



SAMPLE TESTING REPORT

## TABLE OF CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>Scope of Testing</b>	<b>4</b>
<b>Vulnerability Rating</b>	<b>5</b>
<b>Summary of Vulnerabilities &amp; Recommended Remediations</b>	<b>6</b>
• No limit for unsuccessful logins onto SSH service	7
• Default password policy for SSH service (Length + Complexity)	8
• Access Control, Principle of least privilege (Cameras, printer)	9
• Non encrypted port communication (Switches, Cameras, printer)	10
• Unused open ports	11
• Weak or default passwords (Switches)	12
• Patchable Systems (Apache)	13
• Patchable Systems (Samba)	14
• Utilization of end of life software and packages (Python2)	15
<b>Recommendations for Best Practices</b>	<b>16</b>
• Wireless Security (WPA2 vs WPA3)	16
• Third Party Repository Insecure Upgrades	17
• Insecure Cryptographic Algorithm (Md5)	17
<b>Security Matrix</b>	<b>18</b>
<b>Known Vulnerabilities / End of Life</b>	<b>19</b>
<b>Recommendations</b>	<b>20</b>
<b>Appendix</b>	<b>21</b>
• Criticality Rating	21
• Criticality Reference Table	22
• Tools Referenced	23
• Acronyms	24

## EXECUTIVE SUMMARY

A vulnerability assessment and penetration test was conducted in accordance with the organization [REDACTED] in regards to the internal network and security environment.

Efforts were based on analyzing nodes on the internal segment of the environment of organization [REDACTED] and to analyze for improved security posture and configuration.

After assessing the internal environment, we found several vulnerabilities that should be remediated in order to create better defensive posture and a more secure set of systems. Our findings, which will be outlined in this report, include the following areas of vulnerabilities:

- No limit for unsuccessful logins onto SSH service
- Default password policy for SSH service (Length + Complexity)
- Access Control, Principle of least privilege (Cameras, printer)
- Non encrypted port communication (Switches, Cameras, printer)
- Unused open ports
- Weak or default passwords (Switches)
- Patchable Systems (HTTP Server)
- Patchable Systems (File Sharing Server)
- Utilization of end of life software and packages (Python2)

We have included remediation steps for the vulnerabilities in this report.

In conclusion [REDACTED] should look to remediate these findings in order to increase the effectiveness of security within the organization.

## SCOPE OF TESTING

The scope of testing discussed and agreed upon with organization [REDACTED] included both an external and internal segments test. The external test would cover vulnerabilities associated with the internet-facing applications of organization [REDACTED], while the internal testing would cover the intranet and internal segments of the network.

The testing was done utilizing a gray box approach. Some credentials were provided in order to speed up the process of testing and vulnerability finding.

The external test included the web server, file sharing server, and DMZ switch. There were two (2) external public facing IPs provided in scope for organization [REDACTED] including [REDACTED] (Web server) and [REDACTED] (file sharing server). Furthermore, A minimalistic privileged user account for the SSH service on the linux environment of the web server was provided so a deep internal assessment of the SSH environment could be completed, in which we did find significant vulnerabilities needing to be addressed.

The internal test included the core switch, the access switches, the security cameras, the VoiP phones, the printer, and the wireless access point configurations. A spreadsheet of the two Vlans in this environment were provided and thereafter tested with internal testing tools. Our findings for the vulnerabilities are outlined in this report.

## VULNERABILITY RATING (CRITICALITY)

A criticality score, between 0 to 49, is calculated by adding individual scores from “Time”, “Expertise”, “Knowledge required”, “Access to product by attacker”, “Type of equipment”. A following example is shown:

Factor	Value	Points
Time	< 1 week	1
Expertise	Expert	6
Knowledge required	Restricted information	3
Access from Attacker	Moderate	4
Type of equipment	Standard	0

**Criticality: Medium (14)**

Scores are also labeled based on three levels of criticality:

**Critical - Score  $\geq 25$**

**Very High - Score between 20-24**

**High - Score between 14-19**

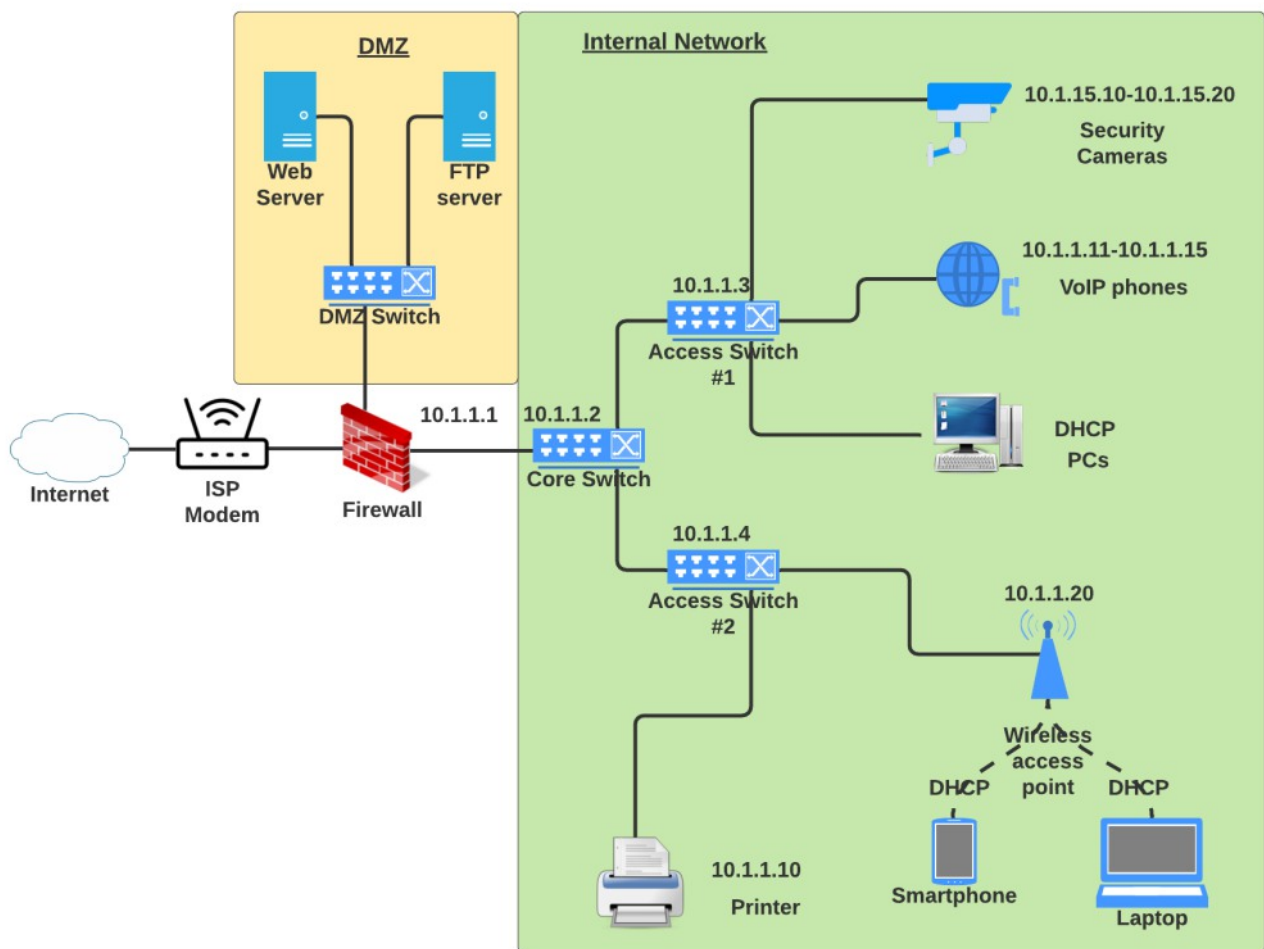
**Medium - Score between 10-13**

**Low - Score between 0-9**

Please refer to the criticality matrix in the appendix for more information.

