Source

Source

Exploit a recent vulnerability and hack Webmin, a web-based system configuration tool.

[Task 1] Embark

Enumerate and root the box attached to this task.
Can you discover the source of the disruption and leverage it to take control?

This virtual machine is also included in the room AttackerKB as part of a guided experience. Additionally, you can download the OVA of Source for offline usage from https://www.darkstar7471.com/resources.html

#1
user.txt

THM{SUPPLY_CHAIN_COMPROMISE}

#2
root.txt

THM{UPDATE_YOUR_INSTALL}

writeup

IP Address: 10.10.204.179

-run nmap scan and enumerate services
-found Webmin running on port 10000
-visited site and got SSL error message so I set it for https
-fired up metasploit and used `exploit/linux/http/webmin_backdoor`
-setup correct options including setting SSL to true
-ran and got shell, switched to meterpreter using ctrl+z

-went to /home/dark directory and got user flag **THM{SUPPLY_CHAIN_COMPROMISE}**

-went to /root directory and got root flag **THM{UPDATE_YOUR_INSTALL}**

nmap-scan

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

10000/tcp open  http    MiniServ 1.890 (Webmin httpd)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=7/15%OT=22%CT=7%CU=31387%PV=Y%DS=4%DC=I%G=Y%TM=5F0F191
OS:E%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M508ST1
OS:1NW6%O6=M508ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN
OS:(R=Y%DF=Y%T=40%W=F507%O=M508NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```