Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

[JP Cyber Solutions], LLC

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	JP Cyber Solutions, LLC
Contact Name	Joey Peter
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	[joey]@[jpcsllc].com

Document History

Version	Date	Author(s)	Comments
001	10/29/2023	Joey Peter	
002	11/3/2023	Joey Peter	

Introduction

In accordance with MegaCorpOne's policies, JP Cyber Solutions, LLC (henceforth known as JPCS) 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 JPCS during October 2023.

For the testing, JPCS 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.

JPCS 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

JPCS 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

JPCS 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

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

Reporting

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

Scope

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

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

IP Address/URL	Description
172.22.117.0/24 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

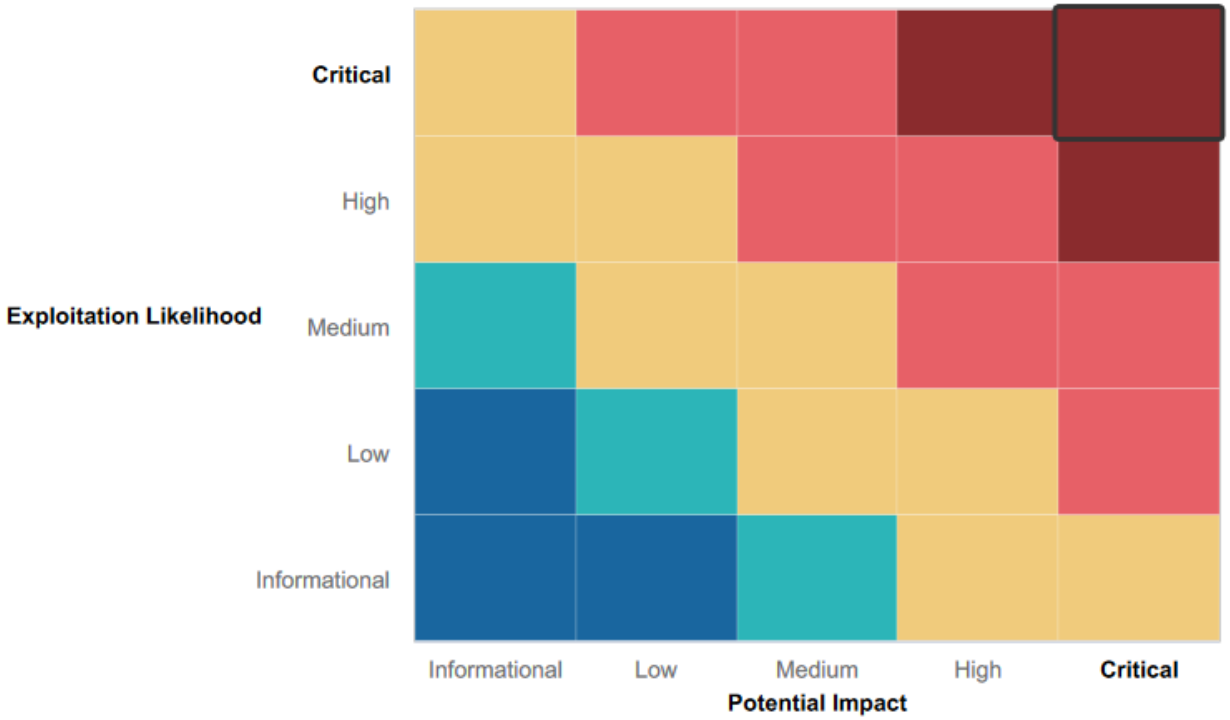
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Several metasploit exploits were rated positively but were ultimately unsuccessful in granting us access to the domain

Summary of Weaknesses

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

- Weak password policy across domain
- Least Privilege
- Critical ports open
- Reverse shell backdoor
- Admin credentials stored in plaintext
- LLMNR
- Internal IP addresses are public
- Several CVEs on apache server

Executive Summary

JPCS identified several critical vulnerabilities that need to be immediately addressed to prevent an attacker from gaining unauthorized access to Megacorpone's assets.

Our testing revealed vulnerabilities with open ports that allowed us to establish backdoor access. During our initial reconnaissance we identified the IP address for the web application then used shodan.io and to identify server information for the application. While shodan.io revealed multiple CVE's associated with the web server version used, we did not specifically test them. A zenmap scan showed a backdoor vulnerability associated with 172.22.117.150, a linux machine.

We were able to guess weak passwords to gain initial access to the domain on the Linux machine. We then exfiltrated additional user credentials after using metasploit to open a root shell then cracked those hashes on our attacking machine. We also determined that Megacorpone is vulnerable to LLMNR attacks, which is another method of obtaining credentials. With these cracked credentials we were able to laterally move between machines and continue escalating our privileges to domain administrator, granting us unrestricted access to the entire domain.

