Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

BigBox Security, 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	BigBox Security, LLC
Contact Name	Dylan Strube
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	dylan@bbsecurity.com

Document History

Version	Date	Author(s)	Comments
001	2/14/2024	Dylan	

Introduction

In accordance with MegaCorpOne's policies, BigBox Security, LLC (henceforth known as BBS) 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 BBS during February of 2024.

For the testing, BBS 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.

BBS 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

BBS 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

BBS 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

BBS'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

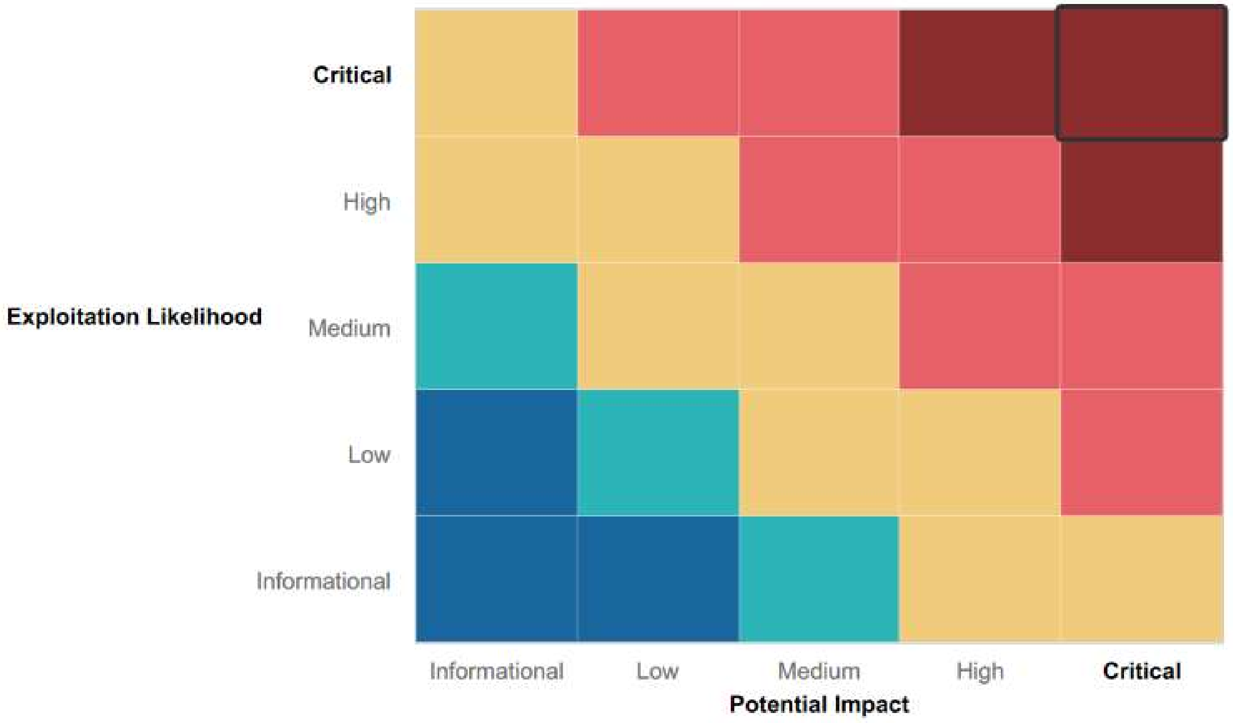
Executive Summary of Findings

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.

- Debian used as the OS.
- Uses a VPN.

