Cybersecurity

Penetration Test Report

MegaCorpOne

Penetration Test Report

Kristina's Cloud Security, KCS

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Kristina's Cloud Security, LLC
Contact Name	Kristina Fong
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	Kristina@KCS.com

Document History

Version	Date	Author(s)	Comments
001	01/01/2023	Kristina Fong	First Draft
002	01/02/2023	Kristina Fong	Initial Review
003	01/09/2023	Kristina Fong	Final Review

Introduction

In accordance with MegaCorpOne's policies, Kristina's Cloud Security, LLC (henceforth known as KCS) 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 KCS during December 2022.

For the testing, KCS 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.

KCS 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

KCS 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

KCS 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

KCS's normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, MegaCorpOne and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in-scope for the scheduled assessment.

It is MegaCorpOne's responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

IP Address/URL	Description
172.16.117.0/16 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

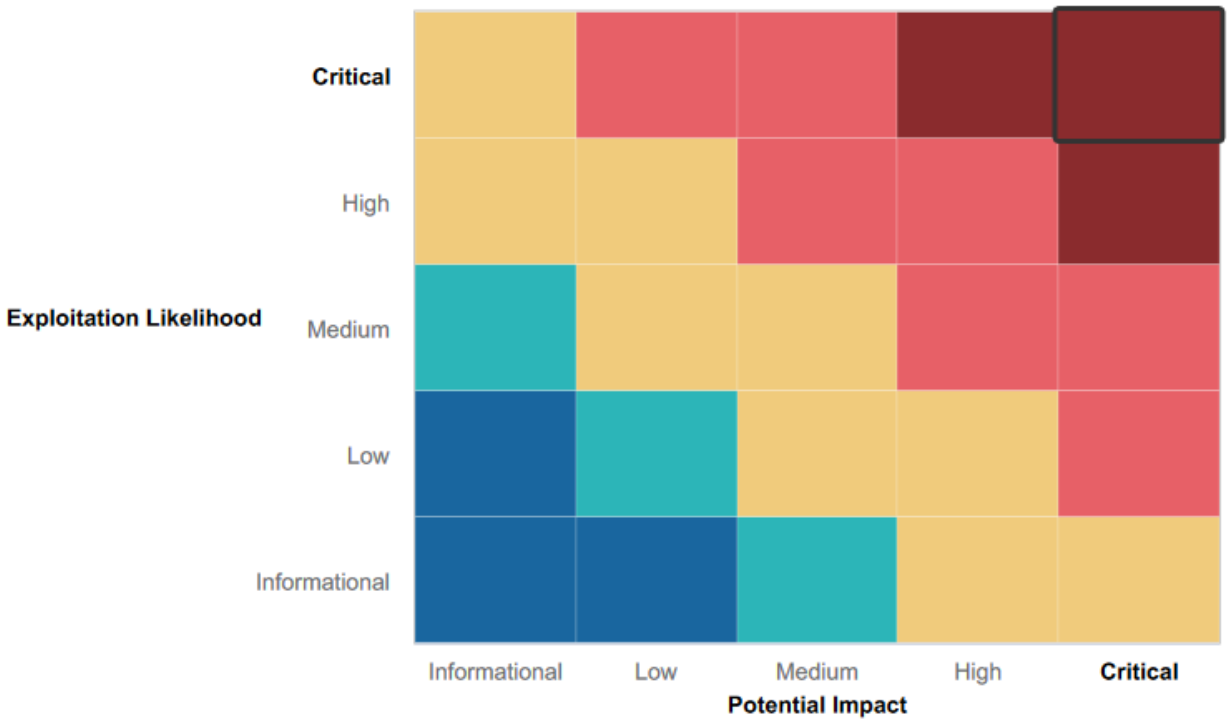
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within MegaCorpOne's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- The MegaCorpOne system was split into two machines, Windows and Debian Apache.
- Within some of the employee passwords, there was a mixture of special characters, Capital/lowercase letters as well as some numbers.
- Each employee of MegaCorpOne had their own individual credentials and logins into the system.

Summary of Weaknesses

KCS 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.

