Task 27/01/25: Remediation e Mitigazione

Traccia 1

Obiettivo dell'Esercizio:

Immagina di essere un amministratore di sicurezza per una media azienda che ha scoperto una campagna di phishing mirata contro i propri dipendenti. Gli attaccanti inviano email fraudolente che sembrano provenire da fonti affidabili, inducendo i dipendenti a divulgare informazioni sensibili o a scaricare malware.

Passaggi da Seguire:

a. **Identificazione della Minaccia:**
   i. Ricerca e documenta cos'è il phishing e come funziona.
   ii. Spiega come un attacco di phishing può compromettere la sicurezza dell'azienda.
b. **Analisi del Rischio:**
   i. Valuta l'impatto potenziale di questa minaccia sull'azienda.
   ii. Identifica le risorse che potrebbero essere compromesse (ad es. credenziali di accesso, informazioni sensibili, dati aziendali).
c. **Pianificazione della Remediation:**
   i. Sviluppa un piano per rispondere all'attacco di phishing. Il piano dovrebbe includere:
      1. Identificazione e blocco delle email fraudolente.
      2. Comunicazione ai dipendenti sull'attacco e sulle misure da adottare.
      3. Verifica e monitoraggio dei sistemi per individuare eventuali compromissioni.
d. **Implementazione della Remediation:**
   i. Descrivi i passaggi pratici che intraprenderesti per mitigare la minaccia di phishing. Questo potrebbe includere:
      1. Implementazione di filtri anti-phishing e soluzioni di sicurezza email.
      2. Formazione dei dipendenti su come riconoscere e segnalare tentativi di phishing.
      3. Aggiornamento delle policy di sicurezza aziendali.
e. **Mitigazione dei Rischi Residuali:**
   i. Identifica misure di mitigazione da implementare per ridurre il rischio residuo, come:
      1. Esecuzione di test di phishing simulati per valutare la reattività dei dipendenti.
      2. Implementazione di autenticazione a due fattori 2FA) per l'accesso ai sistemi critici.
      3. Regolari aggiornamenti e patching dei sistemi per ridurre le vulnerabilità sfruttabili.

Traccia 2

Obiettivo dell'Esercizio:

Immagina di essere un amministratore di sistema per una media azienda che ha subito un attacco DoS Denial of Service). Gli attaccanti inondano i server aziendali di richieste, rendendo i servizi web inaccessibili agli utenti legittimi.

Passaggi da Seguire:

f. Identificazione della Minaccia:
   i. Ricerca e documenta cos'è un attacco DoS e come funziona.
   ii. Spiega come un attacco DoS può compromettere la disponibilità dei servizi aziendali.
g. Analisi del Rischio:
   i. Valuta l'impatto potenziale di questa minaccia sull'azienda.
   ii. Identifica i servizi critici che potrebbero essere compromessi (ad es. server web, applicazioni aziendali).
h. Pianificazione della Remediation:
   i. Sviluppa un piano per rispondere all'attacco DoS. Il piano dovrebbe includere:
      1. Identificazione delle fonti dell'attacco.
      2. Mitigazione del traffico malevolo.
i. Implementazione della Remediation:
   i. Descrivi i passaggi pratici che intraprenderesti per mitigare la minaccia di DoS. Questo potrebbe includere:
      1. Implementazione di soluzioni di bilanciamento del carico per distribuire il traffico.
      2. Utilizzo di servizi di mitigazione DoS offerti da terze parti.
      3. Configurazione di regole firewall per bloccare il traffico sospetto.
j. Mitigazione dei Rischi Residuali:
   i. Identifica misure di mitigazione da implementare per ridurre il rischio residuo, come:
      1. Monitoraggio continuo del traffico di rete per rilevare e rispondere rapidamente a nuovi attacchi.
      2. Collaborazione con il team di sicurezza per migliorare le difese contro DoS.
      3. Test periodici di resilienza per valutare l'efficacia delle misure di mitigazione adottate.

Task 27/01/25: Remediation e Mitigazione

Report

Parte 1: Minaccia di Phishing

Scenario

Un amministratore di sicurezza per una media azienda ha rilevato una campagna di phishing mirata contro i dipendenti. Gli attaccanti inviano email fraudolente che sembrano provenire da fonti affidabili, inducendo i dipendenti a divulgare informazioni sensibili o a scaricare malware.

Cos'è il phishing?

Il phishing è un tipo di attacco informatico che utilizza email o messaggi fraudolenti per indurre le vittime a rivelare informazioni sensibili, come credenziali di accesso o dati finanziari. Gli attacchi si basano su inganni che simulano comunicazioni legittime.

Impatto sulla sicurezza aziendaleGli attacchi di phishing possono compromettere:

- Credenziali di accesso.
- Informazioni sensibili dei clienti.
- Integrità dei sistemi aziendali attraverso malware o ransomware.