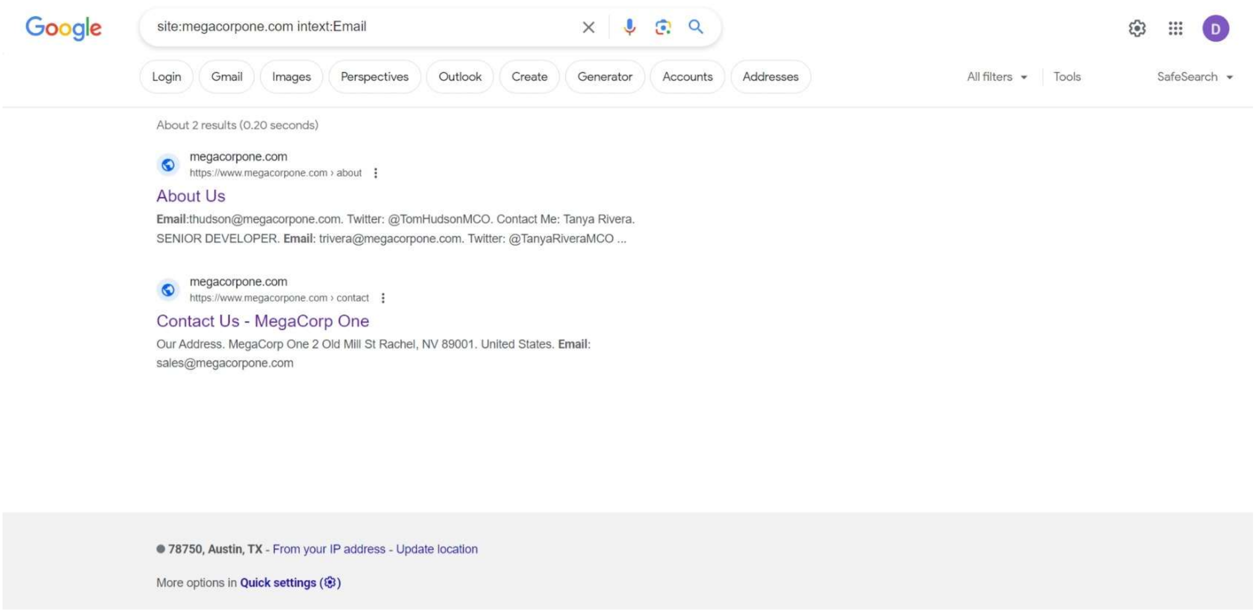
Summary of Weaknesses

BBS 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.

- Usernames and passwords are very weak.
- Port 22 was open during a Shodan scan, meaning weak SSH configuration and network is open to Port Scanning.
- A Machine on the network with an open port was vulnerable to backdoor exploitation.
- Weak firewall rules.
- Weak SMB settings.

Executive Summary

Using Google Hacking, I found a list of contact information for several employees. I also found a page showing a list of assets as well as information about what OS is used for the website. Next, I used Shodan to determine what ports were open, the version of SSH it uses, the version of the web server, the OS, a list of its vulnerabilities, and the location of the server. Using Recon-ng, I compiled a report of available OSINT information. Using the information I found when looking for contact info on employees, I was able to successfully guess a password for user thudson and login to the website. I then identified the subnet and used Zenmap to identify an IP address with port 21 open and vulnerable to a backdoor exploit.



site:megacorpone.com intext:Email

About 2 results (0.20 seconds)

megacorpone.com
https://www.megacorpone.com › about

About Us

Email:thudson@megacorpone.com. Twitter: @TomHudsonMCO. Contact Me: Tanya Rivera. SENIOR DEVELOPER. **Email**: trivera@megacorpone.com. Twitter: @TanyaRiveraMCO ...

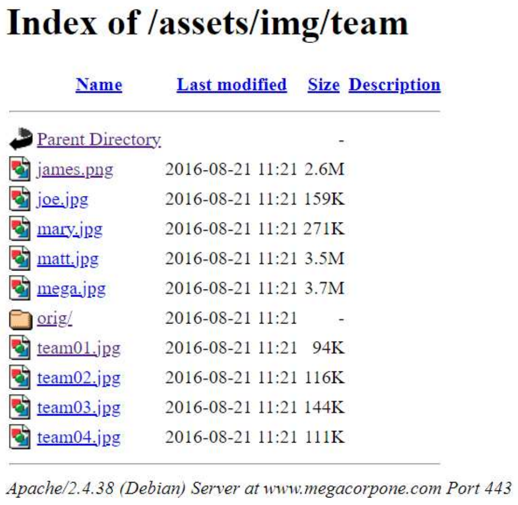
megacorpone.com
https://www.megacorpone.com › contact

Contact Us - MegaCorp One

Our Address. MegaCorp One 2 Old Mill St Rachel, NV 89001. United States. **Email**: sales@megacorpone.com

