Analisi di Sicurezza: Rilevamento e Mitigazione di un Attacco di Rete

Benvenuti a questa presentazione sull'analisi di un possibile attacco di rete rilevato tramite Wireshark. Esamineremo gli Indicatori di Compromissione (IOC), i potenziali vettori di attacco e le azioni consigliate per mitigare l'incidente attuale e prevenire attacchi futuri.

La nostra analisi ha rivelato un'attività sospetta caratterizzata da scansioni di porte, tentativi di sfruttamento di vulnerabilità note e potenziali manipolazioni del traffico di rete. Seguiremo un approccio metodico per comprendere la natura dell'attacco e formulare una risposta efficace.

Panoramica dell'Incidente

Attività Sospetta Rilevata

Attacco in corso sulla rete locale con scansioni di porte e tentativi di sfruttamento di vulnerabilità note

Obiettivo dell'Attacco

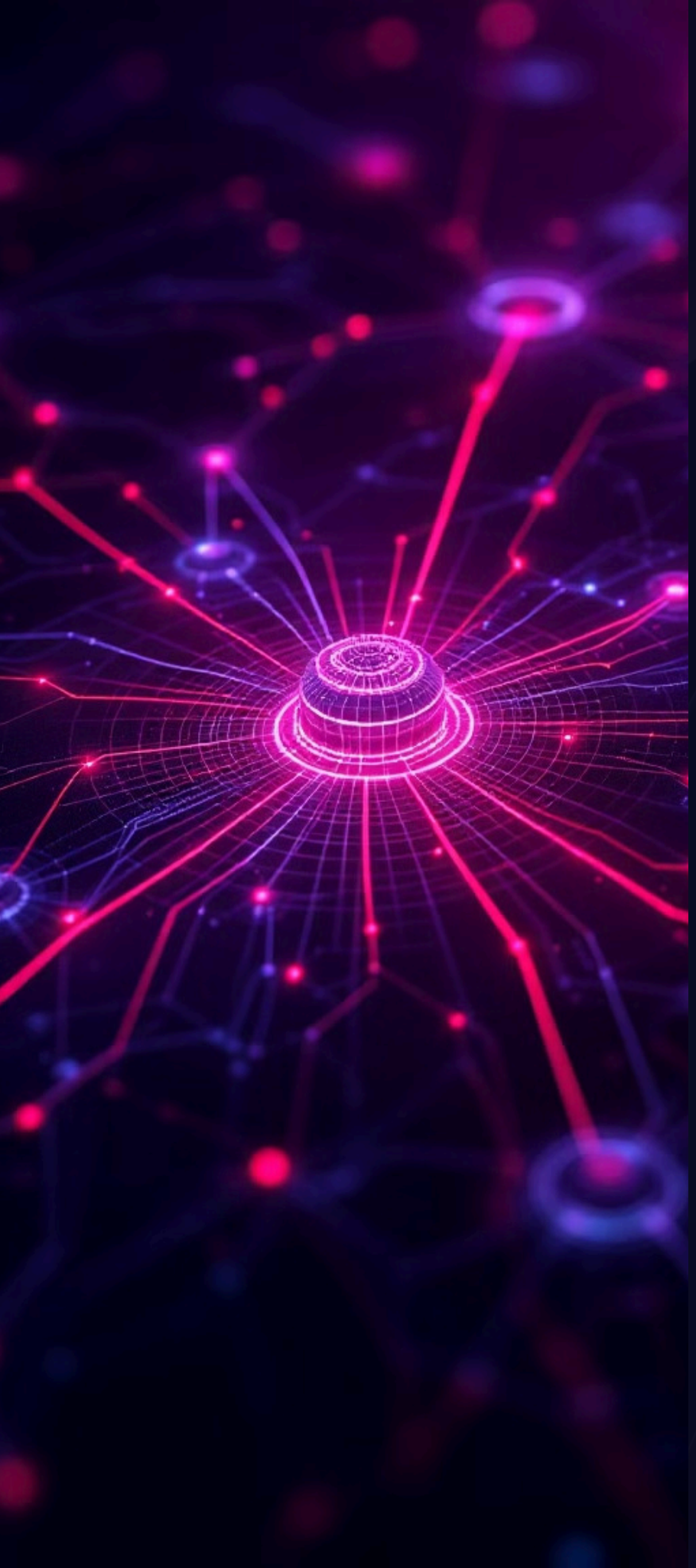
Ottenere accesso non autorizzato ai sistemi e ai dati sensibili presenti sulla rete