## SUMMARY OF VULNERABILITIES

The following simplified network diagram illustrates the scope of internal testing in the infrastructure for the organization of [REDACTED] including the DMZ, Core Switch, Access switches, Surveillance Cameras, Printer, Server, VoIP Phones, and Wireless Access Points.



**VULNERABILITIES FOUND:****VULNERABILITY #1****CRITICALITY: CRITICAL (31)****NO LIMIT FOR SSH SERVICE  
LOGIN ATTEMPTS****LOCATION: WEB SERVER  
SSH SERVICE**

The SSH service on the web server has no limits for entering password attempts. This can lead to a successful brute-force login via tools such as Hydra. There should be a lock out mechanism established after a certain amount of login attempts.

```
(kali@kali)-[~]
└─$ sudo hydra -t 4 -V -f -l kali -P /usr/share/wordlists/wfuzz/others/common_pass.txt ssh://
[sudo] password for kali:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes
(this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-22 17:44:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, .
/hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 52 login tries (l:1/p:52), ~13 tries per task
[DATA] attacking ssh://www.target.com:22/
[ATTEMPT] target www.target.com - login "kali" - pass "" - 1 of 52 [child 0] (0/0)
[ATTEMPT] target www.target.com - login "kali" - pass "123456" - 2 of 52 [child 1] (0/0)
[ATTEMPT] target www.target.com - login "kali" - pass "1234567" - 3 of 52 [child 2] (0/0)
[ATTEMPT] target www.target.com - login "kali" - pass "12345678" - 4 of 52 [child 3] (0/0)
[ATTEMPT] target www.target.com - login "kali" - pass "123asdf" - 5 of 53 [child 0] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "Admin" - 6 of 53 [child 1] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "admin" - 7 of 53 [child 2] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "administrator" - 8 of 53 [child 3] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "asdf123" - 9 of 53 [child 0] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "backup" - 10 of 53 [child 1] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "backupexec" - 11 of 53 [child 0] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "changeme" - 12 of 53 [child 2] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "clustadm" - 13 of 53 [child 3] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "cluster" - 14 of 53 [child 1] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "compaq" - 15 of 53 [child 0] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "default" - 16 of 53 [child 2] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "dell" - 17 of 53 [child 3] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "dmz" - 18 of 53 [child 1] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "domino" - 19 of 53 [child 0] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "exchadm" - 20 of 53 [child 2] (0/1)
[ATTEMPT] target www.target.com - login "kali" - pass "exchange" - 21 of 53 [child 3] (0/1)
```

**RECOMMENDED  
REMEDATION #1****CRITICALITY: CRITICAL (31)****NO LIMIT FOR SSH SERVICE  
LOGIN ATTEMPTS****LOCATION: WEB SERVER  
SSH SERVICE**

We will need to set password attempt limits on SSH login. To do so, one would go to the file `/etc/ssh/sshd_config`. For us the line of interest is `"#MaxAuthTries"`. One would need to uncomment (remove the `#`) on this line, and enter the number of maxim authentication tries afterwards. For example, if 6 tries are allowed, then this line would become `"#MaxAuthTries 6"`. A restart of the SSH server is then required for the changes to take effect.

VULNERABILITY #2

CRITICALITY: **CRITICAL (26)**DEFAULT SERVICE PASSWORD  
POLICY (LENGTH, COMPLEXITY)LOCATION: WEB SERVER  
SSH SERVICE

The SSH service on the web server has a default password policy currently set. The minimum length and maximum length of the password have not been set, leading to a potential insecure password creation by users or admins. Not properly setting password length requirements can lead to brute force or dictionary attempts.

```
##### OBSOLETE BY PAM #####
#
# These options are now handled by PAM. Please
# edit the appropriate file in /etc/pam.d/ to
# enable the equivalent of them.
#
#####
#MOTD_FILE
#DIALUPS_CHECK_ENAB
#LASTLOG_ENAB
#MAIL_CHECK_ENAB
#OBSCURE_CHECKS_ENAB
#PORTTIME_CHECKS_ENAB
#SU_WHEEL_ONLY
#CRACKLIB_DICTPATH
#PASS_CHANGE_TRIES
#PASS_ALWAYS_WARN
#ENVIRON_FILE
#NOLOGINS_FILE
#ISSUE_FILE
#PASS_MIN_LEN
#PASS_MAX_LEN
#ULIMIT
#ENV_HZ
#CHFN_AUTH
#CHSH_AUTH
#FAIL_DELAY
```