● **78750, Austin, TX** - From your IP address - Update location

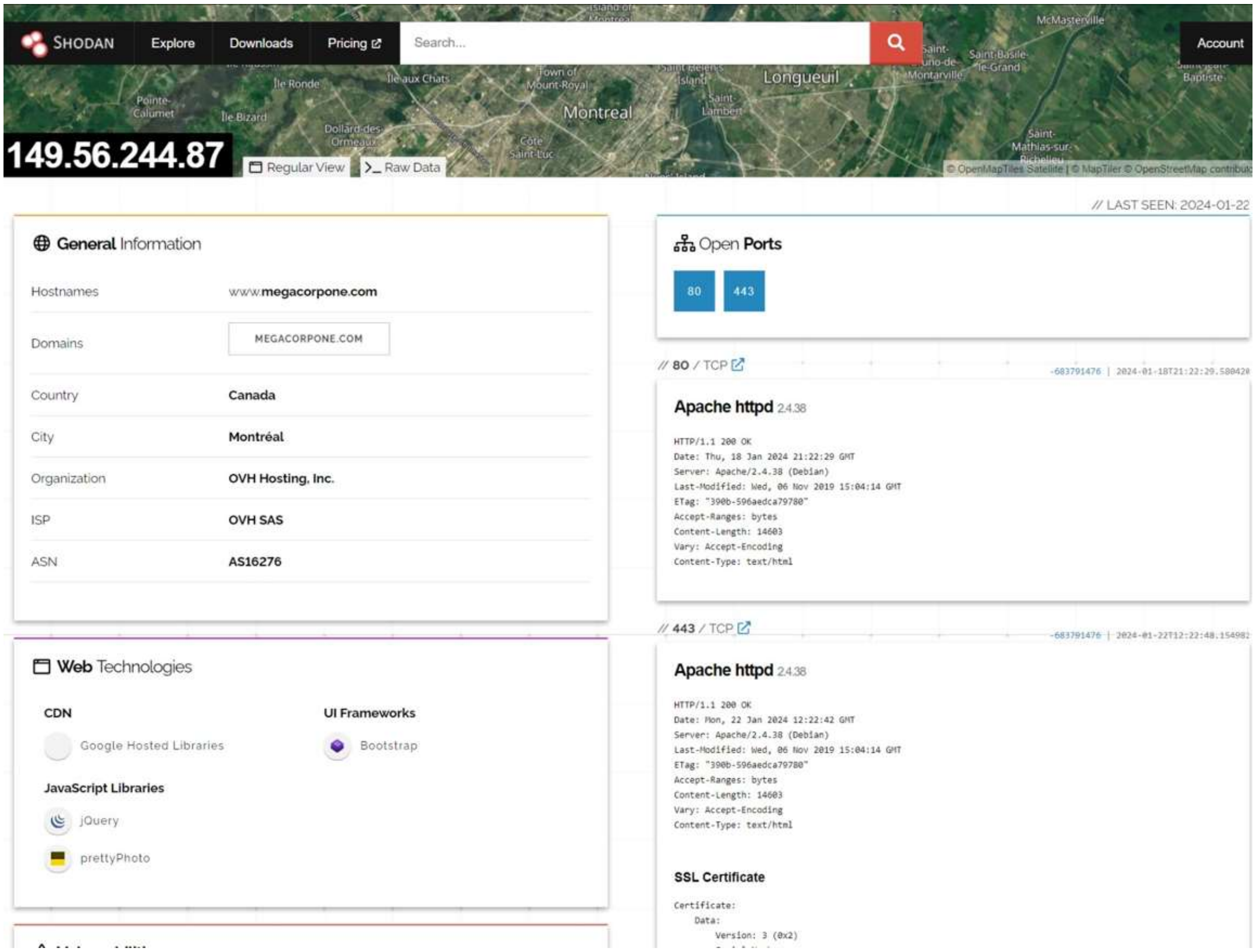
More options in **Quick settings** (⚙)