- Contact Information on Company Site
- Server Details on Assets page
- Company profile on Shodan.io
- Open ports on the network
- Weak passwords on Public web application
- Weak passwords on company machine
- Credential dumping
- Reverse shell vulnerability
- Privilege Escalation

Executive Summary

Kristina's Cloud Security, KCS conducted an intensive penetration test of MegaCorpOne to determine specific vulnerabilities, and security risks to their network. Within this report, our KCS pentesters used a wide range of techniques and tactics in order to understand the scope of security around MegaCorpOne.The KCS team started by using Google Dorking, in order to find a basis of the information publicly available on the company. We were able to gather MegaCorpOne employee email addresses and usernames from the company site. We were also able to determine the web service and version of the company server based off of a google search for the companies assets; Apache 2.4.38 on Debian OS. KCS then turned their attention to Shodan.io to perform a nslookup on www.megacorpone.com and get the ip address.With the ip address we were able to gather open ports and several vulnerabilities present on the server: CVE-2019-0215, CVE-2019-0220, CVE-2019-0217, CVE-2019-0197, CVE-2019-0196, CVE-2019-02111 and the location of the server: Montreal, Canada.

Since the KCS pentesters were able to obtain company email addresses and usernames; our team was able to use common passwords to attempt a login onto the company site; we were able to find thudson/thudson and trivera/Spring2021.

Using Zenmap our pentesters were able to perform an intense scan over several ports on the company network; finding port 21 open. Our team decided to use port 21 as a backdoor exploit.Following the port 21 finding, we used a python script to exploit MegaCorpOnes vulnerability and gain a reverse shell into the machine.

Our pentesters were able to comb through several files on the machine to find confidential admin credentials; with the credentials we were able to find more user passwords under the /etc/shadow file.
Since our pentesters were able to crack several passwords, we then decided to enable an additional port for the SSH service to listen on and opened the port on the firewall. We created an account and escalated its privileges by adding it to the sudoers group; being able to SSH over into port 10022.

Our pentesters then turned their focus to compromising MegaCorpOnes Window machines. We conducted another port scan to determine any vulnerabilities or open ports.
We found that MegaCorpOne uses two window machines; they have port 445 smb, 139 rpc/smb, 3389 rdp, and 88 kerberos open.

Our team was able to perform a brute force attack by doing a credential spray. Referencing back to the /etc/shadow file, our team was able to use each of the credentials hacked in order to find a set/matching pair that worked on the machine.
We were able to log into machine 172.22.117.20 MegaCorpOne.
We set the SMBUser and SMBpass to:Tstark Password!

Using LLMNR spoofing our team set out to find another set of credentials from another user. Using John the Ripper, we were able to crack one of the hashes, giving us the credentials: pparker Spring2021. Using our two sets of credentials, we ran commands on a remote machine.

Using msfvenom, our team created a custom payload and was able to transfer it to the designated host and run WMI commands.

Since we were able to grasp some credentials in the windows machine, pentesters were able to escalate user privilege in order to gain full control of the entire machine. Now that our team has system access over the windows machine, we created a scheduled task that will execute a meterpreter payload ensuring that we will always have a reverse shell into the target system.Using the metasploit kiwi extension, our team dumped the credentials that were cached on the WIN10 machine. By doing this, we were able to get a new account: credentialsbanner Winter2021. Using the credentials from the new account, we successfully launched the WMI exploit from our meterpreter session on Windows 10 to WINDC01; we made a copy of the NTDS.dit file and then were able to crack the password hashes in it.

Overall, KCS's vulnerability testing revealed Critical, High, Medium and Low vulnerabilities on the MegaCorpOne network/system.The MegaCorpOne's internal network requires immediate remediation efforts in order to protect and preserve sensitive company information. By reviewing the steps taken in this KCS Pentesting Report, it is advised that MegaCorpOne take the appropriate measures to ensure security is up-to-date.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Command and Control Risk	Critical
Weak passwords on company machine	Critical
Privilege Escalation and Exploiting	Critical
Password Cracking	Critical
LLMNR Spoofing Vulnerability	Critical
Company Profile on Shodan.io	Critical
Open Ports on the Network	Critical
Credential Dumping/Lateral Movement	High
Windows Open Ports	High
Reverse shell vulnerability	High
Contact Information on Company Site	Medium
Server Details on Assets page	Low

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

Scan Type	Total
Hosts	172.22.117.20 172.22.117.150
Ports	445 smb, 139 rpc/smb, 3389 rdp, 88 kerberos 21, 22, 80, 443.

