Appelli di MARCO PRANDINI

Sicurezza - Parte II - esercizi - 2023-07-27

Svolgere i tre esercizi descritti di seguito, caricando i file richiesti via EOL esattamente coi nomi specificati.

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 - Web

Collegarsi all'indirizzo 137.204.57.183:8082

Obbiettivo dello studente 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 le istruzioni presenti sul sito per eseguire correttamente l'input.

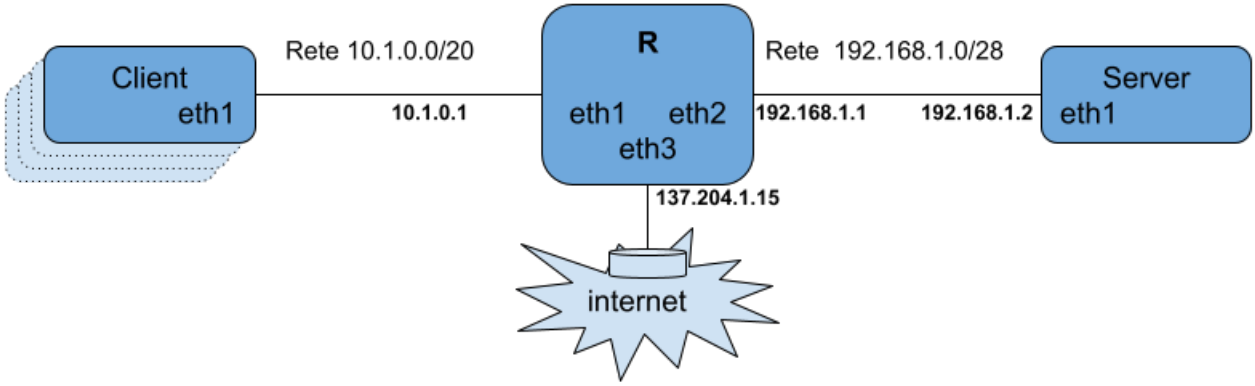
MODALITÀ DI CONSEGNA:

Lo studente dovrà consegnare:

- Un file **payload.(png|jpg)** che mostri l'esecuzione del payload e relativo alert
- Un file **web.txt** che descriva:
  - I passi eseguiti che hanno portato a scoprire la vulnerabilità
  - Un piccola descrizione di come, ponendosi dal punto di vista dell'amministratore del sistema vittima, mitighereste o risolvereste questa vulnerabilità.

Il livello di dettaglio e precisione della descrizione sarà considerato ai fini della valutazione della prova.

Esercizio 2 - Firewall



Facendo riferimento allo schema di rete sopra riportato, si definiscano regole di filtraggio il più possibile specifiche che consentano il traffico come sotto specificato; qualsiasi altro pacchetto deve essere scartato. **NOTA**: le regole devono essere installate su **ogni host** coinvolto nel flusso di traffico specificato.

So noti che i client e il server sono su subnet RFC1918.

1. i Client devono poter accedere via HTTPS (porta TCP 443) a qualunque host di internet;
2. da Internet si deve poter contattare il servizio SMTP (TCP/25) del Server
3. i Client della subnet 10.1.1.0/24 devono poter accedere via SSH al server

MODALITÀ DI CONSEGNA:

Lo studente dovrà consegnare 1 file **iptables.txt** contenente quattro sezioni chiaramente contrassegnate, una per ogni host su cui è richiesto di installare le regole necessarie, nelle quali elencare i comandi (sintatticamente corretti) che le realizzano.

Esercizio 3 - Intrusion detection

L'esercitazione consiste nel creare una serie di regole per l'IDS visto a lezione, Suricata.

Se non funziona sudo apt install suricata:

- **scaricate questo file**
- **installate il pacchetto con**
- **sudo apt install PATH_COMPLETO_DEL_FILE_SCARICATO**

Le regole saranno testate per verificarne la correttezza.

Le regole includono semplici regole di base più alcune da applicare ad un file di un tracciato di traffico.

ESERCIZI

0) Spiegare che differenza c'è tra Suricata in modalità IPS e suricata in modalità IDS. Evidenziare in particolare in quale modalità è stato da noi utilizzato, evidenziandone pregi e svantaggi.

1) Scrivere una regola suricata in modalità alert per il traffico icmp SOLTANTO IN ENTRATA sulla rete 192.168.56.X

Hint. (Se pensate sia necessario cambiare la configurazione di suricata è bene specificarlo inserendo le righe da modificare)

2) Scrivere una regola suricata in modalità alert per qualsiasi richiesta che viene eseguita accedendo al portale virtuale.unibo.it.

Ogni dominio che fa richiesta ad un JS o Font VA CONSIDERATA.

Nota bene NON è possibile utilizzare il protocollo http o la porta 80 per creare questa regola.

3) Ricavare dal file del tracciato in allegato le seguenti informazioni

- Protocollo del traffico (non è SSH)

- I 2 Indirizzi Ip in gioco (considerate che ovviamente il traffico è in due direzioni)
- La/Le porte del protocollo in gioco

Hint: Avete un tool valido per recuperare queste informazioni

Successivamente lo studente deve scrivere una(o più di una se necessario) regola suricata in modalità alert per il traffico del protocollo in questione, specificandone gli IP trovati precedentemente.

Se creata correttamente la regola e configurato correttamente suricata (si ricordi l'esercitazione in classe su MQTT) nei log dovrebbe essere possibile leggere il contenuto del tracciato di traffico.

Parsare a piacimento il contenuto e ricomporre la flag.

Hint. La flag di solito è una frase di senso compiuto

MODALITÀ DI CONSEGNA:

Devono essere consegnati

- Un file **report.txt** dove si relazionino DETTAGLIATAMENTE tutte le osservazioni fatte nelle diverse fasi e la flag trovata
- Un file **suricata.yml** con la configurazione di suricata
- Un file **seclab.rules** con le regole create e utilizzate
- Un file **screenshot.***{png|jpg}* che mostri l'output del parsing con la relativa flag.

Stato consegna

Numero tentativo	Tentativo 1.
Stato consegna	Consegnato per la valutazione
	Il compito non accetta consegne
Stato valutazione	Non valutata
Termine consegne	Thursday, 27 July 2023, 12:00
Tempo rimasto	Il compito è stato consegnato 4 min. 45 secondi in anticipo
Ultima modifica	Thursday, 27 July 2023, 11:55
Consegna file	✚ 7 file

Commenti alle consegne	Commenti (0)

◄ Sicurezza Parte I - teoria - 2023-07-27

Vai a...