Cyber Security Report

W14D1

08/10/2025

Autore :
Pace Massimiliano
email : *efmpas@gmail.com*

Indice :

INTRODUZIONE

° Nell'esercitazione odierna ci viene chiesto di recuperare le password di DVWA e di eseguire un crack degli Hash trovati con o Hashcat o John the ripper.

SPIEGAZIONE ESERCIZIO

° Step 1: Avvio delle VM Kali e Metasploit

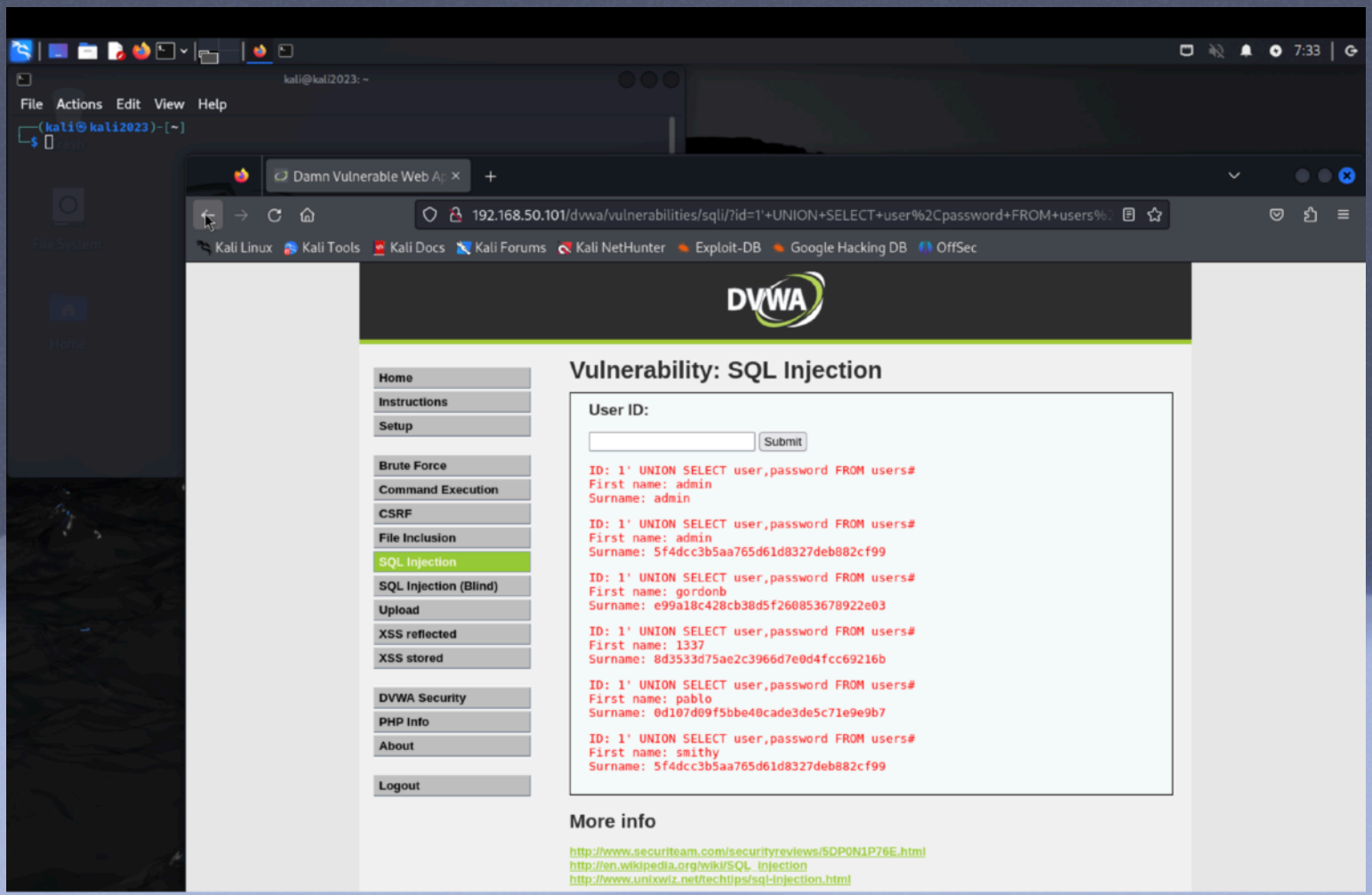
° Step 2 : Una volta avviate le 2 VM tramite Kali avviamo il terminale

° Step 3: Colleghiamoci alla Dvwa tramite ip 192.168.50.101 settiamo la low security e procediamo ad estrarre le password richieste

° Step 4 : Conosciamo già' determinati parametri scoperti nell'esercizio precedente, quindi andremo a prelevare direttamente cio' che ci interessa tramite il comando Union.

