Cybersecurity

Penetration Test Report - BryanSec, LLC

MegaCorpOne

Penetration Test Report

BryanSec, LLC

Confidentiality Statement

Table of Contents

Contact Information

Company Name	BryanSec, LLC
Contact Name	Bryan Harrick
Contact Title	Penetration Tester
Contact Phone	203.807.1887
Contact Email	HarrickBryan@gmail.com

Document History

Version	Date	Author(s)	Comments
001	10/17/2024	Bryan Harrick	

Introduction

In accordance with MegaCorpOne's policies, BryanSec, LLC (henceforth known as BSec 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 BSec during October of 2024.

For the testing, BSec 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.

BSec 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

BSec 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

BSec 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

BSec '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

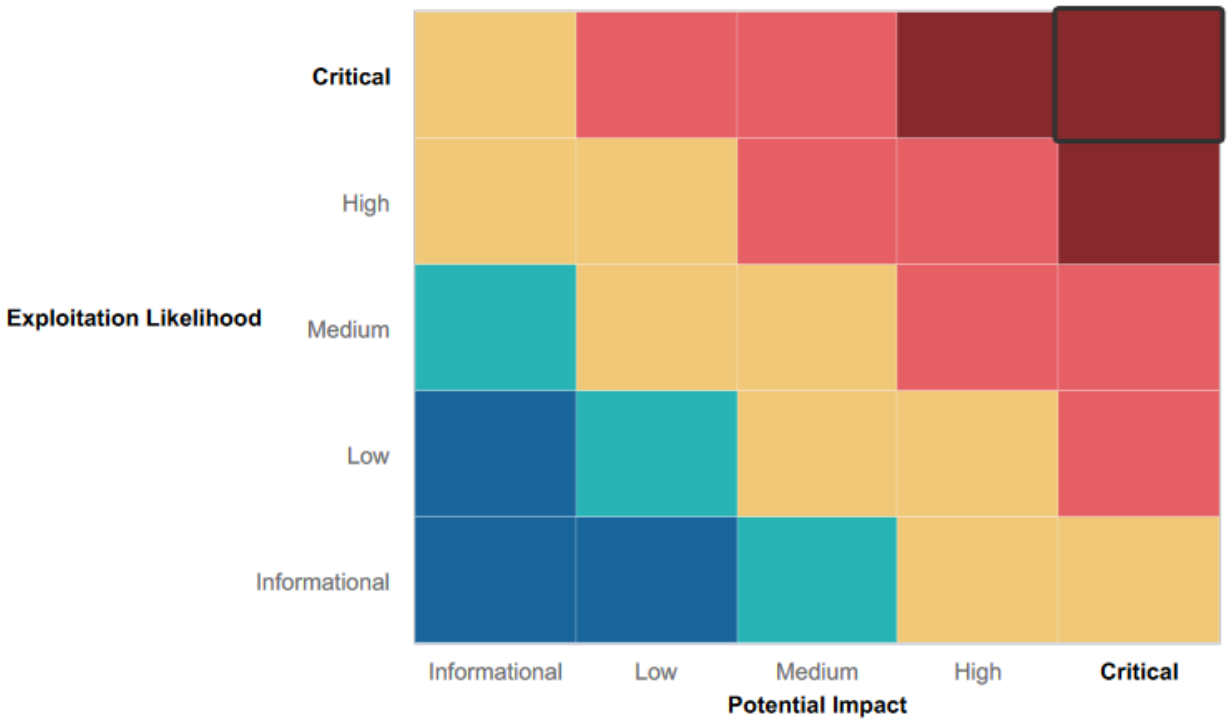
Executive Summary of Findings

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.