Exploitation Risk	Total
Critical	7
High	3
Medium	1
Low	1

Vulnerability Findings

Server Details on Assets Page

Risk Rating: Low

Description:
By searching up megacorpone.com assets, details about the company's server and version were detailed. Apache 2.4.38 on Debian OS.

Affected Hosts: vpn.megacorpone.com

Remediation:

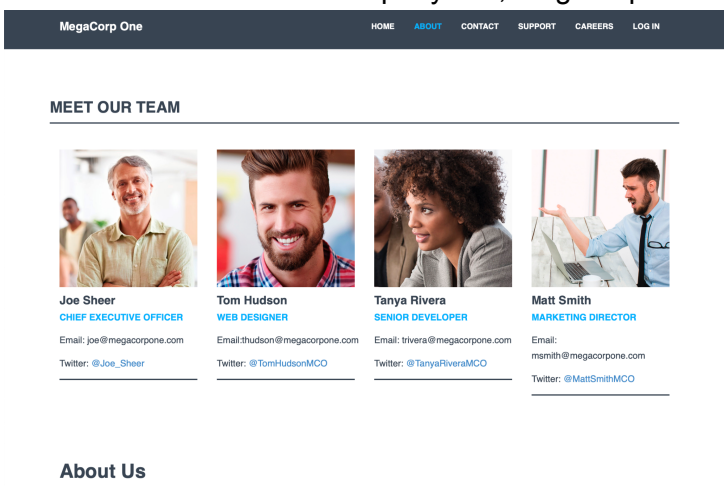
- Constantly upgrade software and operating systems.

Contact Information on Company Site

Risk Rating: Medium

Description:
When searching megacorpone.com, the public is able to find company contact information. Information can then be used to guess usernames and passwords for login attempts. The KCS team started by using Google Dorking, in order to find a basis of the information publicly available on the company. We were able to gather MegaCorpOne employee email addresses

and usernames from the company site; megacorpone.com.



Affected Hosts: vpn.megacorpone.com

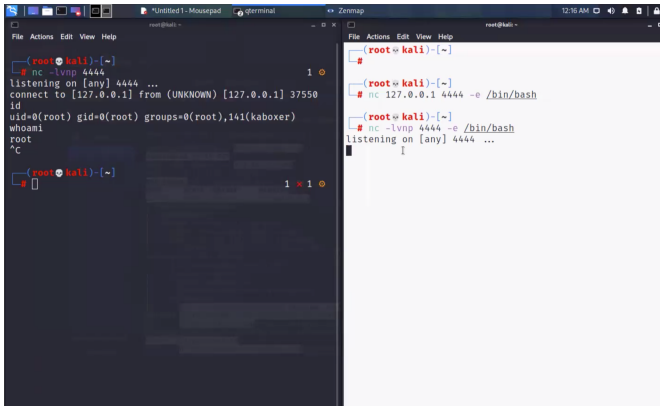
Remediation:

- Take down company employee contact information.
- Have one main text box with company contact. For example: megacorponehelp@gmail.com

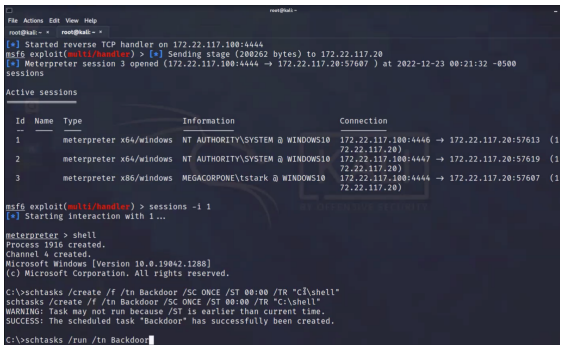
Reverse Shell Vulnerability

Risk Rating: High

Description:
Users attack open ports on the network in order to gain access into the target machine. Following the port 21 finding, we used a python script to exploit MegaCorpOnes vulnerability and gain a reverse shell into the machine.



Now that our team has system access over the windows machine, we created a scheduled task that will execute a meterpreter payload ensuring that we will always have a reverse shell into the target system.