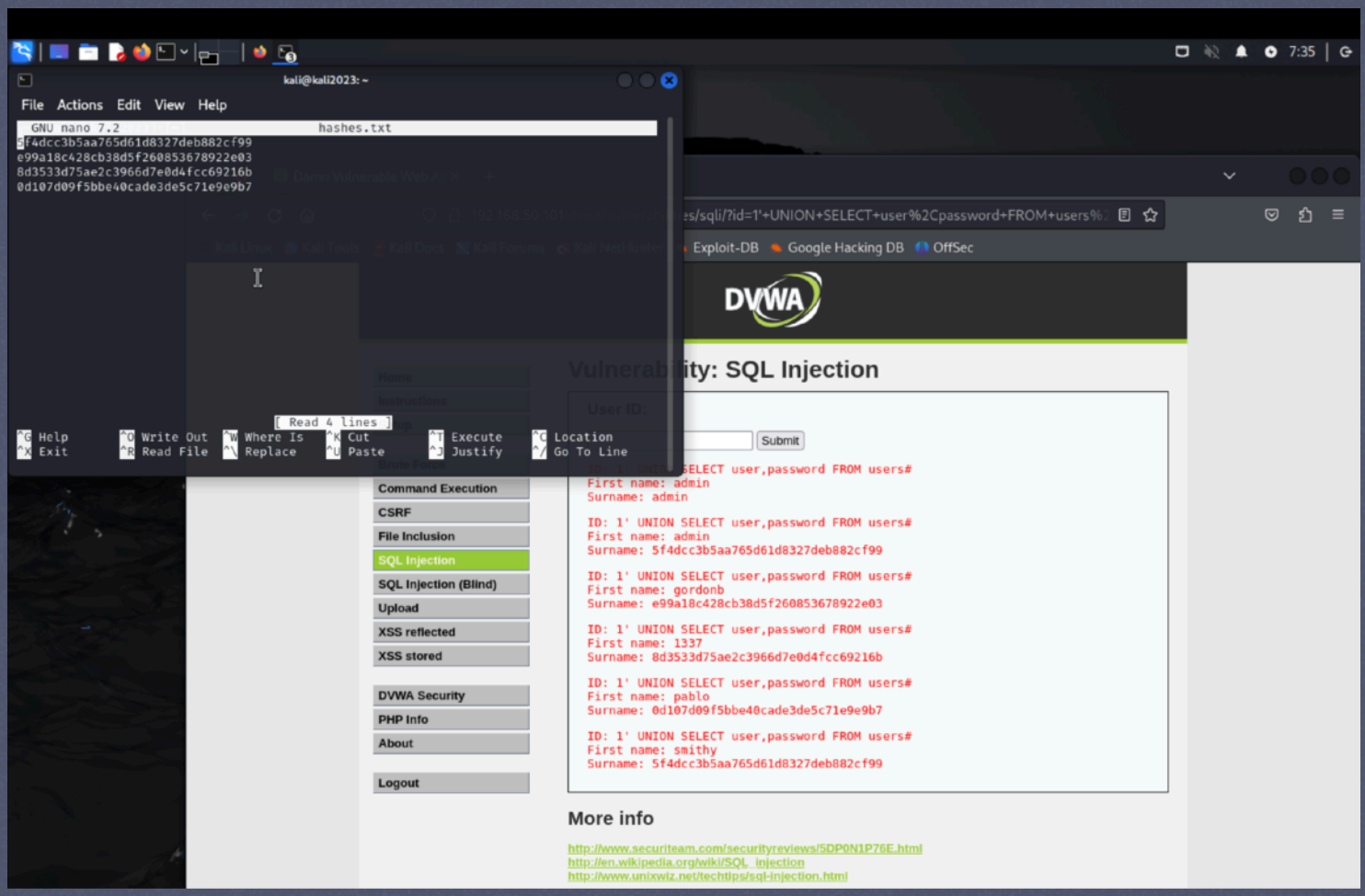
Codice usato :

1' UNION SELECT user, password FROM users#



° Step 5 : Abbiamo estratto le nostre password da DVWA. Noteremo subito che le password sono illeggibili, per rendere comprensibili e visibili i nostri Hash utilizzeremo (nel mio caso) HASHCAT.
Hashcat è uno strumento potentissimo per craccare gli hash, ossia per recuperare le password a partire dal loro hash. Funziona sfruttando la potenza della CPU o della GPU ed è molto usato per fare attacchi a forza bruta o basati su dizionario.