- Firewall being utilized by Megacorpone

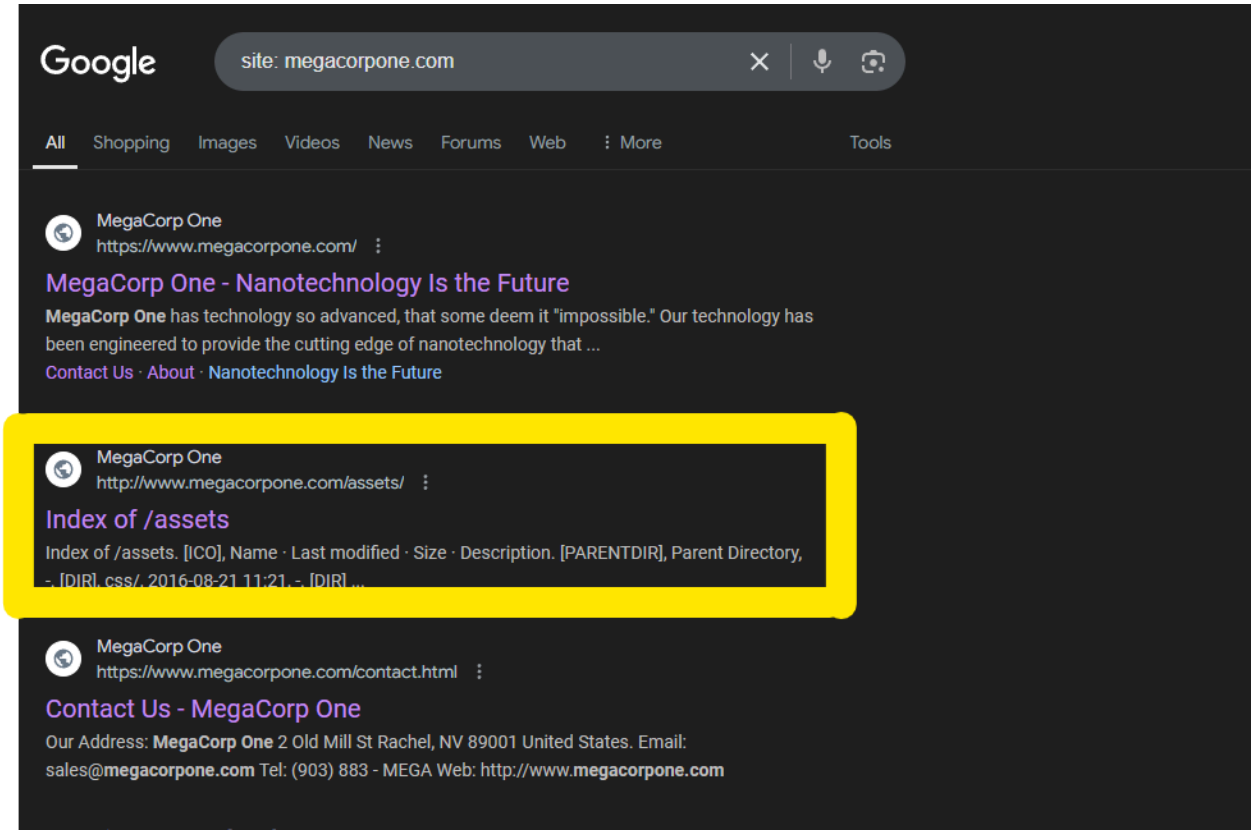
Summary of Weaknesses

BSec 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.

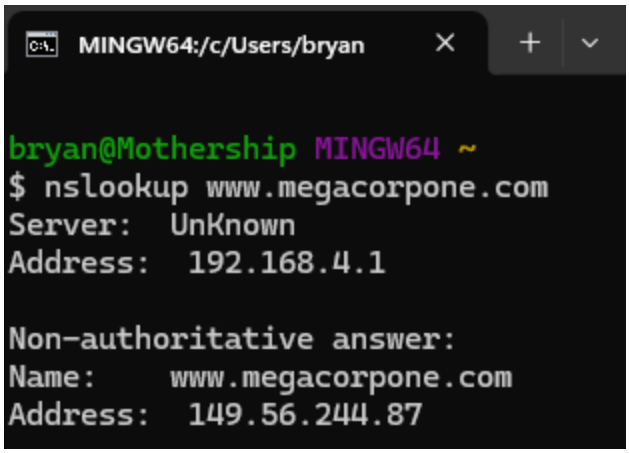
- Very weak passwords for User accounts, as well as for the Servers.
- Many open ports when scanning with Nmap, many known exploits/ Bind shell Backdoor exploit.
- Google dorking exposed employee email addresses, first and last names, and domain information.

Executive Summary

- First I went Google Hacking, also known as Google dorking which is the practice of using advanced search queries and operators on Google to find sensitive information that may generally not be as easily accessible with normal searches. Using Google dorking, I was able to uncover employee email addresses, employees first and last names, and domain information.

