MITIGATION E REMEDIATION

ESERCIZIO S11-L1

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 1: Minaccia di Phishing

Scenario

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.

Istruzioni

1. **Identificazione della Minaccia:**
   - Ricerca e documenta cos'è il phishing e come funziona.
   - Spiega come un attacco di phishing può compromettere la sicurezza dell'azienda.
2. **Analisi del Rischio:**
   - Valuta l'impatto potenziale di questa minaccia sull'azienda.
   - Identifica le risorse che potrebbero essere compromesse (ad es. credenziali di accesso, informazioni sensibili, dati aziendali).

ESERCIZIO S11-L1

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 1: Minaccia di Phishing

3. **Pianificazione della Remediation:**
   - Sviluppa un piano per rispondere all'attacco di phishing. Il piano dovrebbe includere:
     - Identificazione e blocco delle email fraudolente.
     - Comunicazione ai dipendenti sull'attacco e sulle misure da adottare.
     - Verifica e monitoraggio dei sistemi per individuare eventuali compromissioni.
4. **Implementazione della Remediation:**
   - Descrivi i passaggi pratici che intraprenderesti per mitigare la minaccia di phishing. Questo potrebbe includere:
     - Implementazione di filtri anti-phishing e soluzioni di sicurezza email.
     - Formazione dei dipendenti su come riconoscere e segnalare tentativi di phishing.
     - Aggiornamento delle policy di sicurezza aziendali.
5. **Mitigazione dei Rischi Residuali:**
   - Identifica misure di mitigazione da implementare per ridurre il rischio residuo, come:
     - Esecuzione di test di phishing simulati per valutare la reattività dei dipendenti.
     - Implementazione di autenticazione a due fattori (2FA) per l'accesso ai sistemi critici.
     - Regolari aggiornamenti e patching dei sistemi per ridurre le vulnerabilità sfruttabili.

ESERCIZIO S11-L1

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 2: Attacco DoS (Denial of Service)

Scenario

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.

Istruzioni

1. **Identificazione della Minaccia:**
   - Ricerca e documenta cos'è un attacco DoS e come funziona.
   - Spiega come un attacco DoS può compromettere la disponibilità dei servizi aziendali.
2. **Analisi del Rischio:**
   - Valuta l'impatto potenziale di questa minaccia sull'azienda.
   - Identifica i servizi critici che potrebbero essere compromessi (ad es. server web, applicazioni aziendali).
3. **Pianificazione della Remediation:**
   - Sviluppa un piano per rispondere all'attacco DoS. Il piano dovrebbe includere:
     - Identificazione delle fonti dell'attacco.
     - Mitigazione del traffico malevolo.

ESERCIZIO S11-L1

Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 2: Attacco DoS (Denial of Service)

4. **Implementazione della Remediation:**
    - Descrivi i passaggi pratici che intraprenderesti per mitigare la minaccia di DoS. Questo potrebbe includere:
        - Implementazione di soluzioni di bilanciamento del carico per distribuire il traffico.
        - Utilizzo di servizi di mitigazione DoS offerti da terze parti.
        - Configurazione di regole firewall per bloccare il traffico sospetto.
5. **Mitigazione dei Rischi Residuali:**
    - Identifica misure di mitigazione da implementare per ridurre il rischio residuo, come:
        - Monitoraggio continuo del traffico di rete per rilevare e rispondere rapidamente a nuovi attacchi.
        - Collaborazione con il team di sicurezza per migliorare le difese contro DoS.
        - Test periodici di resilienza per valutare l'efficacia delle misure di mitigazione adottate.

Documentazione e Report

- Compila un report che includa:
    - Descrizione delle minacce di phishing e DoS.
    - Analisi del rischio per entrambe le minacce.
    - Piano di remediation dettagliato per entrambe le minacce.
    - Misure di mitigazione adottate per entrambe le minacce.

ESERCIZIO S11-L1

Wireshark che cattura un attacco Dos:

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-07-19 06:51:17.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
2	2024-07-19 06:51:18.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
3	2024-07-19 06:51:19.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
4	2024-07-19 06:51:20.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
5	2024-07-19 06:51:21.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
6	2024-07-19 06:51:22.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
7	2024-07-19 06:51:23.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
8	2024-07-19 06:51:24.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet
9	2024-07-19 06:51:25.946205	192.168.1.1	10.0.0.1	TCP	60	DoS attack packet
10	2024-07-19 06:51:26.946205	192.168.1.2	10.0.0.1	TCP	60	DoS attack packet

ESERCIZIO S11-L1: ATTACCO DOS

1. Identificazione della Minaccia

- **Cos'è un attacco DoS e come funziona?** Un attacco **DoS** mira a rendere inaccessibili servizi web o risorse di rete, inondandoli con un numero elevato di richieste false. Questi attacchi sfruttano la capacità limitata dei server, saturandoli e impedendo agli utenti legittimi di accedere.
- **Impatto sugli ambienti aziendali:** Gli attacchi DoS possono causare:
  - **Perdita di accesso ai servizi critici** (es. siti web, applicazioni aziendali).
  - **Danni reputazionali** dovuti all'inaccessibilità.
  - **Perdite economiche** legate all'interruzione delle attività e alla risoluzione.

ESERCIZIO S11-L1: ATTACCO DOS

2. Analisi del Rischio

- **Valutazione dell'impatto potenziale:**
  - Servizi critici compromessi: server web, database aziendali, piattaforme di comunicazione.
  - Dipendenti e clienti non possono accedere ai sistemi, causando disservizi e insoddisfazione.
- **Identificazione dei servizi vulnerabili:**
  - Individuare server esposti a internet senza protezioni adeguate.
  - Analizzare punti di ingresso nella rete aziendale.