Then on the file “/etc/pam.d/common-password”.

```
# here are the per-package modules (the "Primary" block)
password [success=1 default=ignore] pam_unix.so obscure sha512
# here's the fallback if no module succeeds
```

RECOMMENDED  
REMEDATION #2CRITICALITY: **CRITICAL (26)**DEFAULT SERVICE PASSWORD  
POLICY (LENGTH, COMPLEXITY)LOCATION: WEB SERVER  
SSH SERVICE

The parameters in the file “/etc/pam.d/common-password” must be added to the line highlighted in above screenshot to set stronger parameters. We recommend the following parameters: minlen=12 maxrepeat=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 reject\_username enforce\_for\_root



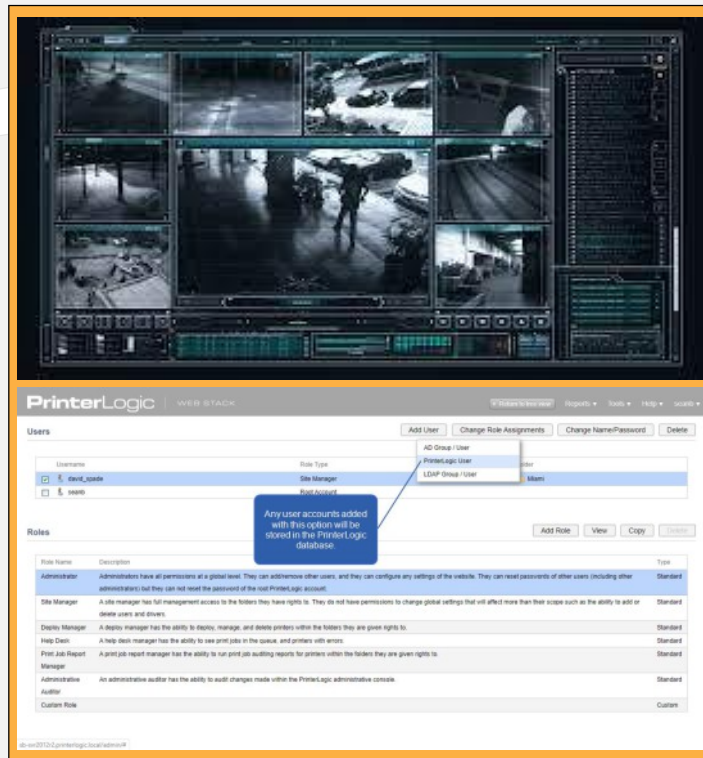
**VULNERABILITY #3**

**CRITICALITY: VERY HIGH (22)**

**WEAKLY CONFIGURED OR NON-EXISTENT ACCESS CONTROL**

**LOCATION: CAMERAS, PRINTER**

The Cameras and the printer have no access control. Anyone with access to the internal IPs will have complete and full access to the cameras and printer, this includes view rights and also configuration changes.



**RECOMMENDED REMEDIATION #3**

**CRITICALITY: VERY HIGH (22)**

**WEAKLY CONFIGURED OR NON-EXISTENT ACCESS CONTROL**

**LOCATION: CAMERAS, PRINTER**

Port 80 (HTTP) utilization for the graphical user interface should be removed, and instead replaced by port 443 (HTTPS) which will provide a secure and encrypted communication of data flow, including any inputted fields, including usernames and passwords.

