***PE Red Team: Linux Privilege Escalation Arena (1ster)***

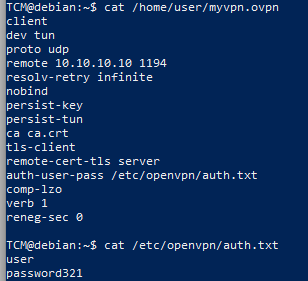
Task 1, 2, 3:

No answer needed

Task 4:

4.1

De gegeven commando’s in volgorde gebruikt om tot het resultaat te komen.



Task 5:

Het gegeven commando gebruikt om tot het resultaat te komen.

In het resultaat kan je zien dat er een poging is gedaan om verbinding te maken met “mysql” als

user (-u) “root” met paswoord (-p) “password123”

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Task 6:

Eerst hebben we de inhoud van /etc/passwd en /etc/shadow gekopieerd naar een bestandje.

cat /etc/passwd > PASSWORD-FILE en cat /etc/shadow > SHADOW-FILE



Daarna hebben we deze files via scp overgezet naar onze attacker machine.  
scp PASSWORDFILE student@ip-adres:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Om in de attacker machine het commando unshadow te kunnen gebruiken hebben we dit eerst moeten installeren met volgend commando: sudo apt install john

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Om de hashcat te kunnen gebruiken hebben we dit eerst moeten installeren via: sudo apt install hashcat

De rockyou.txt file hebben we gedownload in onze vm om zo het gegeven hashcat commando te kunnen uitvoeren.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

hashcat -m 1800 unshadowed.txt rockyou.txt -O

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Na het uitvoeren van de hashcat kregen we het paswoord te zien.

De /etc/shadow file had ook volgende permissies:

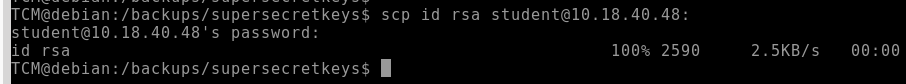


Task 7:

De gegeven commando’s uitgevoerd:



Deze zijn dan via scp naar de attacker machine gekopieerd.



Hier zie je ook het volledige pad waar de file gesaved is.

Task 8, 9, 10 en 11:

No answer needed, enkel de gegeven commando’s uitgevoerd in de vm.

Task 12:

De gegeven commando’s uitgevoerd en nginx gestart.

Als nginx gestart is kan je hier de cve exploit vinden

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Er werd gevraagd om in een 2de terminal volgende commando’s uit te voeren:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Na het uitvoeren van deze commando’s kregen we een nieuwe shell in onze eerste teminal (waar nginx gestart was). Hier kan je zien dat dit via de /usr/bin/sudo SUID binary gedaan word.

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Task 13:

Na het ingeven van de geven commando’s werd er gevraagd wat het laatste resultaat was van het commando “strings /usr/local/bin/suid-env”

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Task 14:

Na het ingeven van de geven commando’s werd er gevraagd wat het laatste resultaat was van het commando

“strings /urs/local/bin/suid-env2"

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Task 15, 16, 17, 18, 19:

No answer needed, enkel de gegeven commando’s uitgevoerd in de vm.