° Step 6 : Per realizzare un Crack dei nostri Hash dovremo prima creare un txt contenente gli hash da noi scovati.



° Step 7 : Una volta creato il file hashes.txt su terminale Kali useremo il codice :

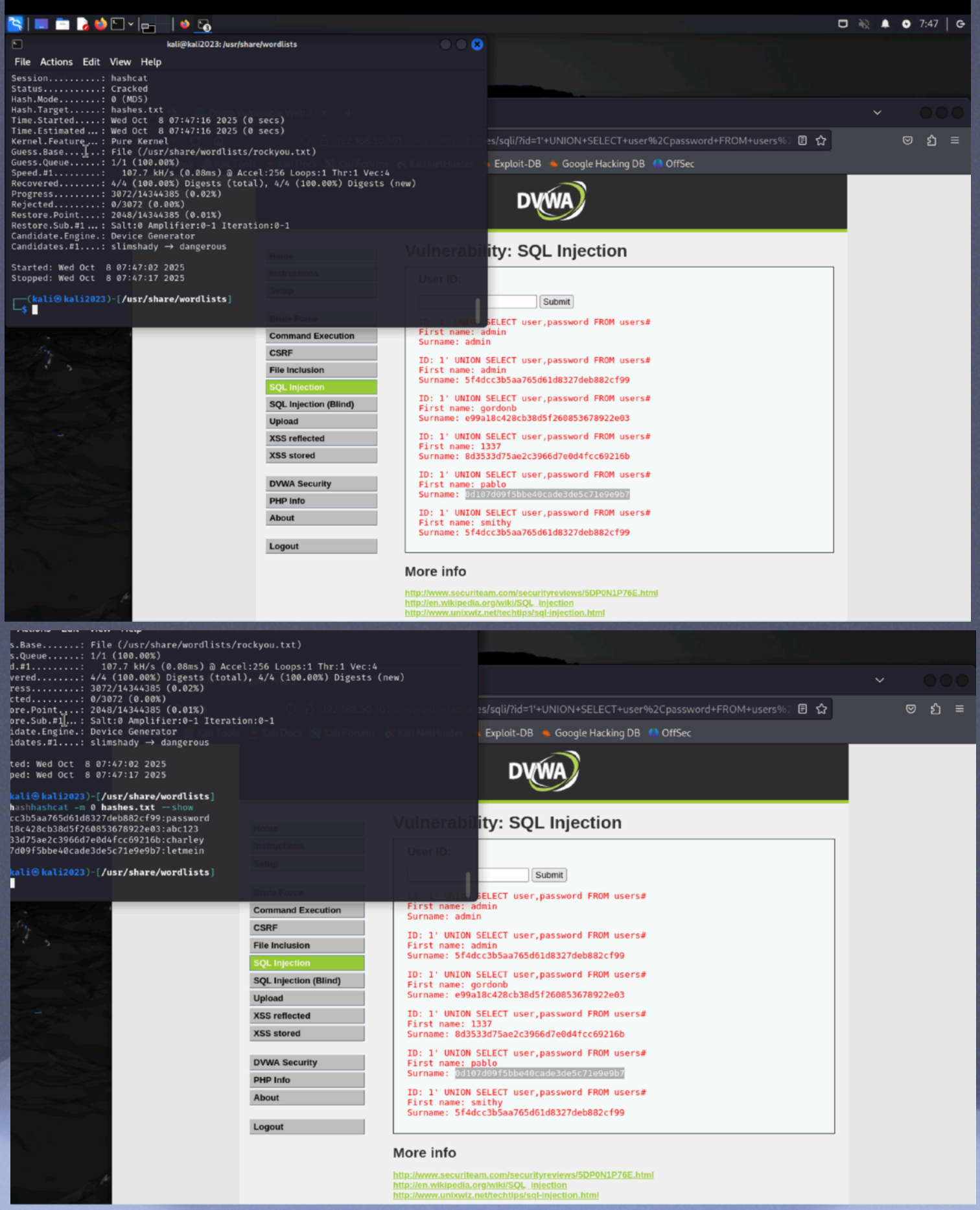
hashcat -m 0 -a 0 hashes.txt /usr/share/wordlists/rockyou.txt

per iniziare la fase di CRACK.