**VULNERABILITY #4**

**CRITICALITY: HIGH (19)**

**NON-ENCRYPTED COMMUNICATION**

**LOCATION: SWITCHES, CAMERAS, PRINTER**

The switches on 10.1.1.3 and 10.1.1.4, as well as the Security Cameras on 10.1.15.10 to 10.1.15.20, and the printer on 10.1.1.10 are all utilizing port 80 for web graphical user interface communication. Utilizing port 80 for communication does not encrypt any data in transfer, hence all activity, including account names and passwords, will be sent in communication through cleartext and can be intercepted easily.

```

Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
> Content-Length: 38\r\n
Origin: http://10.0.2.15:8080\r\n
Connection: keep-alive\r\n
Referer: http://10.0.2.15:8080/[REDACTED]/login\r\n
> Cookie: JSESSIONID=zNM7fK4Qi_5_An9h5yeRsMcIW2x89RkGu5TvA-6p\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://10.0.2.15:8080/[REDACTED]/login]
[HTTP request 1/1]
[Response in frame: 60]
File Data: 38 bytes
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "username" = "johnturner"
  > Form item: "password" = "[REDACTED]"
    
```

**RECOMMENDED REMEDIATION #4**

**CRITICALITY: HIGH (19)**

**NON-ENCRYPTED COMMUNICATION**

**LOCATION: SWITCHES, CAMERAS, PRINTER**

Port 80 (HTTP) utilization for the web server should be removed, and instead replaced by port 443 (HTTPS) which will provide a secure and encrypted communication of data flow, including any inputted fields such as usernames and passwords.

VULNERABILITY #5

CRITICALITY: HIGH (18)

UNUSED OPEN PORTS

LOCATION: PORTS

Some insecure ports are open for internal and external communication such as Telnet - 23 and HTTP - 80, they must be closed or redirected to secure ports automatically. Also port 4000 is open with service running as “remote anything” which signifies it can accept almost any TCP connection which is a big security risk.

Also, it is recommended to filter the services running on these port to mask the services and not to use the defaults ports for example ssh service can be moved to port number 1222 instead of 22 to make a guess attack from an attacker harder.

```
(kali@kali)-[~]
└─$ nmap 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-27 15:08 CEST
Nmap scan report for 10.0.2.15
Host is up (0.00010s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
4000/tcp  open  remoteanything
8080/tcp  open  http-proxy
9001/tcp  open  tor-orport
```

RECOMMENDED  
REMEDIAION #5

CRITICALITY: HIGH (18)