ESERCIZIO S11-L1: ATTACCO DOS

3. Pianificazione della Remediation

Piano di risposta all'attacco:

1. **Identificazione delle fonti dell'attacco:**
   - Analizzare i log di rete (es. Wireshark) per individuare IP sospetti, come mostrato nello screenshot (IP **10.0.0.1** inonda il server).
   - Utilizzare strumenti di monitoraggio come IDS/IPS (Intrusion Detection/Prevention Systems).
2. **Mitigazione del traffico malevolo:**
   - Bloccare gli indirizzi IP degli aggressori tramite regole di firewall.
   - Implementare un servizio di mitigazione DoS (es. Cloudflare, Akamai) per distribuire e filtrare il traffico.
   - Configurare regole di **rate-limiting** per limitare le richieste da singoli IP.

ESERCIZIO S11-L1: ATTACCO DOS

4. Implementazione della Remediation

- **Bilanciamento del carico:** Usare bilanciatori (load balancers) per distribuire il traffico.
- **Protezione offerta da terze parti:** Servizi come **CDN (Content Delivery Network)** aiutano a filtrare e ridurre il carico sui server.
- **Regole firewall:** Bloccare traffico sospetto, configurare whitelist di IP fidati.

ESERCIZIO S11-L1: ATTACCO DOS

5. Mitigazione dei Rischi Residuali

1. **Monitoraggio continuo:**
   - Usare strumenti di monitoraggio della rete in tempo reale (es. Zabbix, Nagios) per identificare nuovi attacchi rapidamente.
2. **Collaborazione:**
   - Formare il personale IT sulle strategie di difesa contro attacchi DoS.
3. **Test periodici di resilienza:**
   - Simulare attacchi DoS per verificare l'efficacia delle misure implementate.

ESERCIZIO S11-L1: ATTACCO PHISHING

1. Identificazione della Minaccia

- **Cos’è il phishing e come funziona?** Il **phishing** è una tecnica utilizzata dagli attaccanti per ingannare le vittime, inducendole a fornire informazioni sensibili (come credenziali, dati bancari o informazioni personali) tramite email fraudolente, siti web falsi o altri metodi. Spesso si maschera come una comunicazione legittima (es. una banca o un fornitore di servizi).
- **Impatto sugli ambienti aziendali:**
  - **Furto di credenziali:** Gli attaccanti possono accedere a sistemi critici dell’azienda.
  - **Perdita di dati sensibili:** Violazione di dati aziendali o personali di dipendenti e clienti.
  - **Danni reputazionali:** Perdita di fiducia da parte dei clienti.
  - **Impatto finanziario:** Transazioni non autorizzate o costi di recupero dai danni.

ESERCIZIO S11-L1: ATTACCO PHISHING

2. Analisi del Rischio

- **Valutazione dell’impatto potenziale:**
  - **Dipendenti ingannati da email fraudolente:** Consentono accesso non autorizzato a sistemi aziendali.
  - **Accesso ai sistemi IT interni:** Potenziale perdita di proprietà intellettuale e riservatezza dei dati.
- **Servizi critici vulnerabili:**
  - Sistemi di gestione email.
  - Piattaforme cloud (es. Google Workspace, Microsoft 365).
  - Dati sensibili contenuti in server e database.

ESERCIZIO S11-L1: ATTACCO PHISHING

3. Pianificazione della Remediation

Piano di risposta a un attacco phishing:

1. **Identificazione delle fonti dell'attacco:**
   - Analizzare i log dei server email per individuare le email sospette inviate ai dipendenti.
   - Raccogliere informazioni su link o allegati malevoli per segnalarli come phishing.
2. **Mitigazione dei danni:**
   - **Bloccare i domini di phishing:** Configurare il server email per rifiutare email provenienti dai domini identificati come fraudolenti.
   - **Reset credenziali:** Forzare il reset delle password per account compromessi.
   - **Contenimento del danno:** Isolare i dispositivi infettati o compromessi per evitare la propagazione.

ESERCIZIO S11-L1: ATTACCO PHISHING

4. Implementazione della Remediation

- **Protezione email:**
  - Implementare filtri antispam e antiphishing nei sistemi di posta (es. SPF, DKIM, DMARC).
  - Utilizzare soluzioni di sicurezza avanzata per email, come Proofpoint o Microsoft Defender for Office 365.
- **Sensibilizzazione dei dipendenti:**
  - Organizzare sessioni di formazione per insegnare a riconoscere email sospette.
  - Simulare attacchi phishing periodici per aumentare la consapevolezza.
- **Protezione dei dati:**
  - Attivare autenticazione a due fattori (2FA) per tutti gli accessi critici.
  - Configurare policy di accesso basate su ruoli per ridurre l’accesso non necessario ai dati.

ESERCIZIO S11-L1: ATTACCO PHISHING

5. Mitigazione dei Rischi Residuali

1. **Monitoraggio continuo:**
   - Utilizzare soluzioni SIEM (es. Splunk, QRadar) per rilevare attività sospette nei sistemi.
   - Monitorare costantemente i tentativi di accesso non autorizzato.
2. **Collaborazione con esperti di sicurezza:**
   - Lavorare con team esterni o aziende specializzate per analizzare email di phishing avanzate.
   - Segnalare domini e indirizzi email fraudolenti agli enti competenti.
3. **Test di resilienza:**
   - Simulare campagne di phishing per verificare la preparazione dei dipendenti.
   - Eseguire penetration test per individuare eventuali vulnerabilità