Nell' utilizzare hashcat il terminale restituiva un errore. Il file rockyou era compresso e non veniva riconosciuto. Per dezipparlo ho utilizzato :

sudo gzip -d rockyou.txt.gz

Una volta fatto partire hashcat ci verra' restituito il nostro risultato



° Step 8 : Per visulizzare il risultato delle password visibili utilizzeremo il codice

hashcat -m 0 ~/hashes.txt --show

CONCLUSIONI

° NB. L'esercizio e' stato ripetuto utilizzando John the ripper.

Risultati dell'Analisi

L'esercizio ha dimostrato con successo la vulnerabilità critica presente nell'applicazione DVWA al livello di sicurezza Low, dove è stato possibile estrarre completamente il database delle credenziali utente attraverso una semplice UNION-based SQL injection.

Vulnerabilità Identificate

La query SQL non sanitizzata ha permesso l'iniezione del payload `' UNION SELECT user,password FROM users#`, rivelando tutti gli username e i rispettivi hash MD5 delle password memorizzate nel database. Questa vulnerabilità rappresenta un rischio critico in quanto consente l'accesso non autorizzato a credenziali sensibili.

Problematiche Tecniche Riscontrate

Durante l'esercizio e' emerso un problema:
File rockyou.txt compresso: La necessità di decomprimere `rockyou.txt.gz` prima dell'utilizzo

ESERCIZIO W14D1 FACOLTATIVO

Esercizio Traccia

Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows infettato dal malware WannaCry. Cosa fai per mettere in sicurezza il tuo sistema?

NB. LA PROVA E' STATA EFFETTUATA SU UNA VM WINDOWS PRECEDENTEMENTE INSTALLATA. NEL MIO CASO PER METTERE IN SICUREZZA IL SISTEMA E' BASTATO ELIMINARE LA VIRTUAL MACHINE.

SEGUE UNA GUIDA DETTAGLIATA SU COSA FARE IN CASO DI INCONTRO REALE CON WANNACRY BASATA SU RICERCHE CONDOTTE CON AI E INTERNET.

Intervento Immediato (Fase di Contenimento)

Isolare immediatamente il sistema infetto disconnettendolo fisicamente dalla rete. Scollegare il cavo ethernet, disabilitare il WiFi e spegnere tutti i dispositivi di rete per prevenire la propagazione del ransomware agli altri computer. Questa è l'azione più critica da eseguire nei primi minuti dall'identificazione dell'infezione.

Disconnettere tutti i dispositivi esterni come unità USB, hard disk esterni, backup su cloud e network drive. WannaCry può diffondersi attraverso dispositivi connessi e criptare anche i file di backup accessibili. Isolare completamente il sistema infetto da qualsiasi altra risorsa di rete o storage.

Identificare il tipo di ransomware verificando che si tratti effettivamente di WannaCry attraverso la nota di riscatto visualizzata, i file criptati con estensioni modificate e il comportamento del sistema. Questa conferma è fondamentale per applicare la strategia di remediation corretta e per segnalare l'attacco alle autorità competenti.

Valutazione dell'Infezione

Validare l'estensione dell'infezione utilizzando strumenti antivirus, sistemi IPS (Intrusion Prevention System) e SIEM per confermare la presenza del malware e identificare eventuali altri sistemi compromessi nella rete. Analizzare i log di rete per tracciare la diffusione del worm attraverso le porte SMB (TCP 139, 445 e UDP 137, 138).

Reimpostare tutte le credenziali compromesse cambiando immediatamente le password di tutti gli account che potrebbero essere stati esposti. Implementare l'autenticazione a più fattori (MFA) su tutti gli account per prevenire accessi non autorizzati che potrebbero facilitare ulteriori infezioni.

Eradicazione del Malware

Rimuovere WannaCry utilizzando strumenti specializzati come Sophos Virus Removal Tool o altri software antimalware aggiornati per eliminare il payload del ransomware e tutti gli artefatti associati dal sistema infetto. È fondamentale rimuovere anche eventuali backdoor come DOUBLEPULSAR che WannaCry potrebbe aver installato.