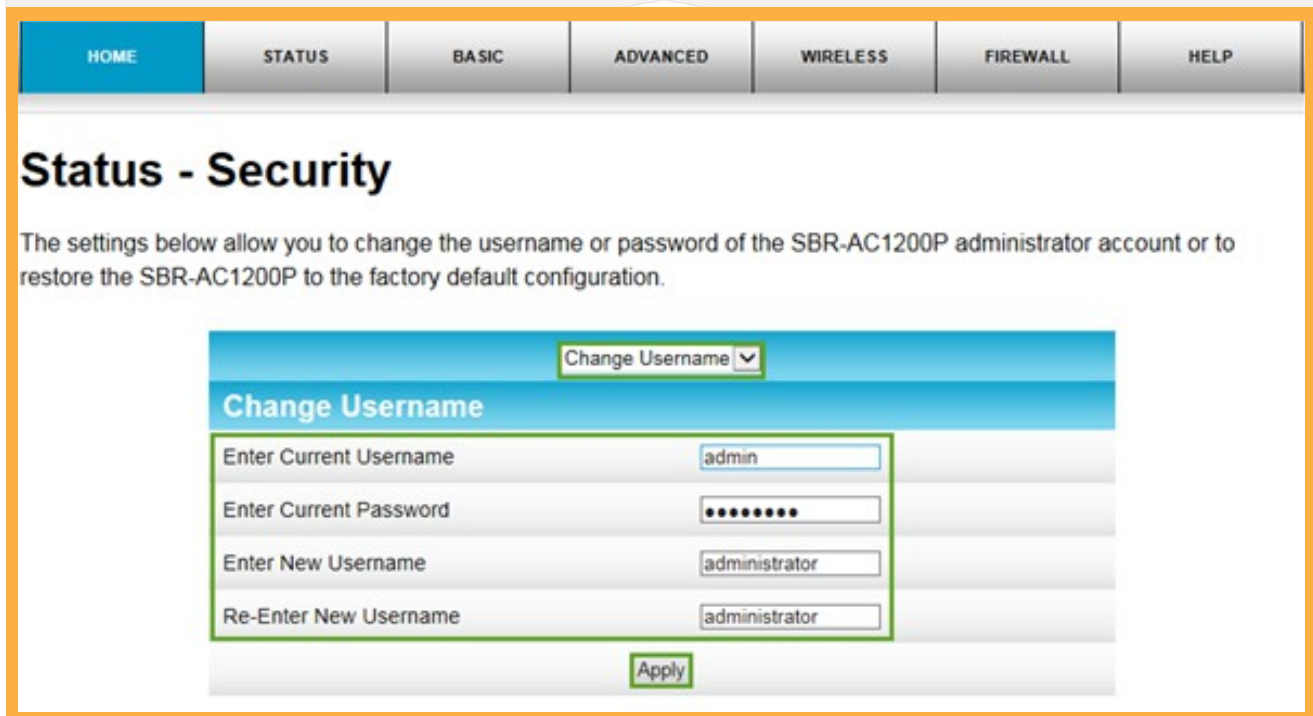
UNUSED OPEN PORTS

LOCATION: PORTS

This vulnerability is found upon scanning the installed packages on the system of which we were given SSH access to.

**VULNERABILITY #6****CRITICALITY: HIGH (16)****WEAK OR DEFAULT  
PASSWORDS****LOCATION: ACCESS SWITCHES**

The access switches at 10.1.1.3 and 10.1.1.4 have default login credentials still enabled (admin/admin). These need to be modified in order to not allow access and configuration changes to the switches.



The screenshot shows the 'Status - Security' page of the SBR-AC1200P web interface. The navigation menu includes HOME, STATUS, BASIC, ADVANCED, WIRELESS, FIREWALL, and HELP. The main heading is 'Status - Security'. Below the heading, a message states: 'The settings below allow you to change the username or password of the SBR-AC1200P administrator account or to restore the SBR-AC1200P to the factory default configuration.' The 'Change Username' form is highlighted with a green border. It includes a dropdown menu for 'Change Username', four input fields: 'Enter Current Username' (containing 'admin'), 'Enter Current Password' (masked with dots), 'Enter New Username' (containing 'administrator'), and 'Re-Enter New Username' (containing 'administrator'). An 'Apply' button is located at the bottom of the form.

**RECOMMENDED  
REMEDIAION #6****CRITICALITY: HIGH (16)****WEAK OR DEFAULT  
PASSWORDS****LOCATION: WEB SERVER  
SSH SERVICE**

Default credentials (admin/admin) should be deleted from the user base, and proper accounts should be created corresponding to the authorized users and administrators that will be configuring and maintaining the switches.

VULNERABILITY #7

CRITICALITY: HIGH (15)

PATCHABLE SYSTEMS

LOCATION: APACHE 2  
HTTP SERVER

Using a known vulnerable version of apache2 (HTTP server).

On our internal test we found the HTTP server is running apache2 version 2.4.46 which has known documented vulnerabilities.

```
(kali@kali)-[~]
└─$ apache2 -v
Server version: Apache/2.4.46 (Debian)
```

The description of the vulnerability, as stated in CVE-2019-17567 (<https://nvd.nist.gov/vuln/detail/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.”

To investigate further and to determine if this vulnerability affects us, we see that the vulnerable modules mod\_proxy and proxy\_wstunnel modules are in being used.

```
(kali@kali)-[~]
└─$ apache2ctl -M | grep proxy
AH00558: apache2: Could not reliably
y to suppress this message
proxy_module (shared)
proxy_wstunnel_module (shared)
```

RECOMMENDED  
REMEDATION #7

CRITICALITY: HIGH (15)

PATCHABLE SYSTEMS

LOCATION: APACHE 2  
HTTP SERVER

Upgrade server to a newer safer version.

**VULNERABILITY #8****CRITICALITY: Medium (13)****PATCHABLE SYSTEMS****LOCATION: SAMBA FILE SHARING SERVER**

DMZ : The samba server inside the DMZ is running a more ancient version with known, documented vulnerabilities.

On doing an internal pentest on servers running under DMZ we found a vulnerable version of samba server.