Affected Hosts: vpn.megacorpone.com

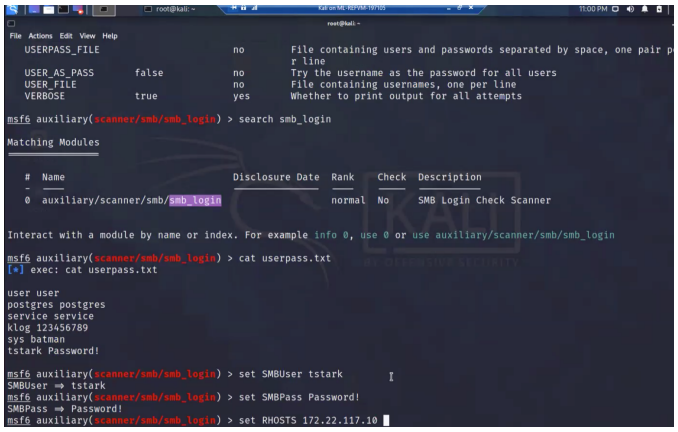
Remediation:

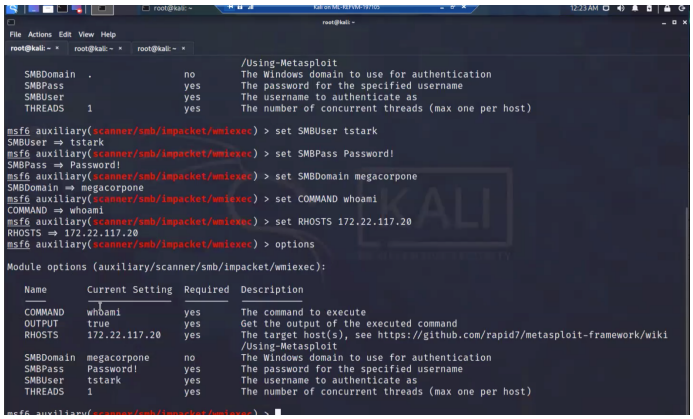
- Set up a firewall to detect reverse shell attempts. Monitor network activity.
- Have strict regulations on connections to computer plugins.

Command and Control Risk

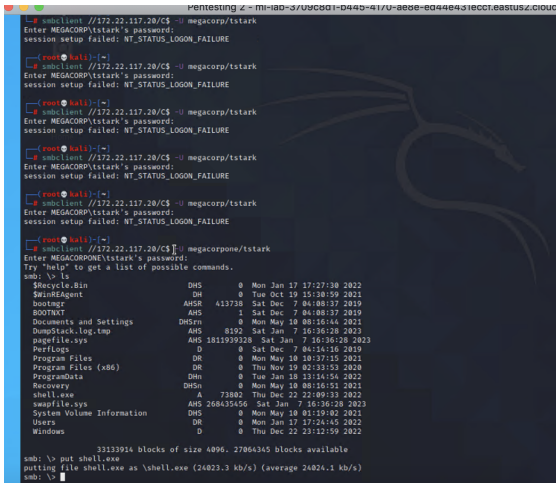
Risk Rating: High

Description:
When a malicious actor gains control of the system, they are able to perform malicious acts, by writing commands. Using our two sets of credentials, we ran commands on a remote machine.

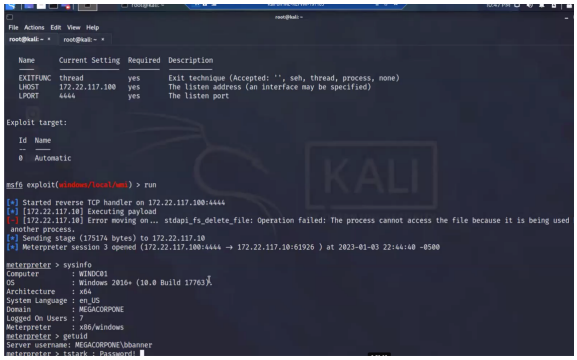




Using msfvenom, our team created a custom payload and was able to transfer it to the designated host and run WMI commands.



Using the credentials from the new account, we wanted to move from the Windows 10 machine to WINDC01.
By doing this, we successfully launched the WMI exploit from our meterpreter session on Windows 10 to WINDC01.