The Vulnerabilities Findings section of this report will provide more details about each vulnerability we discovered. Although most of these vulnerabilities are critical, they should be fairly easy to implement and little-to-no-cost.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Port 21 open on 172.22.117.150	Critical
Admin credentials stored in plaintext	Critical
LLMNR	High
CVE Vulnerabilities	High
Public Domain IP addresses	Medium

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

Scan Type	Total
Hosts	149.56.244.87 - megacorpone.com 172.22.117.100 – host machine 172.22.117.150 – Linux machine 172.22.117.20 – Windows10 machine 172.22.117.10 – WinDC01 – Domain Controller
Ports	21 FTP, 22 SSH, 80 HTTP, 443 HTTPS, 445 SMB, 139 RPC/SMB, 3389 RDP, 88 Kerberos

Exploitation Risk	Total
Critical	3
High	2
Medium	1
Low	0

Vulnerability Findings

Weak Password Policy

Risk Rating: Critical

Description:
Initial access was gained through Google reconnaissance and password guessing. Admin credentials were stored in plaintext on a Linux machine. Users of all privilege levels are using weak passwords and are vulnerable to dictionary attacks.

Affected Hosts: vpn.megacorpone.com; 172.22.117.150, 172.22.117.20, 172.22.117.10

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.
Enforce policy prohibiting plaintext password storage
Reset all user passwords

Admin Credentials Stored In Plaintext

Risk Rating: Critical

Description:
The machine with port 21 open had a plaintext file in the root directory called “adminpassword.txt”, which was not encrypted or password protected. It contained admin credentials which we were able to use to quickly escalate our privileges to the root on this machine. From there we could begin exfiltrating data and start to move around within the domain.

Affected Hosts: 172.22.117.150 - Linux Machine

```
find / -type f -iname *admin*.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/Main/TWikiAdminGroup.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/AdminSkillsAssumptions.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/TWikiAdminCookBook.txt
/var/tmp/adminpassword.txt
/var/www/twiki/data/Main/TWikiAdminGroup.txt
/var/www/twiki/data/TWiki/AdminSkillsAssumptions.txt
/var/www/twiki/data/TWiki/TWikiAdminCookBook.txt
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
```

Remediation:

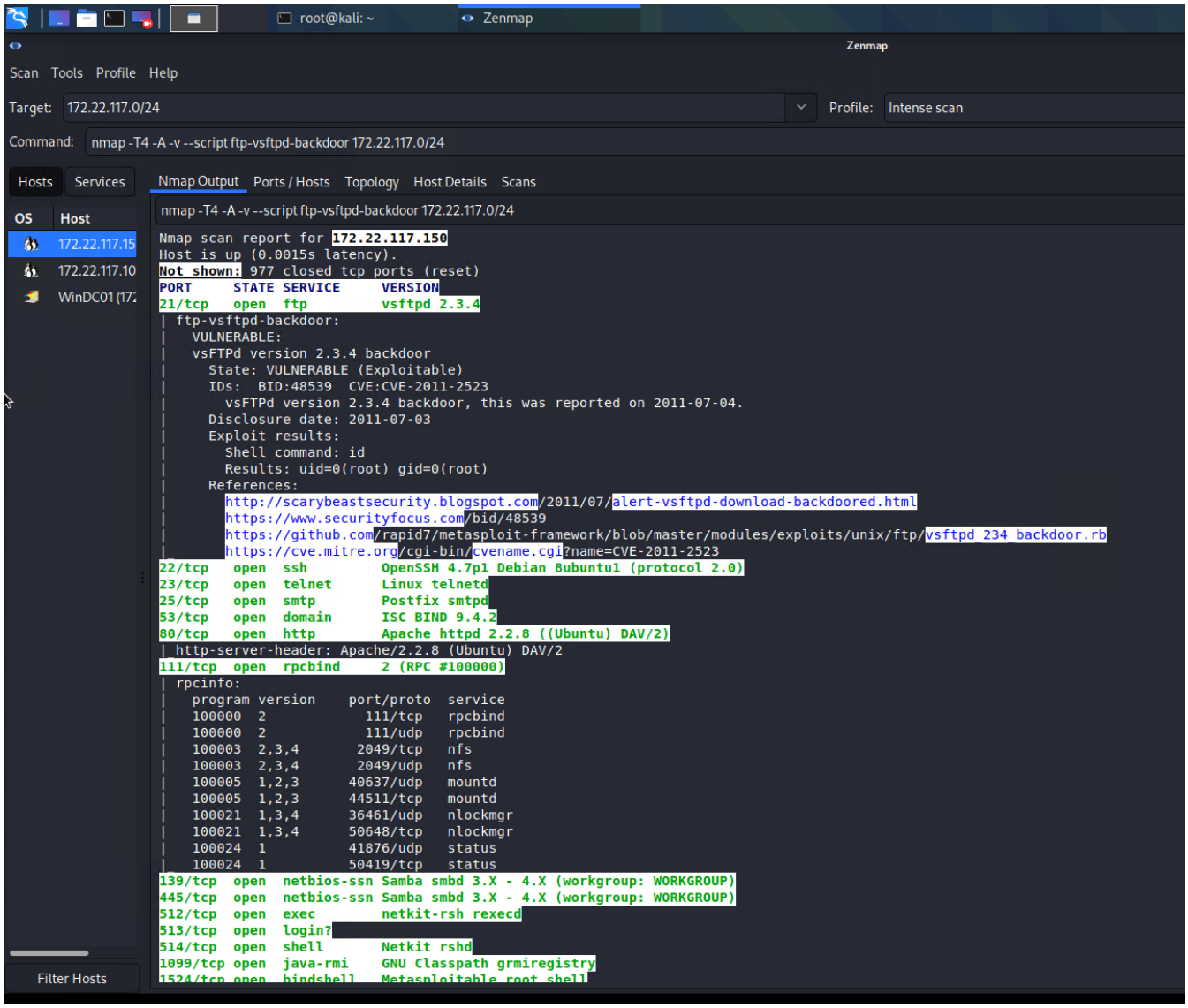
- Implement acceptable use policy that prohibits storing credentials in plaintext anywhere on the domain
- Address in conjunction with weak password policy and principles of least privilege