A know vulnerability with CVSS 3.x score of 7.5 can be found at <https://nvd.nist.gov/vuln/detail/CVE-2020-27840>

This vulnerability causes the server crash and affects the system availability which is crucial for a file sharing server under DMZ.

Which is affecting all versions from 4.0.0 upto 4.12.13 (excluding), 4.13.0 upto 4.16.3 (excluding) and 4.14.0 upto 4.14.1 (excluding). Our version being 4.12.5 falls under the vulnerable version and needs to be updated immediately.

```
(kali@kali)-[~]
└─$ samba --version
Version 4.12.5-Debian
```

**RECOMMENDED REMEDIATION #8****CRITICALITY: Medium (13)****PATCHABLE SYSTEMS****LOCATION: SAMBA FILE SHARING SERVER**

Upgrade server to a newer safer version.

**VULNERABILITY #9****CRITICALITY: Low (5)****UTILIZATION OF END  
OF LIFE SOFTWARE****LOCATION: PYTHON2**

Since python is no longer supporting (have reached its end of life) python2 no fixes or patches will be given in future even if vulnerabilities on the versions (previous to python 3.x) are discovered. Hence we recommend the use of python 3.x instead of current python 2.x to avoid the security issues which can occur in future.

```
(kali@kali)-[~]  
└─$ python --version  
Python 2.7.18
```

**RECOMMENDED  
REMEDiation #9****CRITICALITY: Low (5)****UTILIZATION OF END  
OF LIFE SOFTWARE****LOCATION: PYTHON2**

This vulnerability is found upon scanning the installed packages on the system of which we were given SSH access to.

## RECOMMENDATIONS FOR BEST PRACTICES:

### RECOMMENDATION [1] WIRELESS SECURITY (WPA2 VS WPA3)

CRITICALITY: **Low (5)**

The wireless system is currently utilizing WPA2, which is reasonably secure but still crackable. It is recommended to move to WPA3.

#### Properties

SSID:	██████████
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	<b>WPA2-Personal</b>
Network band:	5 GHz
Network channel:	149
Link speed (Receive/Transmit):	433/433 (Mbps)
IPv6 address:	2a04:cec0:11cd:b3b1:c4e8:3e80:746:19fd
Link-local IPv6 address:	fe80::c4e8:3e80:746:19fd%11
IPv4 address:	192.168.196.224
IPv4 DNS servers:	192.168.196.245
Manufacturer:	Intel Corporation
Description:	Killer(R) Wireless-AC 1550i Wireless Network Adapter (9560NGW) 160MHz
Driver version:	22.40.0.7
Physical address (MAC):	██████████



**RECOMMENDATION [2]  
THIRD PARTY REPOSITORY  
INSECURE UPGRADES****CRITICALITY: Low (9)**

Third party repositories found in main sources.list under “apt” directory. Use of third party repositories are recommended to use with caution as on every “apt-get update” and “apt-get upgrade” packages from these repositories can be installed on the system and can lead to security issues.

```
(kali@kali)-[~]
└─$ cat /etc/apt/sources.list
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-reposit
ories/
deb http://http.kali.org/kali kali-rolling main contrib non-free

# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free
deb https://[REDACTED]/linux ./
# deb-src https://[REDACTED].io/linux ./

deb http://mirrors.cloud.[REDACTED]/debian/ buster-backports main non-free c
ontrib

deb http://http.sft.[REDACTED] sft-win main non-free contrib
```

**RECOMMENDATION [3]  
USE OF INSECURE CRYPTOGRAPHIC  
ALGORITHM (MD5)****CRITICALITY: HIGH (19)**

Here we can see the passwords are getting encrypted in MD5, which have proven to be prone to brute force attack as well as MD5 algorithm has also proven issues within its cryptographic method such as collision. A collision is when two words have the same hash generated.

```
def checkPassword():
    for key in range(3):
        p = input("Enter the password >>")
        hashpass = hashlib.md5(p.encode('utf8')).hexdigest()

        if hashpass == encrypt:
```