Index of /assets/img/team

Name	Last modified	Size	Description
Parent Directory		-	
james.png	2016-08-21 11:21	2.6M	
joe.jpg	2016-08-21 11:21	159K	
mary.jpg	2016-08-21 11:21	271K	
matt.jpg	2016-08-21 11:21	3.5M	
mega.jpg	2016-08-21 11:21	3.7M	
orig/	2016-08-21 11:21	-	
team01.jpg	2016-08-21 11:21	94K	
team02.jpg	2016-08-21 11:21	116K	
team03.jpg	2016-08-21 11:21	144K	
team04.jpg	2016-08-21 11:21	111K	

Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 443



149.56.244.87

// LAST SEEN: 2024-01-22

General Information

Hostnames	www.megacorpone.com
Domains	MEGACORPONE.COM
Country	Canada
City	Montréal
Organization	OVH Hosting, Inc.
ISP	OVH SAS
ASN	AS16276

Web Technologies

CDN
- Google Hosted Libraries

UI Frameworks
- Bootstrap

JavaScript Libraries
- jQuery
- prettyPhoto

Open Ports

80 443

// 80 / TCP   -683791476 | 2024-01-18T21:22:29.580420

Apache httpd 2.4.38

```
HTTP/1.1 200 OK
Date: Thu, 18 Jan 2024 21:22:29 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
```

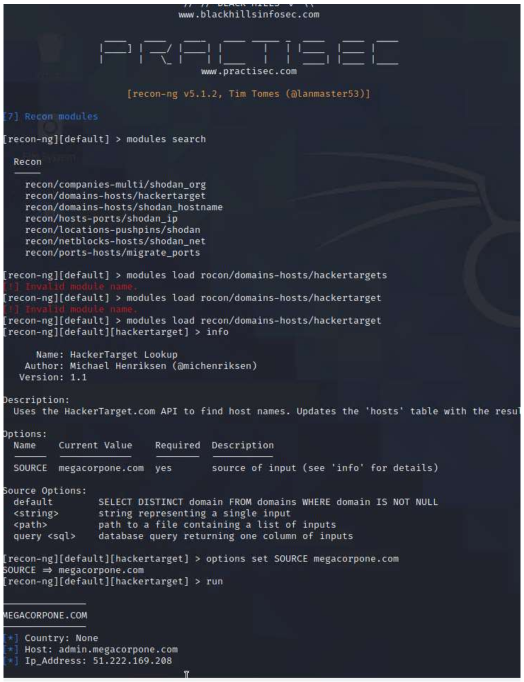
// 443 / TCP   -683791476 | 2024-01-22T12:22:48.154982

Apache httpd 2.4.38

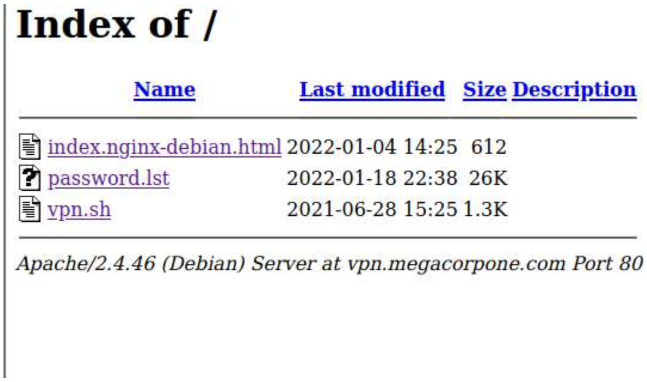
```
HTTP/1.1 200 OK
Date: Mon, 22 Jan 2024 12:22:42 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
```



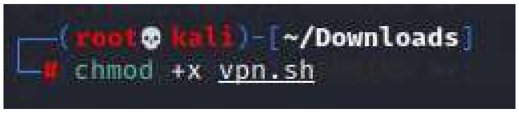
```
                  www.blackhillsinfosec.com

                        PRACTISEC
                      www.practisec.com

           [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[7] Recon modules

[recon-ng][default] > modules search

  Recon
  -----
    recon/companies-multi/shodan_org
    recon/domains-hosts/hackertarget
    recon/domains-hosts/shodan_hostname
    recon/hosts-ports/shodan_ip
    recon/locations-pushpins/shodan
    recon/netblocks-hosts/shodan_net
    recon/ports-hosts/migrate_ports

[recon-ng][default] > modules load rocon/domains-hosts/hackertargets
[!] Invalid module name.
[recon-ng][default] > modules load rocon/domains-hosts/hackertarget
[!] Invalid module name.
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the resul

Options:
  Name    Current Value    Required  Description
  ------  ---------------  --------  -----------
  SOURCE  megacorpone.com  yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][hackertarget] > options set SOURCE megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][hackertarget] > run

---------------
MEGACORPONE.COM
---------------
[*] Country: None
[*] Host: admin.megacorpone.com
[*] Ip_Address: 51.222.169.208
```



