

;; Query time: 48 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun Oct 30 12:23:41 EDT 2022
;; MSG SIZE  rcvd: 136
```

Metasploit Framework

SSH Exploitation

```
┌──(root㉿kali)-[~]
└─# service postgresql start

┌──(root㉿kali)-[~]
└─# service postgresql status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
     Active: active (exited) since Sun 2022-10-30 13:12:52 EDT; 16min ago
    Process: 2517 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 2517 (code=exited, status=0/SUCCESS)
        CPU: 3ms

Oct 30 13:12:52 kali systemd[1]: Starting PostgreSQL RDBMS ...
Oct 30 13:12:52 kali systemd[1]: Finished PostgreSQL RDBMS.

┌──(root㉿kali)-[~]
└─# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--||  *


       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
```

```
   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   BLANK_PASSWORDS      false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED     5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS         false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS          false            no        Add all passwords in the current database to the list
   DB_ALL_USERS         false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING     none             no        Skip existing credentials stored in the current database (Accepte
                                                   d: none, user, user&realm)
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE                             no        File containing passwords, one per line
   RHOSTS                                yes       The target host(s), see https://github.com/rapid7/metasploit-fram
                                                   ework/wiki/Using-Metasploit
   RPORT                22               yes       The target port
   STOP_ON_SUCCESS      false            yes       Stop guessing when a credential works for a host
   THREADS              1                yes       The number of concurrent threads (max one per host)
   USERNAME                              no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair
                                                   per line
   USER_AS_PASS         false            no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VERBOSE              false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.56.103
rhosts => 192.168.56.103
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE Desktop/user.txt
USER_FILE => Desktop/user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

References

All the Labs and lectures.