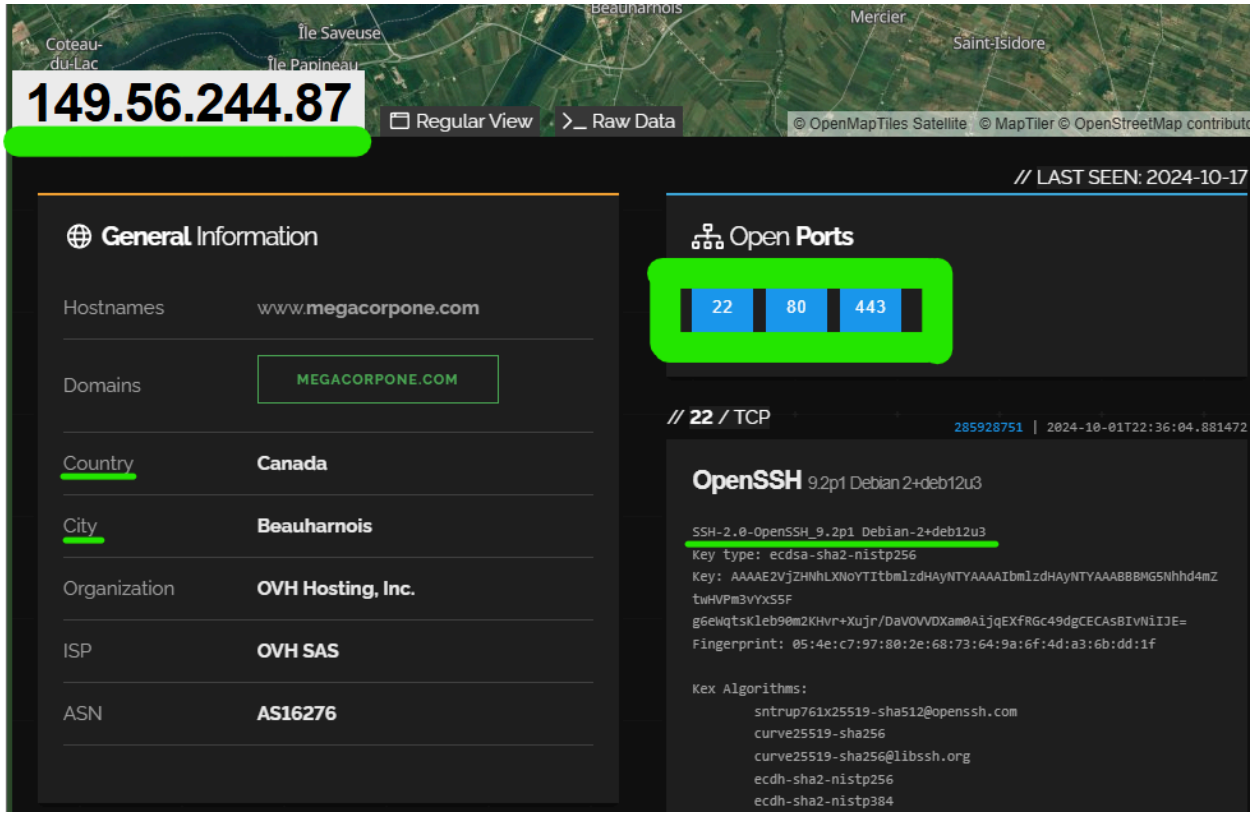


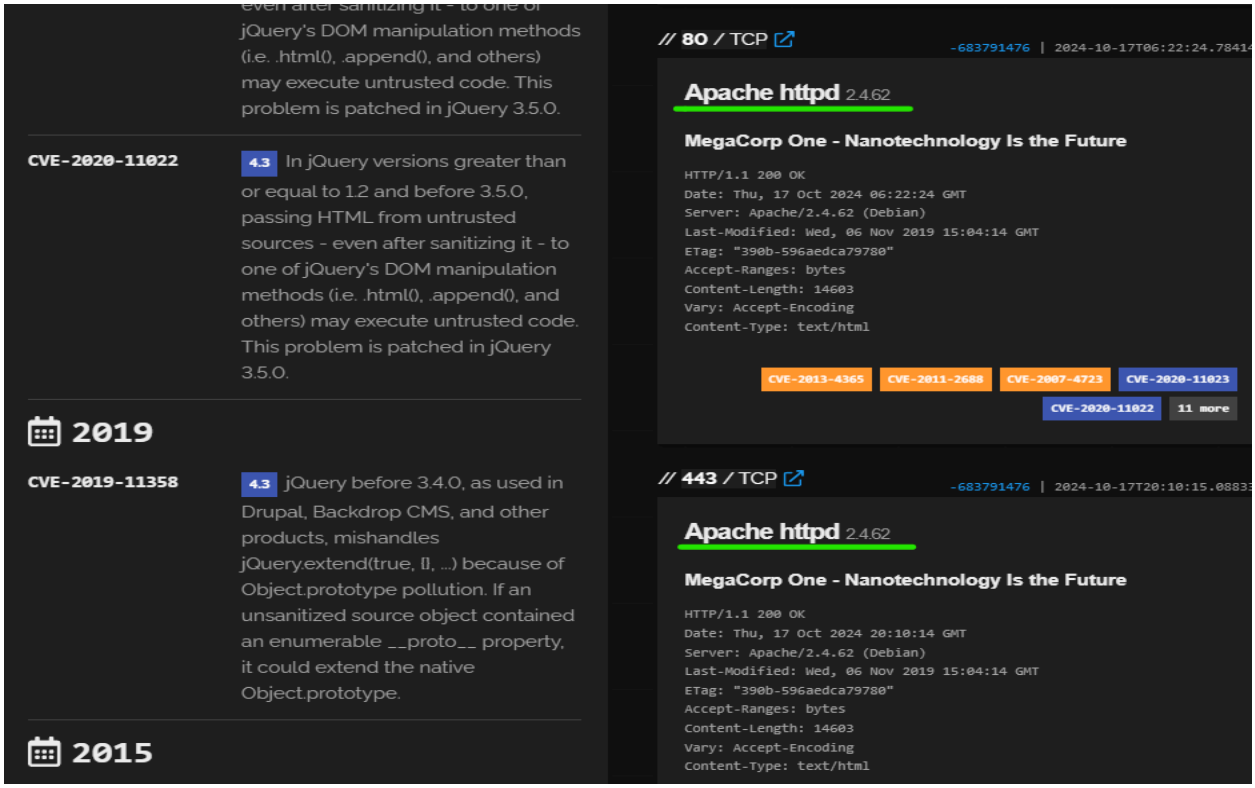
- After dorking, I was able to Password guess via the website vpn.megacorpone.com and was able to log into multiple accounts. This shows that users and servers have very weak passwords.
- Next I used an NSLOOKUP to obtain the IP address of MegaCorpOne. Which is 149.56.244.87



- Next I used the website Shodan.io to enumerate the network. This showed me numerous ports that are open. Including Ports 22, 80 and 443. This also showed that the SSH version the server is running is SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3. The Operating System of the server is Debian. The web server that is being utilized is Apache 2.4.62. It also

shows many vulnerabilities that may be present on the server. Also showing me where the server is located, which is Beauharnois, Canada.





Vulnerabilities All ports Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

2020

CVE-2020-11023	4.3	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
CVE-2020-11022	4.3	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

2019

CVE-2019-11358	4.3	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

2015

CVE-2015-9251	4.3	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

2013

CVE-2013-4365	7.5	Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
CVE-2013-2765	5.0	The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
CVE-2013-0942	4.3	Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