Analisi del Rischio

Impatto Potenziale: Una compromissione tramite phishing può comportare perdita di dati sensibili, danni reputazionali e interruzioni operative.

Risorse Critiche a Rischio: Account email aziendali, dati dei clienti e informazioni finanziarie.

Pianificazione della Remediation

Identificazione e blocco:

- Implementare filtri anti-phishing nei server email utilizzando tecnologie come SPF, DKIM e DMARC.
- Bloccare gli indirizzi IP sospetti e configurare una sandbox per analizzare email sospette.

Comunicazione:

- Avvisare i dipendenti dell'attacco tramite una comunicazione ufficiale interna.
- Fornire istruzioni su come riconoscere email fraudolente con esempi concreti.

Monitoraggio:

- Analizzare i log per identificare eventuali compromissioni e tracciare comportamenti sospetti.

Implementazione della Remediation

Filtri Anti-Phishing: Configurare sistemi di protezione email con tecnologie avanzate di machine learning per individuare schemi di phishing.

Formazione Dipendenti: Sessioni di training interattive con simulazioni di phishing per migliorare la consapevolezza.

Policy di Sicurezza: Aggiornamento delle policy aziendali con linee guida su come segnalare tentativi di phishing.

Mitigazione dei Rischi Residuali

Simulazioni di Phishing: Test regolari per valutare la preparazione dei dipendenti e identificare aree di miglioramento.

Autenticazione a Due Fattori (2FA): Per proteggere gli account critici, aggiungendo un ulteriore livello di sicurezza.

Patching Regolare: Per eliminare vulnerabilità sfruttabili nei sistemi operativi e software aziendali.

Parte 2: Attacco DoS

Scenario

Un amministratore di sistema ha rilevato un attacco DoS contro i server aziendali, che risultano inondati di richieste, rendendo i servizi web inaccessibili agli utenti legittimi.

Cos'è un attacco DoS?

Un attacco Denial of Service mira a sovraccaricare un server o una rete, impedendo l'accesso ai servizi legittimi. Può essere effettuato tramite botnet o script automatici che generano traffico anomalo.

Impatto sulla disponibilità dei servizi:

- Interruzione dei servizi web.
- Perdita di clienti e danni reputazionali.

Analisi del Rischio

Impatto Potenziale: Rallentamenti o blocchi completi dei sistemi critici aziendali.

Servizi a Rischio: Server web, applicazioni aziendali e database, con particolare attenzione ai server che gestiscono transazioni finanziarie o dati sensibili.

Pianificazione della Remediation

Identificazione delle fonti: Analisi dei log per individuare gli IP malevoli utilizzando strumenti come Wireshark o Splunk.

Mitigazione del traffico: Configurare soluzioni di bilanciamento del carico e CDN per distribuire il traffico legittimo e mitigare quello malevolo.

Implementazione della Remediation

Bilanciamento del Carico: Distribuire il traffico su server multipli e configurare limiti di richieste per IP specifici.

Servizi di Mitigazione DoS: Collaborare con provider di sicurezza (ad esempio, Cloudflare o Akamai) per attivare protezioni avanzate.

Regole Firewall: Bloccare gli indirizzi IP sospetti e configurare regole di rate limiting.

Mitigazione dei Rischi Residuali

Monitoraggio Continuo: Controllo costante del traffico di rete per individuare anomalie tramite strumenti come Nagios o Zabbix.

Collaborazione con il Team di Sicurezza: Rafforzare le difese e creare un piano di risposta rapida per futuri attacchi.

Test Periodici: Valutare la resilienza dei sistemi aziendali contro nuovi attacchi, utilizzando simulazioni controllate.

Analisi Wireshark

Nel traffico catturato durante l'attacco DoS, è evidente un pattern di richieste ripetitive da indirizzi IP sospetti (ad esempio: 192.168.1.1 e 192.168.1.2 verso 10.0.0.1). Questi dati sono utili per configurare regole di blocco specifiche nel firewall e migliorare le difese contro futuri attacchi. Si raccomanda di utilizzare Wireshark per filtrare e analizzare il traffico anomalo e configurare regole di protezione appropriate nei sistemi aziendali.

Relazione in breve

Descrizione delle Minacce:

- Il phishing è un attacco mirato al furto di dati attraverso email fraudolente.
- Gli attacchi DoS mirano a sovraccaricare i sistemi per impedirne l'accesso.

Analisi del Rischio:

Entrambe le minacce hanno un alto potenziale di impatto economico e reputazionale.

Piano di Remediation:

- Filtri anti-phishing, formazione dei dipendenti e monitoraggio per il phishing.
- Soluzioni di bilanciamento, firewall e servizi anti-DoS per gli attacchi DoS.

Misure di Mitigazione:

- Simulazioni di phishing, 2FA e patching regolare.
- Monitoraggio continuo del traffico e collaborazione con provider di sicurezza.