Pattern di Traffico

Tentativi di connessione TCP (SYN) da 192.168.200.100 verso 192.168.200.150 su multiple porte

Target Identificato

La macchina target sembra essere METASPLOITABLE, un tool usato per penetration testing



Indicatori di Compromissione (IOC)

Indirizzo IP Sospetto

192.168.200.100 identificato come origine dell'attività malevola sulla rete

Scansione di Porte

Numerosi tentativi di connessione SYN verso varie porte, indicativi di una fase di ricognizione

Porte Sensibili Prese di Mira

Tentativi di connessione a porte 445 (SMB), 139 (NetBIOS), 3306 (MySQL), 80 (HTTP), 443 (HTTPS) e altre

Connessioni Riuscite

Accesso ottenuto alle porte 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514

Altri indicatori includono traffico TCP anomalo con pacchetti RST e ACK, richieste ARP sospette e stringhe rilevanti come "METASPLOITABLE", "BROWSER" e "Xenix Server NT workstation NT Server Potential".

Vettori di Attacco Identificati

Scansione di Porte

Mappatura sistematica della rete per identificare servizi vulnerabili

Sfruttamento Vulnerabilità

Tentativi di compromettere servizi come SMB, NetBIOS, MySQL

Accesso Non Autorizzato

Obiettivo finale di ottenere controllo sui sistemi target

Evasione Difese

Possibili tecniche per aggirare i sistemi di sicurezza esistenti

L'attaccante sta seguendo un approccio metodico, iniziando con la ricognizione per identificare i punti deboli della rete, per poi tentare di sfruttare le vulnerabilità note nei servizi esposti. Questo pattern è tipico degli attacchi mirati che cercano di stabilire un punto d'appoggio persistente all'interno dell'infrastruttura.