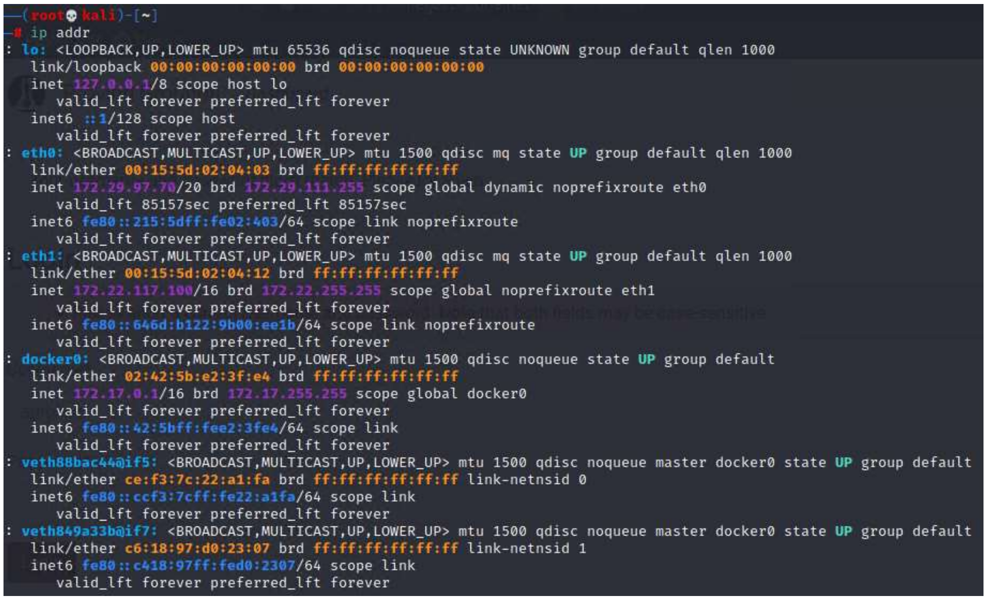
Index of /

Name	Last modified	Size	Description
index.nginx-debian.html	2022-01-04 14:25	612	
password.lst	2022-01-18 22:38	26K	
vpn.sh	2021-06-28 15:25	1.3K	

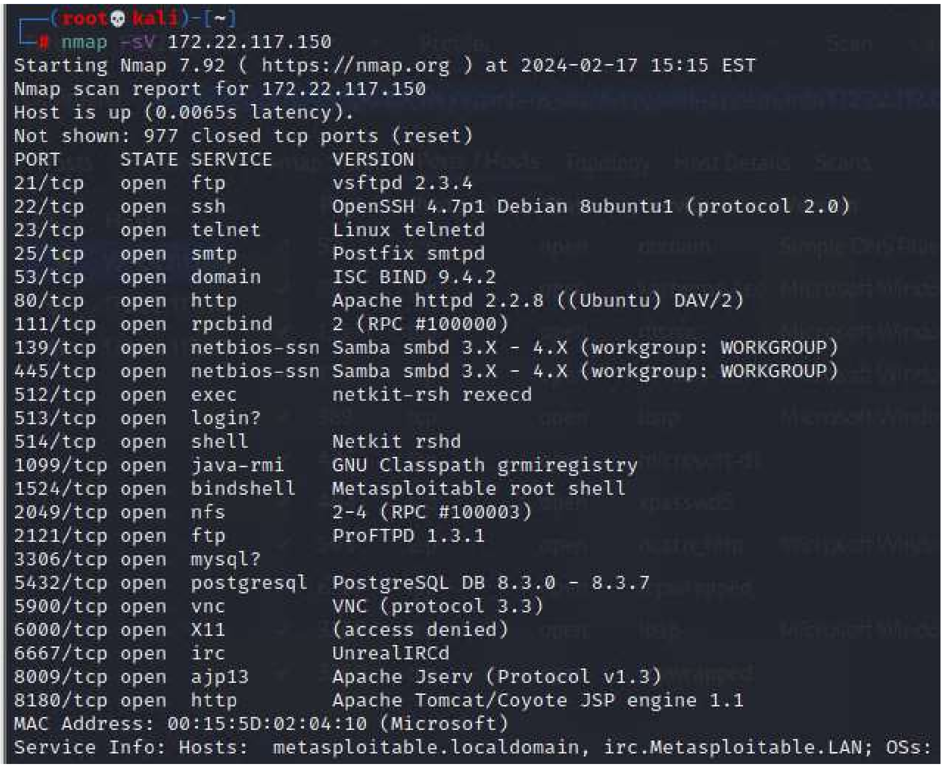
Apache/2.4.46 (Debian) Server at vpn.megacorpone.com Port 80