Applicare la patch di sicurezza MS17-010 rilasciata da Microsoft per correggere la vulnerabilità EternalBlue sfruttata da WannaCry. Questa patch è disponibile anche per sistemi legacy come Windows XP e Windows Server 2003. L'installazione della patch previene reinfezioni attraverso lo stesso vettore di attacco. Considerare la formattazione completa del sistema come approccio più sicuro. Cancellare completamente il disco rigido e reinstallare il sistema operativo garantisce l'eliminazione totale del malware e di eventuali componenti residui.

Ripristino del Sistema

Ripristinare i dati da backup puliti utilizzando copie di backup verificate come non infette e precedenti all'attacco. Durante il ripristino, mantenere i backup disconnessi dalla rete per evitare reinfezioni. Testare l'integrità dei backup prima del ripristino completo.
Bloccare le porte SMB sul firewall per limitare la propagazione del worm. Configurare il firewall perimetrale per bloccare le porte TCP 139 e 445 e le porte UDP 137 e 138, sia in ingresso che in uscita. Implementare anche segmentazione di rete interna per isolare diverse VLAN e limitare l'ambito di eventuali attacchi futuri.

Documentare l'incidente preparando un report dettagliato che includa timeline dell'attacco, sistemi compromessi, vettori di infezione identificati, azioni di remediation intraprese e costi associati. Questa documentazione è essenziale sia per finalità assicurative che per migliorare la postura di sicurezza futura. [exabeam]

Analisi Pro e Contro delle Opzioni

Pagare il riscatto - Non è raccomandato in quanto solo 1 su 5 vittime che pagano ottiene effettivamente la chiave di decriptazione, e il pagamento incentiva ulteriori campagne criminali. Il totale raccolto dagli attaccanti di WannaCry fu di soli $130,634 da 327 pagamenti, suggerendo che la maggior parte delle vittime non ha pagato.

Ripristino da backup vs formattazione completa - Il ripristino da backup è più veloce ma richiede la certezza assoluta che i backup siano puliti. La formattazione completa richiede più tempo ma garantisce l'eliminazione totale del malware e rappresenta l'approccio più sicuro.

Isolamento fisico vs isolamento logico - La disconnessione fisica della rete è immediata e garantita, mentre l'isolamento tramite VLAN o firewall rules richiede configurazione ma permette di mantenere alcune funzionalità di monitoraggio.

ESERCIZIO EXTRA

°Simulazione attacco DOS con Slowloris

Slowloris è uno strumento per attacchi DoS/DDoS che permette a una singola macchina di mandare in blocco un server web utilizzando una larghezza di banda minima. Sviluppato nel 2009 da Robert Hansen (RSnake), prende il nome dal Lori Lento, un mammifero che si muove molto lentamente, riflettendo la natura metodica e lenta di questo attacco.
A differenza degli attacchi DDoS tradizionali che sovraccaricano il server con enormi quantità di traffico, Slowloris opera a livello applicativo (livello 7 del modello OSI) utilizzando richieste HTTP parziali e incomplete. L'attacco richiede solo poche centinaia di richieste eseguite a intervalli lunghi e regolari, anziché decine di migliaia di richieste continuative.

FASE 1 : installazione SLOWLORIS

git clone https://github.com/gkbrk/slowloris.git

FASE 2 : avvio Slowloris contro metasploit

slowloris 192.168.50.101

FASE 3 : personalizzazione attacco

slowloris <ip-metasploitable> -p 80 -s 200 -v

FASE 4: Monitoraggio con tcping

Conclusioni e Riflessioni

Purtroppo pur avendo provato vari metodi compreso hping3 non sono riuscito a monitorare e confermare l'esecuzione positiva dell'esercizio. Dopo aver installato tcping viene visualizzato un errore. Non viene rilevata la dipendenza bc (Basic Calculator) dipendenza necessaria per far funzionare lo script. Pur dandomi l'impressione che bc fosse installato tcping non e' riuscito a girare. Nel momento in cui sto scrivendo il Report mi sono reso conto che l'ultima prova che avrei potuto eseguire non e' stata fatta. (il riavvio della Kali). In alternativa avrei potuto usare Watch:

watch -n 1 'netstat -an | grep :80 | wc -l'

watch -n 1 'netstat -an | grep :80'

Queste prove verranno eseguite in seguito per colmare il senso di amarezza che mi pervade al momento. :)