

Appelli di MARCO PRANDINI

[DASHBOARD](#) / [I MIEI CORSI](#) / [APPELLI DI MARCO PRANDINI](#) / [SEZIONI](#) / [SICUREZZA INFORMATICA \(6CFU\)](#)

/ [SICUREZZA - PARTE II - ESERCIZI - 2024-06-13](#)

Sicurezza - Parte II - esercizi - 2024-06-13

SVOLGERE A SCELTA TRE DEI QUATTRO ESERCIZI descritti di seguito, caricando i file richiesti via EOL esattamente coi nomi specificati. Per semplicità gli screenshot sono indicati nel testo con estensione png, ma sono accettati anche con formato ed estensione jpg, mantenendo lo stesso nome di base.

È possibile ricaricare ogni file un numero illimitato di volte (ogni volta verrà proposto di sovrascrivere la versione precedente) entro il tempo limite assegnato.

Esercizio 1 - Privesc

Leggete tutto il testo prima di fare qualsiasi cosa!

Per questo esercizio è consigliabile usare una VM che non sia mai stata usata: se necessario createla come il primo giorno di laboratorio (e intanto fate gli altri esercizi)

Scaricare sulla VM Kali il file [change_2024_06_13](#) e renderlo eseguibile

\$ chmod +x ./change_2024_06_13

Il comando apporta modifiche a file dentro **/usr/bin** e **/etc**

Prima parte:

1. ideare un modo di identificare il file modificato e il tipo di modifica apportata.
2. lanciare **sudo ./change_2024_06_13**
3. attuare la strategia ideata al punto 1 per identificare il file modificato e il tipo di modifica apportata.

Seconda parte:

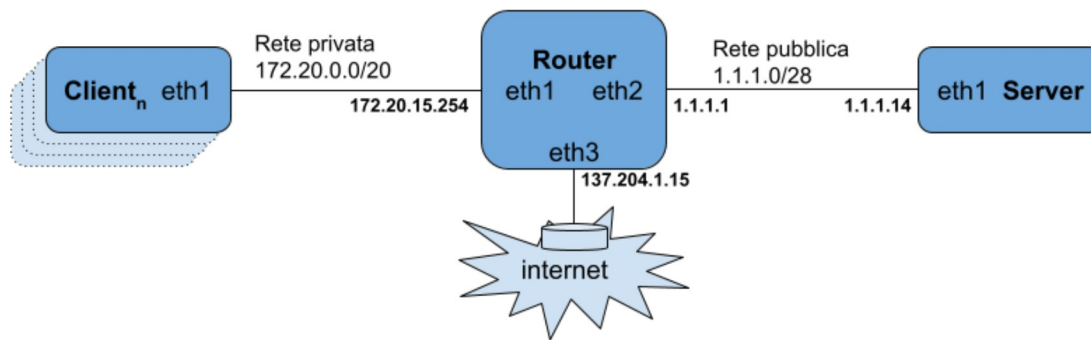
- usare senza sudo il/i file modificato/i dal comando `change_2024_06_13` per diventare root

Documentate tutti i passi svolti in modo dettagliato nel file **integrity.txt**

Catturate le schermate che mostrano il successo nel diventare root senza usare sudo in uno screenshot **privesc.png**

Consegnate i due file.

Esercizio 2 - iptables



Le interazioni consentite nella rete raffigurata devono essere unicamente:

- accesso da parte dei client alla porta TCP 993 del server
- accesso da parte di qualsiasi host su internet alla porta TCP 25 del server
- navigazione sicura dei client sul web (internet, porta TCP 443)
- accesso da parte dei client alla porta UDP 53 del router

Consegnate un file **ipt-router.sh** coi comandi che permettano di configurare il packet filter del router e un file **ipt-server.sh** coi comandi che permettano di configurare il packet filter del server.

Esercizio 3 - pwn

Unzippare il [file](#) con l'eseguibile compilato e dargli i permessi di esecuzione se necessario

```
unzip secret_func1.zip
chmod +x ./secret_func1
```

L'obiettivo è sfruttare il buffer overflow ed eseguire la funzione che contiene il flag corretto.

Ricordate di disabilitare l'ASLR per far sì che l'esercizio riesca; **da root** lanciare

```
echo 0 > /proc/sys/kernel/randomize_va_space
```

Consegnare 3 file

- Un file **bof.txt** contenente:
 - Il payload finale con il quale viene lanciato l'eseguibile
 - Una descrizione il più possibile dettagliata dei passaggi eseguiti per ricavare l'overflow che permette di sovrascrivere l'indirizzo di ritorno. Questa descrizione può includere tutti i tentativi che sono stati fatti oppure soltanto il meccanismo che è stato eseguito. Il livello di dettaglio e precisione della descrizione sarà utilizzato come valutazione della prova.
- Uno screenshot **payload.png** che mostra il payload che esegue l'overflow che dimostra che siate in grado di controllare l'indirizzo di ritorno, es. AAAA..AA+BBBB
- Uno screenshot **exploit.png** che mostra il payload eseguito e la relativa funzione stampata

Esercizio 4 - web

Scaricare i file [xaa](#) e [xab](#) e importare il file nelle immagini docker della VM con

```
$ cat xaa xab | gzip -dc | sudo docker load
```

Lanciare un docker container con l'immagine caricata

```
$ sudo docker run -it web_exams_sec bash
```

Ci si troverà a disposizione una shell all'interno del container, a questo punto lanciare:

service mysql start

Per lanciare il database

service apache2 start

Per lanciare il web server

A questo punto ci si puo' collegare dal browser all'indirizzo ip del container che e' possibile recuperare lanciando sempre nel container il comando

ip a

Collegarsi col browser in http all'indirizzo ip ritrovato e.g. http://INDIRIZZO_IP_TROVATO

CHALLENGE

La challenge e' una Cross Site Scripting, l'obiettivo è sfruttare la vulnerabilità XSS ed eseguire un alert o prompt Javascript.

Non è possibile utilizzare tool di scansione automatica e non è consentito alcun tipo di "bruteforce".








Seguire il link presente sul sito per eseguire correttamente l'input.

File da consegnare:

- Uno screenshot **payload.png** che mostra l'esecuzione del payload e relativo alert
- Un file **web.txt** che descriva i passi eseguiti che hanno portato a scoprire la vulnerabilità e una breve descrizione di come, ponendovi dal punto di vista del sys admin mitighereste e/o risolvereste questa vulnerabilità. Il livello di dettaglio e precisione della descrizione sarà utilizzato come valutazione della prova.

Stato consegna

Numero tentativo	Tentativo 1.
Stato consegna	Consegnato per la valutazione
Stato valutazione	Non valutata
Termine consegne	Thursday, 13 June 2024, 12:00
Tempo rimasto	Il compito è stato consegnato 4 min. in ritardo
Ultima modifica	Thursday, 13 June 2024, 12:04

Consegna file	 bof.txt	13 June 2024, 12:03
	 exploit.png	13 June 2024, 11:57
	 integrity.txt	13 June 2024, 12:03
	 ipt-router.sh	13 June 2024, 12:03
	 ipt-server.sh	13 June 2024, 12:03
	 payload.png	13 June 2024, 11:57
	 privesc.png	13 June 2024, 11:57