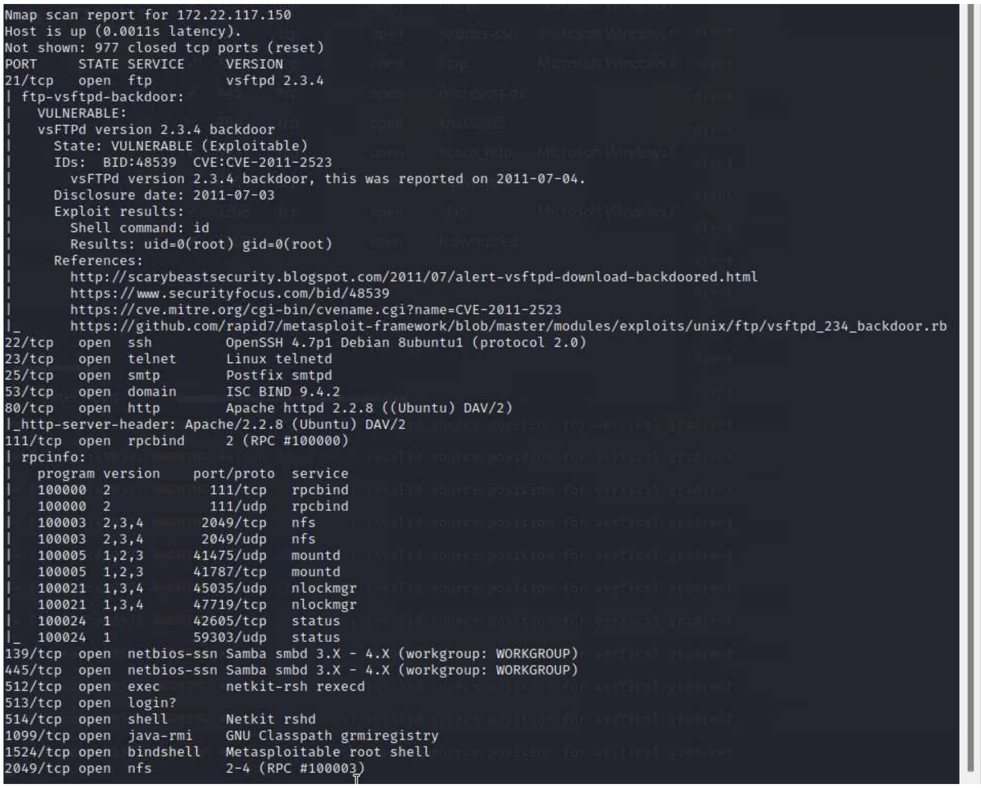
```
┌──(root💀kali)-[~/Downloads]
└─# chmod +x vpn.sh
```



```
──(root💀kali)-[~]
─# ip addr
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
     valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
     valid_lft forever preferred_lft forever
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether 00:15:5d:02:04:03 brd ff:ff:ff:ff:ff:ff
  inet 172.29.97.70/20 brd 172.29.111.255 scope global dynamic noprefixroute eth0
     valid_lft 85157sec preferred_lft 85157sec
  inet6 fe80::215:5dff:fe02:403/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether 00:15:5d:02:04:12 brd ff:ff:ff:ff:ff:ff
  inet 172.22.117.100/16 brd 172.22.255.255 scope global noprefixroute eth1
     valid_lft forever preferred_lft forever
  inet6 fe80::646d:b122:9b00:ee1b/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
  link/ether 02:42:5b:e2:3f:e4 brd ff:ff:ff:ff:ff:ff
  inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
     valid_lft forever preferred_lft forever
  inet6 fe80::42:5bff:fee2:3fe4/64 scope link
     valid_lft forever preferred_lft forever
: veth88bac44@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
  link/ether ce:f3:7c:22:a1:fa brd ff:ff:ff:ff:ff:ff link-netnsid 0
  inet6 fe80::ccf3:7cff:fe22:a1fa/64 scope link
     valid_lft forever preferred_lft forever
: veth849a33b@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
  link/ether c6:18:97:d0:23:07 brd ff:ff:ff:ff:ff:ff link-netnsid 1
  inet6 fe80::c418:97ff:fed0:2307/64 scope link
     valid_lft forever preferred_lft forever
```



```
┌──(root💀kali)-[~]
└─# nmap -sV 172.22.117.150
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-17 15:15 EST
Nmap scan report for 172.22.117.150
Host is up (0.0065s 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?
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:
```



```
Nmap scan report for 172.22.117.150
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
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)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      41475/udp   mountd
|   100005  1,2,3      41787/tcp   mountd
|   100021  1,3,4      45035/udp   nlockmgr
|   100021  1,3,4      47719/tcp   nlockmgr
|   100024  1          42605/tcp   status
|_  100024  1          59303/udp   status
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)
```