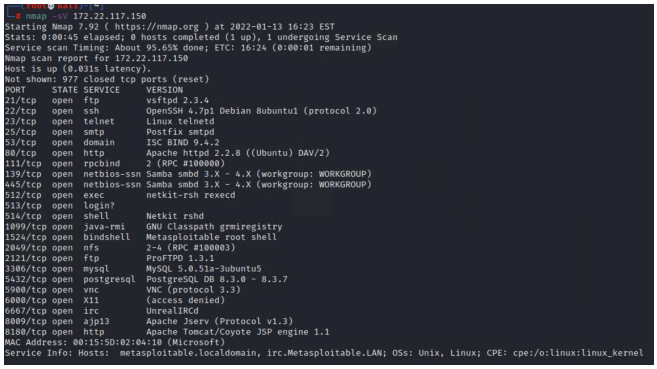
Affected Hosts: vpn.megacorpone.com

Remediation:

- Monitor network activity.
- Limit specific commands for users.

Windows Open Ports/Ports on Network

Risk Rating: High
Description:
Using Zenmap our pentesters were able to perform an intense scan over several ports on the company network; finding port 21 open. Our team decided to use port 21 as a backdoor exploit.



```
nmap -sV 172.22.117.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-13 16:23 EST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 16:24 (0:00:01 remaining)
Nmap scan report for 172.22.117.150
Host is up (0.031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:02:04:10 (Microsoft)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Our pentesters then turned their focus to compromising MegaCorpOnes Window machines. We conducted another port scan to determine any vulnerabilities or open ports.
We found that MegaCorpOne uses two window machines; they have port 445 smb, 139 rpc/smb, 3389 rdp, and 88 kerberos open.
We determined that port 88 is the domain controller since it is kerberos.

Affected Hosts: vpn.megacorpone.com

Remediation:

- Close all unused ports by disabling them.
- Access ports using a secure private VPN.
- Use multi-factor authentication to prevent open port access.
- Scan network ports regularly and monitor traffic.

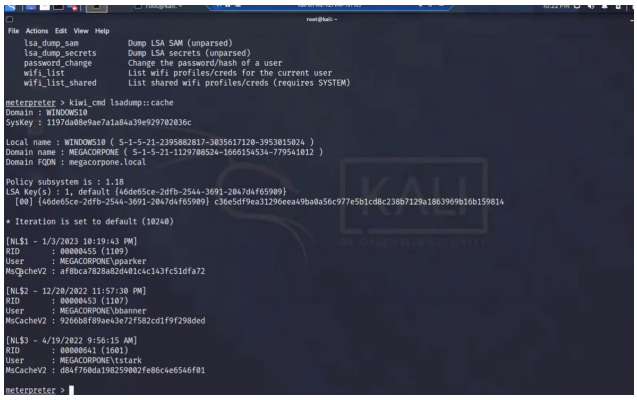
Credential Dumping/Lateral Movement

Risk Rating: High

Description:
Malicious actors will hack into devices and steal credentials in order to access sensitive information or control systems. Malicious users will scan and comb through devices to find credentials.
Our pentesters were able to comb through several files on the machine to find confidential admin credentials. Since we were able to get into an admin user account, we were able to find more user passwords under the /etc/shadow file.

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

Using the metasploit kiwi extension, our team dumped the credentials that were cached on the WIN10 machine. By doing this, we were able to get a new account:
credentialsbanner Winter2021



Affected Hosts: vpn.megacorpone.com

Remediation:

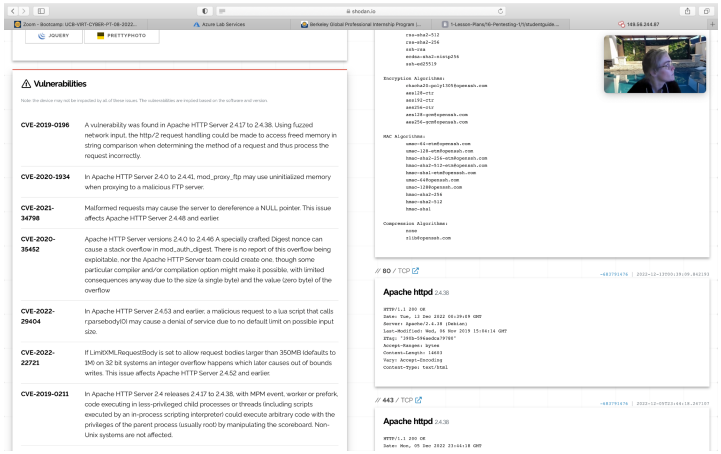
- Do not store passwords in open files.
- Use strong complex passwords that can't be cracked easily.
- Set up two-factor authentication.
- Encrypt passwords to create hashes that can't be easily cracked.