Port 21 (FTP) Open

Risk Rating: Critical

Description:
Using a zenmap scan we identified Port 21 (FTP) open on a linux machine, 172.22.117.150. This port is known to have vulnerabilities if not properly controlled and administered. The scan also showed us the version of FTP being used and a specific backdoor exploit this version was vulnerable to. Further testing confirmed we were able to establish a backdoor session.

Affected Hosts: 172.22.117.150 - Linux Machine



Remediation:

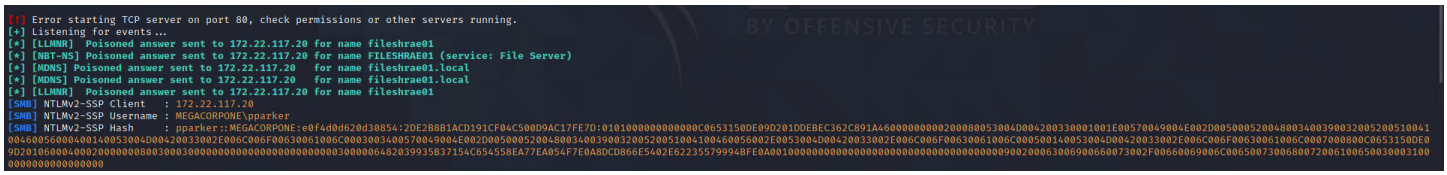
- Close port 21
- Use a firewall and throttle port 21 activity if kept open
- Deploy updated OS versions
- Use antimalware/antivirus and update regularly

LLMNR

Risk Rating: High

Description:
Local Link Multicast Name Resolution (LLMNR) is sometimes used as a backup protocol for DNS. This can be exploited by listening for LLMNR requests and spoofing a response to initiate a handshake request, which provides credentials. We were able to execute this and obtain a set of credentials we had not yet identified.

Affected Hosts: 172.22.117.20 - Windows 10 Machine



Remediation:

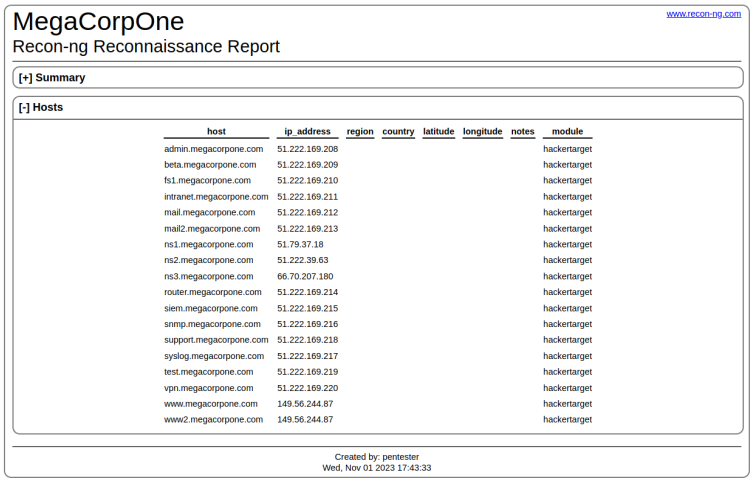
- Disable LLMNR
- Firewall policies

Domain IP Addresses are public

Risk Rating: Medium

Description:
Configuring hackertarget in recon-ng against the web application gave us all the public hosts on the domain. These are publicly available tools that could leave Megacorpone vulnerable to DNS spoofing.