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	**Critical**
Weak firewall rules.	**Critical**
Weak SSH configuration.	**High**
A Machine on the network with an open port was vulnerable to VSFTPD backdoor exploitation.	**High**
Network is open to Port Scanning.	**Medium**

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

Scan Type	Total
Hosts	117.22..117.100 117.22.117.150
Ports	80, 5901, 6001, 8080

Exploitation Risk	Total
Critical	2
High	2
Medium	1
Low	0

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. BBS 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

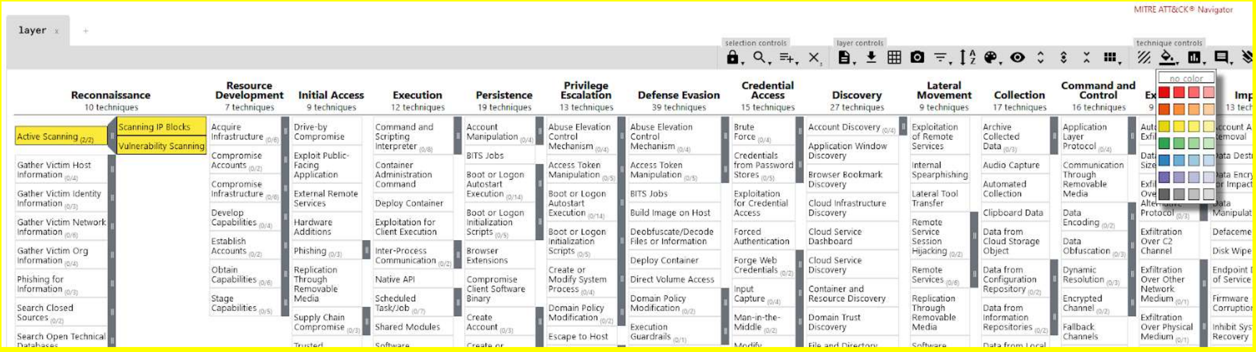
Remediation:

- 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.

Usernames should be changed to something that is different from employee emails. Regular port scanning on the network to ensure there are not any open that should be.