- I used Traceroute, which is a network diagnostic tool which tracks the path that packets take from one device on a network to another, across an IP network. This shows Path Discover, Measures latency, and assists in troubleshooting networks. I ran this command and observed that there are significant measures of security on Megacorpone's network. The most significant security measure I have observed is a Firewall. The Firewall helps Megacorpone against incoming threats to the network.

```
MINGW64:/c/Users/bryan

bryan@Mothership MINGW64 ~
$ tracert 149.56.244.87

Tracing route to www.megacorpone.com [149.56.244.87]
over a maximum of 30 hops:

  1     3 ms     4 ms     3 ms  192.168.4.1
  2     7 ms     5 ms    49 ms  32.221.200.1
  3     5 ms     5 ms     7 ms  ae11---100.car02.wlfr.ct.frontiernet.net [1
72.76.21.25]
  4     9 ms     8 ms     9 ms  45.52.201.234
  5     9 ms    19 ms     9 ms  ae4---0.cbr02.sccs.nj.frontiernet.net [74.4
1.143.173]
  6    15 ms    12 ms    12 ms  eqx.ny.ovh.net [198.32.118.106]
  7    14 ms     *        *     nyc-ny1-sbb2-8k.nj.us [198.27.73.218]
  8     *        *        *     Request timed out.
  9    15 ms    12 ms    11 ms  nyc-ny1-sbb2-8k.nj.us [198.27.73.218]
 10    17 ms    18 ms    18 ms  be102.bhs-g2-nc5.qc.ca [192.99.146.138]
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15    22 ms    42 ms    25 ms  www.megacorpone.com [149.56.244.87]

Trace complete.

bryan@Mothership MINGW64 ~
$
```