## SECURITY MATRIX:

No.	Interface	Attack Path	Result
1.	SWITCH	Vul [1], leads to full switch administration control upon using a set of default username and passwords. However, an access to the switch is required.	Exploitable
2.	HTTP	The traffic between server and host is unencrypted as seen in Vul [1]. This risks the data to be captured and read without any difficulties by an attacker.	Exploitable
3.	CAMERA	Access control to camera devices is absent as seen in Vul [5], once an attacker gains an internal access can access the cameras.	Exploitable
4.	PRINTER	Access control to printers in LAN is absent as seen in Vul [5], once an attacker gains an internal access can access these printers log and other services..	Exploitable
5.	SSH	No limit of entering the wrong password can facilitate brute-force [8]. Attaching this with [9] and [10] which don't enforce a good password policy, can lead to a successful dictionary attack for SSH login.	Exploitable
6.	Crypt - Database	Use of MD5 is proven to be insecure to store sensitive information such as passwords. Passwords cannot be retrieved from the web interface, However Vulns[8],[9],[10] can lead to access to the hashed passwords and can be reversed.	Exploitable
7.	System update	Vuln [11] can lead to installation of non approved	Residual / Not

## KNOWN VULNERABILITIES / END OF LIFE:

No.	CVE No.	Affected Service	CVE - Details	CVSS Score	Result
1.	CVE-2018-12327	Apache 2.4.46	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.	5.3	Exploitable
2.	NIL	Python2	End of Life have been reached	NIL	NIL
3.	CVE-2020-27840	Samba 4.12.15	Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause invalid DN strings with spaces to instead write a zero-byte into out-of-bounds memory, resulting in a crash.	7.3	Exploitable
4.	CVE-2018-12327	NTP1:4.2.8P15	Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11 allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter.	9.8	Exploitable

**RECOMMENDATIONS :**

Recommendations	Description	Required immediate remediation
REC [1]: Wireless Security (WPA2 vs WPA3)	The wireless system is currently utilizing WPA2, which is reasonably secure but still crackable. It is recommended to move to WPA3.	NO
REC [2]: Potential insecure update	Use of unverified third party repositories in "sources.list" might harm the system on performing "update" and "upgrade".	YES
REC [3]: Use of insecure cryptographic algorithm	MD5 hash function is used to store the password without using salt. Highly prone for collision.	YES

**APPENDIX:**
**1. CRITICALITY RATING:**

Listed below are the vulnerability ratings for the first two vulnerabilities. This section has been redacted, please refer to the full report for criticality ratings for all the vulnerabilities found.

**1.A VULN [1]:**

Factor	Value	Points
Time	< = 1 week	15
Expertise	Competent	6
Knowledge required	Restricted information	7
Access to product by	Moderate	1
Type of equipment	Standard	2
<b>Total</b>	31	

**1.B VULN [2]:**

Factor	Value	Points
Time	< = 2 months	7
Expertise	Competent	6
Knowledge required	Restricted information	7
Access to product by	Easy	4
Type of equipment	Standard	2
<b>Total</b>	26	

## 2. CRITICALITY REFERENCE TABLE:

Factor	Value	
Time taken for the exploitation	<= 1 day	18
	<= 1 week	15
	<= 2 weeks	13
	<= 1 month	10
	<= 2 months	7
	<= 3 months	4
	<= 4 months	2
	<= 5 months	1
	>5 months	0
Attacker skills	Layman	8
	Competent	6
	Expert	3
	Multiple experts	0
Knowledge required by the attacker	None	11
	Restricted information	7
	Sensitive information	3
	Critical information	0

Factor	Value	
Access to the product by the attacker	Not necessary/unlimited	10
	Easy	4
	Moderate	1
	Difficult	0
	None	N.A.
Type of equipment needed	None/ standard	2
	Specialised software	0

### 3. TOOLS REFERENCED:

Tool	Version
Burp Suite professional	2021.4
Nmap	7.4p
Firefox browser	21
NetCat	1.10-46
Hydra	9.1

#### 4. ACRONYMS:

Acronyms	Full Form
SSH	Secure Shell
FTP	File Transfer Protocol
NTP	Network Time Protocol
HTTP	HyperText Transfer Protocol
HTTPS	Secure HTTP