- Never reuse the same password for multiple accounts.

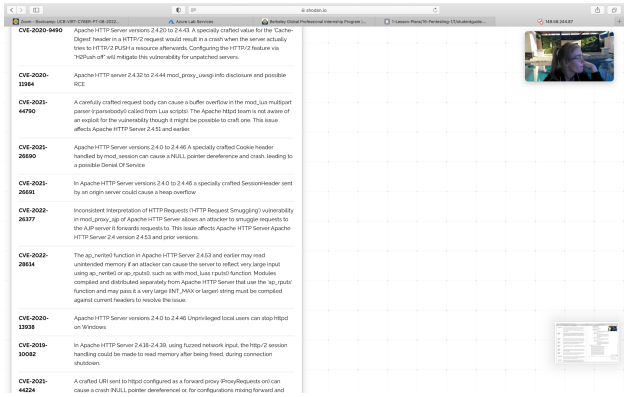
Company Profile on Shodan.io

Risk Rating: **Critical**

Description:
KCS then turned their attention to Shodan.io to perform a nslookup on www.megacorpone.com and get the ip address.
Then with the ip address we were able to gather open ports: 22, 80, 443; the version of SSH the server was running on SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 and reconfirm the web service and version: Debian Apache 2.4.38.With our port scan we found several vulnerabilities present on the server: CVE-2019-0215, CVE-2019-0220, CVE-2019-0217, CVE-2019-0197, CVE-2019-0196, CVE-2019-02111.

We were also able to find the location of the server: Montreal, Canada.





Affected Hosts: vpn.megacorpone.com

Remediation:

- Filter information put out on the company server.
- Continuously update and upgrade server.
- Use private VPN to hide sensitive location details for the company server.

LLMNR Spoofing Vulnerability

Risk Rating: Critical

Description:
LLMNR Spoofing attacks take advantage of requests visible on the local subnet. Attackers are able to capture traffic that comes in.

Affected Hosts: vpn.megacorpone.com

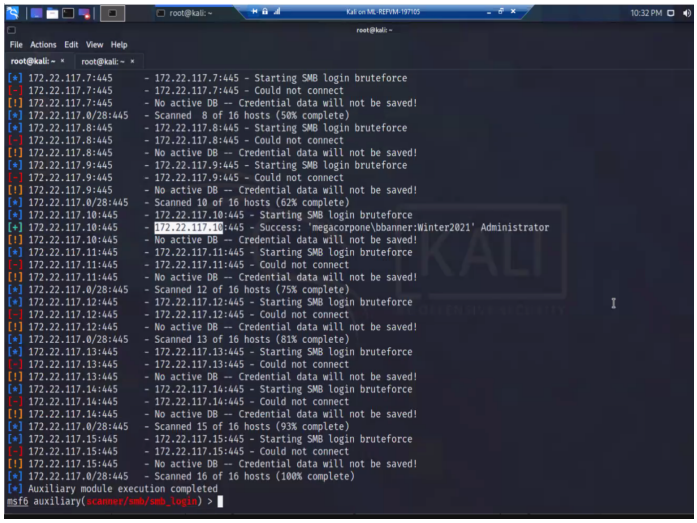
Remediation:

- Disable LLMNR if possible.
- If keeping LLMNR active, then make sure it is up-to-date to eliminate suspicious queries.
- Improve password strength and hashes.

Password Cracking

Risk Rating: Critical

Description:
Passwords can be easily cracked; therefore leading to system access for the malicious user. Our team was able to perform a brute force attack by doing a credential spray. Referencing back to the /etc/shadow file, our team was able to use each of the credentials hacked in order to find a set/matching pair that worked on the machine.
We were able to log into machine 172.22.117.20 MegaCorpOne.
We set the SMBUser and SMBpass to:
Tstark Password!



Using LLMNR spoofing our team set out to find another set of credentials from another user.
Using John the Ripper, we were able to crack one of the hashes, giving us the credentials:
pparker Spring2021.

Affected Hosts: vpn.megacorpone.com

Remediation:

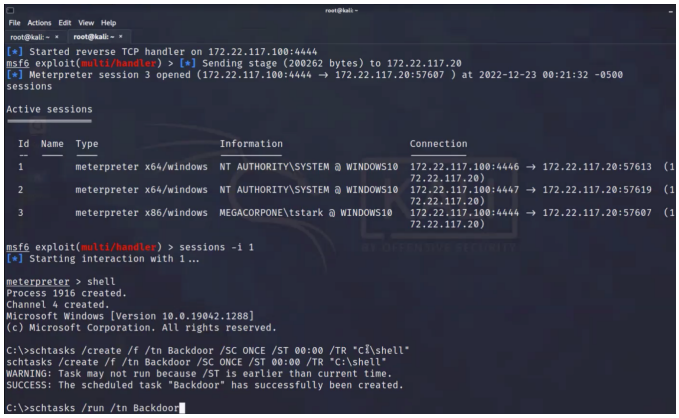
- Strong passwords with special characters, numbers and at least 12 characters in length.
- Hash passwords kept in file and only allow sudo admin access.
- Update passwords and maintain.

Privilege Escalation and Exploiting

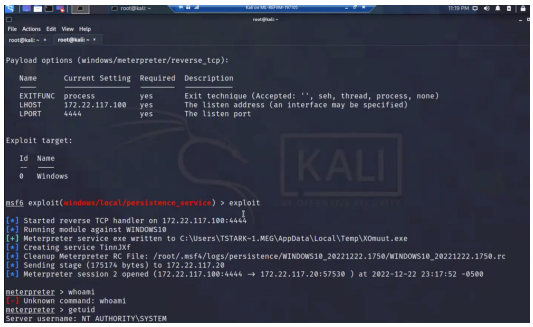