Azioni Immediate di Contenimento

Isolamento dell'Host Compromesso

Disconnettere immediatamente 192.168.200.100 dalla rete per contenere l'attacco

Analisi dei Log

Esaminare i log di sistema, applicazioni e firewall di tutti gli host coinvolti

Scansioni Antimalware

Eseguire scansioni approfondite su tutti i sistemi potenzialmente compromessi

Aggiornamenti di Sicurezza

Applicare immediatamente le patch più recenti a sistemi operativi e applicazioni

Strategie di Mitigazione a Medio Termine

Rafforzamento della Sicurezza

Potenziare la protezione di tutti i servizi e chiudere quelli non indispensabili

Monitoraggio della Rete

Implementare sistemi di sorveglianza continua per rilevare attività sospette

Analisi Forense

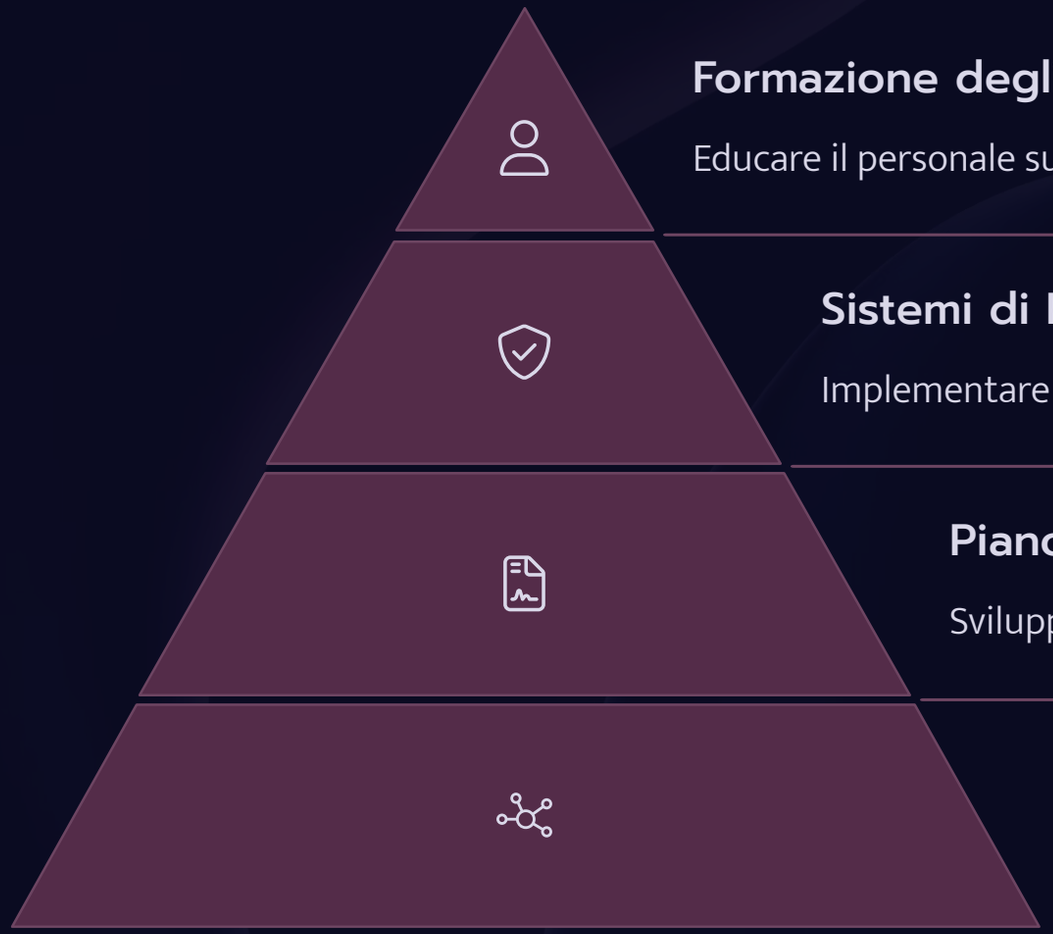
Condurre un'indagine approfondita sull'host compromesso

Cambio Password

Modificare tutte le credenziali di account utente e di servizio

Queste misure aiuteranno a ripristinare la sicurezza dell'ambiente e a raccogliere informazioni cruciali sull'attacco. L'analisi forense in particolare è fondamentale per comprendere l'estensione della compromissione e identificare eventuali backdoor o persistenze lasciate dall'attaccante.

Prevenzione di Attacchi Futuri



Formazione degli Utenti

Educare il personale sulla sicurezza informatica

Sistemi di Protezione Avanzati

Implementare IDS/IPS per rilevare comportamenti sospetti

Piano di Risposta agli Incidenti

Sviluppare procedure formali per gestire le violazioni

Monitoraggio Continuo

Adottare sistemi SIEM per la correlazione dei log

Una strategia di difesa efficace richiede un approccio stratificato che combini tecnologia, processi e persone. Il monitoraggio continuo permette di identificare rapidamente le minacce, mentre la formazione degli utenti riduce il rischio di errori umani che potrebbero compromettere la sicurezza.

Conclusioni e Raccomandazioni Finali

1

Isolamento Immediato

L'isolamento dell'host 192.168.200.100 è fondamentale per contenere il danno potenziale

2

Analisi Approfondita

Necessaria per identificare la causa principale e prevenire futuri incidenti

3

Difesa Stratificata

Implementare multiple linee di difesa per proteggere l'infrastruttura

4

Risposta Rapida

Sviluppare capacità di risposta tempestiva agli incidenti di sicurezza

L'incidente analizzato evidenzia l'importanza di un approccio proattivo alla sicurezza informatica. Combinando misure tecniche, formazione del personale e procedure di risposta agli incidenti ben definite, è possibile ridurre significativamente il rischio di compromissione e minimizzare l'impatto di eventuali violazioni.