**MAPEO INFORME SEGURIDAD OFENSIVA MITRE ATT&AC**

**Informe Técnico de Seguridad Ofensiva basado en ATT&CK**

**Objetivo del Informe:**

Este informe tiene como propósito documentar el pentesting realizado sobre la infraestructura de TI., sobre la mayor sucursal operativa de una firma operativa a nivel internacional, con producción en nuevas fuentes de energía, y localización en un punto geográficamente complejo ( Punto Tripartito en la Frontera de Tres Países ).

Utilizando la matriz ATT&CK para estructurar las tácticas y técnicas identificadas. Además, se presentan recomendaciones basadas en los hallazgos y las mejores prácticas en ciberseguridad.

**Herramientas y Metodología Utilizadas:**

1. **Nmap:** Escaneo de puertos y servicios.
2. **WPScan:** Enumeración de usuarios y directorios vulnerables en aplicaciones web.
3. **Metasploit Framework:** Explotación de vulnerabilidades.
4. **Hashcat y John The Ripper:** Descifrado de hashes.
5. **Phantom:** Eliminación de rastros.
6. **ATT&CK Navigator:** Mapeo de tácticas y técnicas relevantes.

**1. Resumen del Incidente**

El pentesting llevado a cabo sobre la infraestructura de esta Sucursal, identificó múltiples vulnerabilidades críticas, incluyendo:

* Configuración incorrecta de firewall que exponía servicios sensibles.
* Vulnerabilidades en aplicaciones web que permitieron la ejecución de código remoto.
* Falta de mecanismos robustos de autenticación, facilitando ataques de fuerza bruta.

**2. Tácticas y Técnicas Identificadas (ATT&CK):**

| **Táctica** | **Técnica** | **Descripción** |
| --- | --- | --- |
| Initial Access | Valid Accounts (T1078) | Se obtuvieron credenciales válidas mediante ataques de fuerza bruta y hash cracking. |
| Execution | Command and Scripting Interpreter (T1059) | Ejecución de comandos en la shell interactiva para comprometer servicios. |
| Persistence | Web Shell (T1505.003) | Instalación de una shell web para mantener acceso persistente. |
| Defense Evasion | Indicator Removal on Host (T1070) | Eliminación de logs y rastros utilizando herramientas anti-forense. |
| Discovery | Network Service Scanning (T1046) | Identificación de servicios y puertos abiertos mediante escaneo de red. |
| Privilege Escalation | Exploitation for Privilege Escalation (T1068) | Explotación de vulnerabilidades en servicios para obtener privilegios elevados. |
| Command and Control (C2) | Application Layer Protocol (T1071.001) | Uso de HTTP para mantener comunicación con el sistema comprometido. |
| Impact | Data Destruction (T1485) | Manipulación de datos y posibilidad de eliminarlos en el sistema objetivo. |

**3. Hallazgos Clave del Pentesting:**

1. **Configuraciones Incorrectas:**
   * Firewall con reglas laxas que permitían acceso a puertos innecesarios.
   * Servicios FTP expuestos con credenciales por defecto.
2. **Vulnerabilidades en Aplicaciones Web:**
   * Identificación de vulnerabilidades en WordPress que permitieron enumeración de usuarios y explotación de credenciales débiles.
   * Ejecución de código remoto mediante exploits conocidos en servicios no actualizados.
3. **Acceso No Autorizado:**
   * Uso de herramientas como Metasploit para ganar acceso a bases de datos y sistemas.
   * Elevación de privilegios utilizando exploits en sistemas vulnerables.
4. **Eliminación de Rastros:**
   * Uso de Phantom para borrar logs y rastros de actividades en sistemas comprometidos.

**4. Visualización ATT&CK Navigator:**

Se generaron mapas utilizando ATT&CK Navigator, mostrando:

* El flujo del ataque desde el acceso inicial hasta el impacto.
* Técnicas de evasión empleadas para evitar detección.
* Persistencia lograda mediante shells web y escalamiento de privilegios.

**Capturas de las Visualizaciones:** *(Se incluyen captura y mapas generados en ATT&CK Navigator.)*

**5. Recomendaciones:**

1. **Configuración de Firewall:**
   * Restringir accesos a puertos esenciales mediante reglas estrictas.
2. **Actualización de Software:**
   * Parchear todas las aplicaciones y sistemas operativos con actualizaciones de seguridad recientes.
3. **Fortalecimiento de Credenciales:**
   * Implementar políticas de contraseñas fuertes y autenticación multifactor (MFA).
4. **Monitoreo Activo:**
   * Establecer sistemas de detección de intrusos (IDS) para identificar actividades sospechosas.
5. **Revisión de Aplicaciones Web:**
   * Realizar auditorías periódicas en aplicaciones para identificar vulnerabilidades.

**6. Conclusión:**

El pentesting realizado sobre la mayor sucursal operativa de una firma operativa a nivel internacional, reveló importantes áreas de mejora en la infraestructura de TI. La implementación de las recomendaciones ayudará a mitigar riesgos críticos, mejorando la postura de seguridad de la organización. Se recomienda realizar evaluaciones periódicas y adoptar un enfoque proactivo en ciberseguridad.

**Adjuntos:**

* Resultados del análisis en ATT&CK Navigator.
* Extractos del pentesting.
* Mapas tácticos generados.