Risk Rating: Critical

Description:
Privilege escalation attacks exploit weak and vulnerable systems, being able to elevate access to network, applications and sensitive data. Since our pentesters were able to crack several passwords, we then decided to enable an additional port for the SSH service to listen on and

opened the port on the firewall. We created an account and escalated its privileges by adding it to the sudoers group; being able to SSH over into port 10022.



Since we were able to grasp some credentials in the windows machine, pentesters were able to escalate users privilege; moving tstark to system privileges in order to gain full control of the entire machine.



By utilizing system access on the domain controller we made a copy of the NTDS.dit file and then were able to crack the password hashes in it.

Affected Hosts: vpn.megacorpone.com

Remediation:

- Set up a password policy, multi factor authentication.
- Keep the system up-to-date to deter bugs and malfunctions on the network/system.
- Give users minimum privileges.

Weak Passwords

Risk Rating: Critical

Description:

Since the KCS pentesters were able to obtain company email addresses and usernames; our team was able to use common passwords to attempt a login onto the company site.
Going onto the megacorpone.com login page, our pentester tried several common passwords and were able to find thudson/thudson and trivera/Spring2021.

Affected Hosts: vpn.megacorpone.com

Remediation:

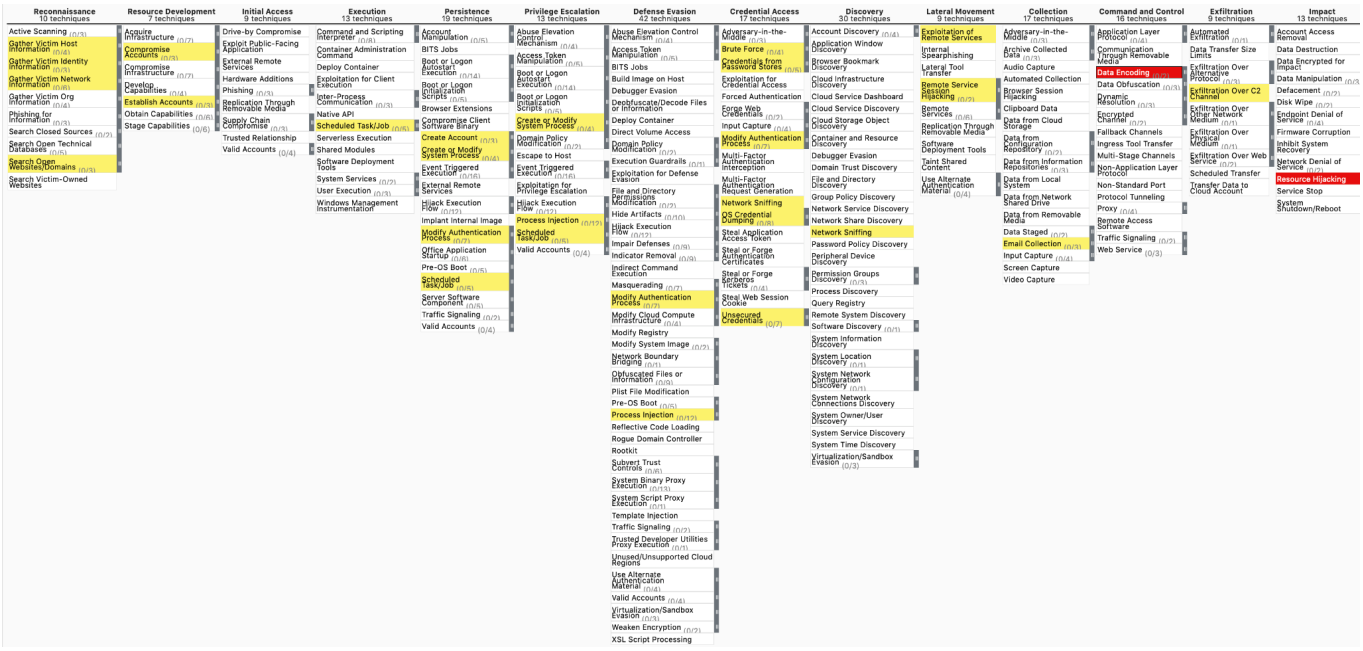
- Strong passwords with special characters, numbers and at least 12 characters in length.
- Hash passwords kept in file and only allow sudo admin access.
- Update passwords and maintain.

MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully
Failure to perform


Reconnaissance
10 techniques
Active Scanning (0/3)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/3)
Search Victim-Owned Websites
Resource Development
7 techniques
Acquire Infrastructure (0/7)
Compromise Accounts (0/3)
Compromise Infrastructure (0/7)
Develop Capabilities (0/4)
Establish Accounts (0/3)
Obtain Capabilities (0/6)
Stage Capabilities (0/6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)
Execution
13 techniques
Command and Scripting Interpreter (0/8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API
Scheduled Task/Job (0/6)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (0/3)
Windows Management Instrumentation
Persistence
19 techniques