Affected Hosts:



MegaCorpOne

www.recon-ng.com

Recon-ng Reconnaissance Report

[+] Summary

[-] Hosts

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

Created by: pentester
Wed, Nov 01 2023 17:43:33

Remediation:

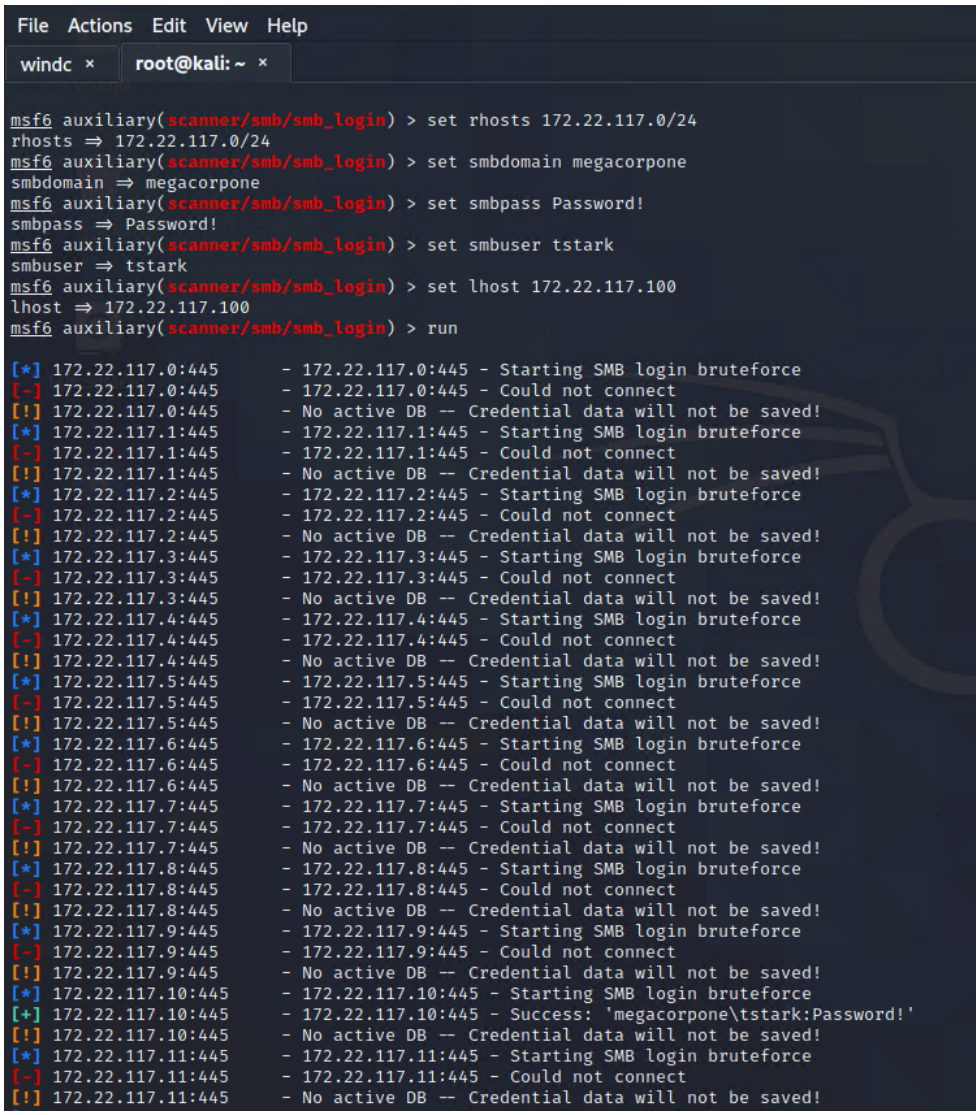
- Make server IP addresses private

Privilege Escalation/Least Privilege

Risk Rating: High

Description:
This is related to the weak password vulnerabilities we found. Through password-spraying and vulnerability scanning we were able to laterally move throughout the domain and escalate our privileges from a low-privileged user to the highest level possible.

Affected Hosts: 172.22.117.150, 172.22.117.20, 172.22.117.10



Remediation:

- Use patched & updated systems to mitigate known vulnerabilities
- Only give admin/root/system privileges to users who truly need it
- Network segmentation to make lateral movement more difficult

MITRE ATT&CK Navigator Map