- I also used a Nmap scan which I observed several ports open that are commonly used for targeting and abuse. These ports include
    1. Port 53- DNS (often used for amplification of DDos Attacks).
    2. Port 139- NetBIOS (primarily used for file/ printer sharing).
    3. Port 80- HTTP (servers exposed and can be a target of an attack).
    4. Port 445- SMB (sharing capabilities of printers/files).
    5. Port 3306- SQL Server/MySQL (Malware may be distributed here).

```
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3390/tcp open  dsc
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
80/tcp   open     http
5901/tcp open     vnc-1
6001/tcp open     X11:1
```

Summary Vulnerability Overview

Vulnerability	Severity
Weak Password on Public Web Application	Critical
Weak-Stored Password Policy	Critical
SSH-Key Exchange	Low
VSFTPD Backdoor	Critical

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

Scan Type	Total
Hosts	Windows 172.22.117.20 Linux 172.22.117.100 WinDC 172.22.117.10
Ports	Linux: 80,5901,6001,8080 Windows: 135, 139, 445, 3390 WinDC10: 53, 88, 135, 139, 389, 445,463, 493, 636, 3268, 3269

Exploitation Risk	Total
Critical	3
High	0
Medium	0
Low	1

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. This site is secured with basic authentication but is susceptible to a dictionary attack. BSec 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.

Affected Hosts: vpn.megacorpone.com

Remediation:

- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset the user **thudson**'s password.

Weak-Stored Password Policy

Risk Rating: Critical

Description:
MegaCorpOne's internal application stores user passwords in plaintext within the database, making them vulnerable to unauthorized access. If an attacker gains access to the database, they can retrieve users' plaintext passwords, posing a serious security risk.

Affected Hosts:
intranet.megacorpone.com

Remediation:

- Update the password storage mechanism to use salted and hashed passwords with a secure hashing algorithm, such as bcrypt or Argon2.
- Implement strong access controls on the database to restrict unauthorized access.
- Enforce a password policy that requires passwords to be over 12 characters long, include both upper and lower case letters, and include a special character.
- Reset passwords for all users and instruct them on the importance of password security best practices.

Weak SSH Key Exchange

Risk Rating: Low

Description:
The SSH service on MegaCorpOne's server uses outdated and weak key exchange algorithms, making it marginally vulnerable to downgrade attacks. While the risk is low, an attacker could potentially exploit this weakness to intercept SSH traffic under specific conditions.

Affected Hosts:
ssh.megacorpone.com

Remediation:

- To improve security, update your SSH configuration so that it only permits strong key exchange algorithms, like `curve25519-sha256` and `diffie-hellman-group-exchange-sha256`. These two are widely compatible with most modern Linux and Unix systems—especially on recent versions of OpenSSH—but a heads-up: some older systems or unique SSH setups might struggle with them.
- Also, be sure to disable any weaker algorithms, such as `diffie-hellman-group1-sha1`, which don't hold up as well against today's security standards. It's a good idea to review your SSH configuration every so often too, just to stay on top of any evolving best practices for secure key exchange.

VSFTPD Backdoor

Risk Rating: Critical

Description:
The VSFTPD (Very Secure FTP Daemon) version 2.3.4 used on MegaCorpOne's server is known to contain a backdoor vulnerability. Attackers can exploit this backdoor to establish unauthorized shell access by simply logging in with a username ending in `:)`. This allows them to potentially gain full control over the system and access sensitive data.

Affected Hosts:
ftp.megacorpone.com

Remediation:

- Immediately update VSFTPD to a secure version that addresses this vulnerability, as version 2.3.4 is no longer safe for use.
- Restrict access to the FTP server temporarily until the update is applied to mitigate potential unauthorized access.
- Review and monitor FTP server logs closely for any suspicious login attempts, particularly those with the `:)` pattern, to detect any backdoor exploitation attempts.

MITRE ATT&CK Navigator Map

domain

Enterprise ATT&CK v15

platforms

Windows, Linux, macOS,
Network, PRE, Containers, Office 365,
SaaS, Google Workspace, IaaS, Azure AD

legend

Success | Failure