Account Manipulation (0/5)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System Process (0/4)
Event Triggered Execution (0/16)
External Remote Services
Hijack Execution Flow (0/12)
Implant Internal Image
Modify Authentication Process (0/8)
Office Application Startup (0/6)
Pre-OS Boot (0/5)
Scheduled Task/Job (0/6)
Server Software Component (0/5)
Traffic Signaling (0/2)
Valid Accounts (0/4)
Privilege Escalation
13 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/16)
Exploitation for Privilege Escalation
Hijack Execution Flow (0/12)
Process Injection (0/12)
Scheduled Task/Job (0/6)
Valid Accounts (0/4)
Defense Evasion
42 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/10)
Hijack Execution Flow (0/12)
Impair Defenses (0/9)
Indicator Removal (0/9)
Indirect Command Execution
Masquerading (0/7)
Modify Authentication Process (0/7)
Modify Cloud Compute Infrastructure (0/4)
Modify Registry
Modify System Image (0/2)
Network Boundary Bridging (0/1)
Obfuscated Files or Information (0/9)
Plist File Modification
Pre-OS Boot (0/5)
Process Injection (0/12)
Reflective Code Loading
Rogue Domain Controller
Rootkit
Subvert Trust Controls (0/6)
System Binary Proxy Execution (0/13)
System Script Proxy Execution (0/1)
Template Injection
Traffic Signaling (0/2)
Trusted Developer Utilities Proxy Execution (0/1)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (0/4)
Valid Accounts (0/4)
Virtualization/Sandbox Evasion (0/3)
Weaken Encryption (0/2)
XSL Script Processing
Credential Access
17 techniques
Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Modify Authentication Process (0/7)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (0/4)
Steal Web Session Cookie
Unsecured Credentials (0/7)
Discovery
30 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (0/1)
System Information Discovery
System Location Discovery (0/1)
System Network Configuration Discovery (0/1)
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtualization/Sandbox Evasion (0/3)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (0/6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)
Collection
17 techniques
Adversary-in-the-Middle (0/3)
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (0/4)
Communication Through Removable Media
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/2)
Web Service (0/3)
Exfiltration
9 techniques
Automated Exfiltration (0/1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking
Service Stop
System Shutdown/Reboot