Reporte de Análisis de Seguridad

Framework de Pentesting con Impacket

---

1. Resumen de la Herramienta

Framework interactivo de pentesting ético en Python que automatiza herramientas de Impacket para pruebas de penetración contra sistemas Windows desde Kali Linux.

Funcionalidades principales:

- Detección automática de IP con 4 métodos diferentes
- Validación de credenciales contra sistemas Windows
- Reconocimiento de red (ping, Nmap)
- Explotación SMB (acceso a recursos compartidos)
- Ejecución remota (PSExec, WMIExec)
- Extracción de hashes de credenciales (secretsdump)
- Interfaz visual tipo terminal hacker

Tecnologías: Impacket, Python 3, Colorama, Netifaces, Subprocess

---

2. Riesgos de Seguridad Identificados

Críticos (CVSSv3: 9.8)

- **Ejecución de Código Remoto:** PSExec y WMIExec permiten control total del sistema
- **Extracción de Credenciales:** secretsdump.py compromete hashes NTLM/LM
- **Acceso SMB No Autorizado:** Acceso a recursos administrativos (C$, ADMIN$)

Altos

- **Enumeración de Servicios:** Revela arquitectura de red y versiones
- **Movimiento Lateral:** Propagación a otros sistemas una vez comprometido

Medios

- Credenciales en texto plano en memoria
- Posible falta de cifrado en transmisiones

---

3. Cinco Recomendaciones de Defensa para Windows

Recomendación 1: Fortalecer Protocolo SMB

Acciones:

```
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Set-SmbServerConfiguration -EncryptData $true -Force
```

Detección: Monitorear eventos Windows ID 5140, 5145 (accesos SMB)

Recomendación 2: Implementar Autenticación Multifactor

Acciones:

- Activar Windows Hello for Business
- Implementar Azure AD MFA para administradores
- Usar tarjetas inteligentes para cuentas privilegiadas

Beneficio: Bloquea acceso incluso con credenciales comprometidas

Recomendación 3: Monitorear Ejecución Remota

Implementación con Sysmon:

```
<ProcessCreate onmatch="include">
  <Image condition="contains">psexec</Image>
  <ParentImage condition="contains">WmiPrvSE.exe</ParentImage>
```

</ProcessCreate>

Eventos críticos a monitorear:

- Event ID 4688: Creación de procesos
- Event ID 4624: Logon tipo 3 (Network)
- Event ID 4672: Privilegios especiales

Recomendación 4: Proteger Credenciales con Credential Guard

Habilitar protección:

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v LsaCfgFlags /t REG_DWORD /d 1 /f

Enable-WindowsOptionalFeature -Online -FeatureName IsolatedUserMode

Adicional:

- Implementar LAPS para contraseñas únicas de administrador local
- Deshabilitar WDigest

Resultado: Protección contra extracción de hashes

Recomendación 5: Segmentación de Red y Firewall

Reglas de firewall restrictivas:

New-NetFirewallRule -DisplayName "Block WMI Remote" -Direction Inbound -LocalPort 135 -Protocol TCP -Action Block

New-NetFirewallRule -DisplayName "Block SMB External" -Direction Inbound -LocalPort 445 -Protocol TCP -Action Block

Arquitectura:

- VLANs separadas (usuarios, servidores, administración)
- Jump servers para acceso administrativo
- IDS/IPS con reglas para detectar Impacket

---

4. Conclusiones

Este framework representa un riesgo crítico si se usa maliciosamente. Las técnicas implementadas son utilizadas por grupos APT y ransomware.

Mejores prácticas defensivas:

- Principio de mínimo privilegio
- Actualizaciones constantes de seguridad
- SIEM centralizado y EDR en endpoints
- Plan de respuesta a incidentes documentado
- Backups aislados y probados

⚠ **Advertencia:** Uso exclusivo en laboratorios autorizados, evaluaciones contratadas y entornos educativos. El uso no autorizado constituye delito penal.

Referencias: Impacket GitHub, MITRE ATT&CK (T1021, T1003), Microsoft Security Baselines

---

Reporte para fines educativos y mejora de seguridad - Septiembre 2025