MITRE ATT&CK Navigator Map

[Using the MITRE ATT&CK Navigator, build out a map showing what techniques you've used so far. To do so, on the MITRE ATT&CK Navigator page, click "Create New Layer," then "Enterprise," and select each technique that you've used. Change the color of each selected technique to highlight it in yellow if it was successful, or in red if it was unsuccessful, as the following image shows:



layer

MITRE ATT&CK® Navigator

Reconnaissance — 10 techniques
- Active Scanning (2/2)
  - Scanning IP Blocks
  - Vulnerability Scanning
- 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

Resource Development — 7 techniques
- Acquire Infrastructure (0/6)
- Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- Establish Accounts (0/2)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/5)

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

Execution — 12 techniques
- Command and Scripting Interpreter (0/8)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/2)
- Native API
- Scheduled Task/Job (0/7)
- Shared Modules
- Software

Persistence — 19 techniques
- Account Manipulation (0/4)
- 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

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

Defense Evasion — 39 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)

Credential Access — 15 techniques
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Man-in-the-Middle (0/2)
- Modify

Discovery — 27 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Container and Resource Discovery
- Domain Trust Discovery
- File and Directory

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

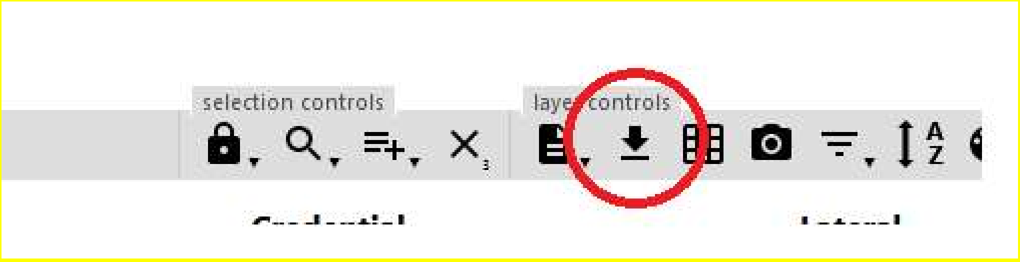
Collection — 17 techniques
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/2)
- Data from Local

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

Ex — 9
- Aut Exfil
- Data Size
- Exfil Ove Alter Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)

Imp — 13 tech
- ccount A emoval
- ata Destr
- ata Encry or Impact
- ata Manipulat
- Defaceme
- Disk Wipe
- Endpoint of Service
- Firmware Corruption
- Inhibit Sys Recovery

When you're done, be sure to download the chart as JSON by clicking the download icon, as the following image shows:

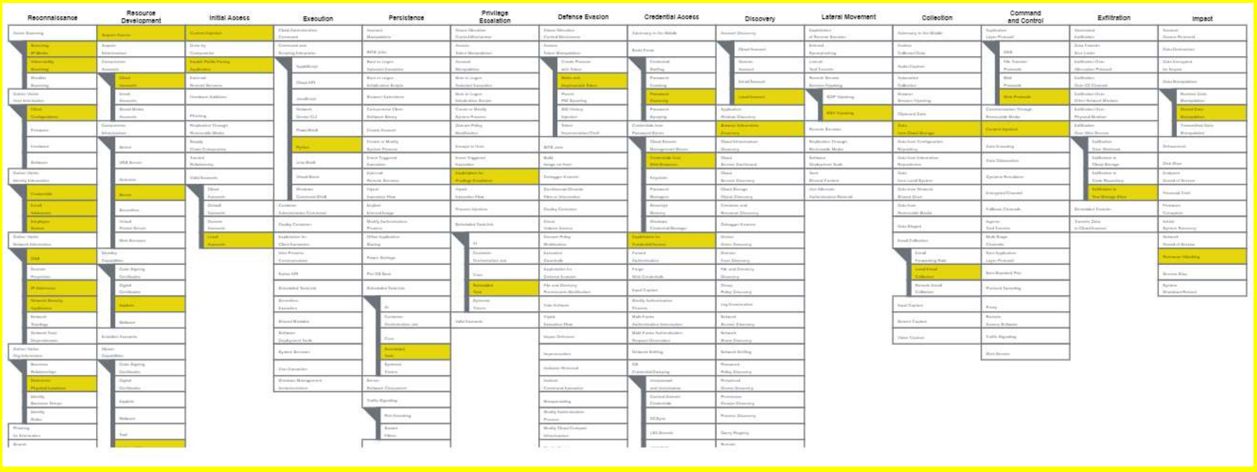


Remember, this report is not yet complete—we will finish it in the next module.

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

Legend:

Performed successfully
Failure to perform


Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact