Informe de Inteligencia de Amenazas

Máquina *“Basic Pentesting”*

Plataforma: *“TryHackMe (THM)”*

TLP:AMBER | Ref: CTI-2026-1010-THM

Fecha de publicación: 10 de agosto de 2026

Autor: Pedro Parmentier

Aspectos a destacar en el Informe:

1. RESUMEN EJECUTIVO (Executive Summary)

- **Propósito**: Proporcionar una visión técnica y operativa sobre la instrusión realizada contra el objetivo en el entorno controlado, detallando las vulnerabilidades explotadas, el movimiento lateral y las medidas para mitigar los riesgos.
- **Impacto Principal**: Acceso no autorizado a nivel de usuario en el sistema operativo objetivo (`Linux Ubuntu 20.04`), permitiendo la lectura de archivos locales, enumeración de la configuración interna y extracción de llaves de acceso privadas de otros usuarios.
- **Vector de Entrada**: Ataque de fuerza bruta/diccionario sobre el servicio SSH (`puerto 22/TCP`) tras la enumeración exitosa de nombres de usuario mediante el servicio **Samba/SMB**.
- **Movimiento Lateral**: Compromiso del usuario `kay` mediante la extracción exógena de su clave privada SSH (`id_rsa`) almacenada con permisos débiles en `/home/kay/.ssh`, seguida del descifrado **offline** de su frase de paso (*passphrase*).
- **Resumen**: Durante la auditoría/ataque de seguridad del host `Basic Pentesting`, se identificó la exposición de servicios **SMB** y **SSH**. Mediante enumeración de usuarios en Samba, se obtuvo el nombre de cuenta de los usuarios `jan` y `kay`. Un ataque de fuerza bruta posterior contra el puerto 22 permitió obtener acceso inicial con el usuario `jan`. Una vez dentro, se identificó una mala configuración en los permisos del directorio personal del usuario `kay`, lo que permitió copiar su clave privada SSH y realizar un movimiento lateral dentro del sistema.

2. METADATOS Y EVALUACIÓN DE CONFIANZA

- **Nivel de Confianza (Confidence Level)**: Alto (Confirmado en pruebas de penetración directas en un entorno controlado de laboratorio / THM).
- **Mapeo de Clasificación (Admiralty System)**: A1 (Fuente totalmente confiable / Información confirmada de forma expermiental).
- **Estatus de la Amenaza**: Inactiva / Contenida en laboratorio.

3. ENTORNO OBJETIVO

- **Nombre de la Amenaza / Host**: TryHackMe - Basic Pentesting
- **Dirección IP / Alcance**: `10.113.159.246`
- **Sistema Operativo**: Linux Ubuntu 20.04.6 LTS (Focal Fossa)
- **Objetivo Comercial/Función**: Servidor web simulado.

4. FASE DE RECONOCIMIENTO Y RECOLECCIÓN (Reconnaissance & Enumeration)

4.1. Escaneo de Red y Servicios Expuestos

Se ejecutó un escaneo completo de puertos mediante `Nmap` para determinar los servicios expuestos en la red:

```
nmap -p- --open -T4 -Pn -n -vvv -oN target.log 10.113.159.246
```

```
nmap -p22,80,139,445,8009,8080 -sV -sC -vvv -oN ports-info.log 10.113.159.246
```

Puerto	Servicio	Versión	Estado
22/TCP	SSH	OpenSSH 8.2p1 Ubuntu 4ubuntu0.13	Abierto
80/TCP	HTTP	Apache httpd 2.4.41 ((Ubuntu))	Abierto
139/TCP	netbios-ssn	Samba smbd 4	Abierto
445/TCP	netbios-ssn	Samba smbd 4	Abierto
8009	ajp13	Apache Jserv (Protocol v1.3)	Abierto
8080	HTTP	Apache Tomcat 9.0.7	Abierto

4.2. Hallazgos de Enumeración Web y SMB

- **Enumeración Web**: Tras revisar el código fuente de la página principal (`http://10.113.159.246/`), se identificó un comentario de los desarrolladores indicando la existencia de una ruta oculta, haciendo referencia a **«dev note»**. Esto permitió descubrir la ruta `http://10.113.159.246/development` (HTTP 200) en donde se hallaron dos archivos de texto (`dev.txt` y `j.txt`) con notas internas de los desarrolladores indicando que la contraseña de uno de los usuarios era débil.
- **Enumeración SMB**: Se utilizó la herramienta `enum4linux` para consultar el servicio **Samba** en los puertos 139/445, logrando descubrir usuarios válidos del sistema operativo, entre ellos las cuentas de `kay` y `jan`.

5. CADENA DE ATAQUE (Kill Chain & Technical Analysis)

5.1. Acceso Inicial (Initial Access)

- **Táctica MITRE ATT&CK**: Brute Force: Pasword Cracking (`T1110.002`)

- **Vulnerabilidad Explotada**: Credenciales débiles en el servicio OpenSSH (`CWE-1391` / `CWE-522` / `CWE-521`)
- **Descripción del Exploit**:
  - Con el usuario `jan` confirmado mediante `enum4linux` y la pista de clave débil en `/development/`, se ejecutó un ataque de diccionario automatizado contra el puerto SSH (`22/TCP`)
- **Prueba de Concepto (*PoC*)**:

```
# Ataque de diccionario para obtener credenciales
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.113.159.246

# Acceso inicial vía SSH
ssh jan@10.113.159.246
```

5.2. Puntuación y Métrica CVSS v3.1

- **Puntuación Base**: 8.2 (Alto - High)
- **Vector CVSS**: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N`

5.3. Establecimiento de Persistencia y Movimiento Lateral

- **Táctica MITRE ATT&CK**: Unsecure Credentials: Private Keys (T1552.004) / Remote Services: SSH (T1021.004)
- **Descripción**: Durante la exploración del sistema de archivos local como el usuario `jan`, se inspeccionó el directorio `/home/kay`. Se detectó que el directorio `.ssh` de `kay` tenía permisos de lectura abiertos a otros usuarios (`rwxr-xr-x`/`766`), permitiendo la extracción del archivo de clave privada `id_rsa`.
- **Payload Utilizado**:

```
# Copia de la llave privada desde la máquina objetivo
scp -r jan@10.113.159.246:/home/kay/.ssh .

# Extracción del hash y crack del mismo
ssh2john id_rsa > hash.txt
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

# Conexión SSH autenticado como el usuario kay
ssh kay@10.113.159.246 -i id_rsa
```

6. INDICADORES DE COMPROMISO (IoCs)

6.1. Indicadores de Red (Network IoCs)

- **IPs Maliciosas Relacionadas**: `192.168.137.56` (IP de la máquina atacante en la VPN)
- **URLs Afectadas**: `http://10.113.159.246/development/`
- **User-Agents Inusuales e Intentos de Conexión**: Múltiples solicitudes de autenticación SSH fallidas registradas desde la IP del atacante (generadas por `hydra`)

6.2. Indicadores en Host (Host-Based IoCs)

- **Rutas de Archivos Sensibles Accesibles**:
  - `/home/kay/.ssh` (Clave privada SSH expuesta a lectura de otros usuarios)
  - `/var/www/html/development/dev.txt` y `j.txt`
- **Registros y Eventos de Autenticación**:
  - Posibles entradas en `/var/log/auth.log` que reflejan el inicio de sesión exitoso vía SSH para el usuario `jan`, seguido de intentos de lecutra sobre el directorio `/home/kay/.ssh`.

7. MAPEO DE TÁCTICAS Y TÉCNICAS (MITRE ATT&CK)

Fase de la Cadena	ID Técnica	Nombre de la Técnica
Reconnaissance	TT1595.002	Active Scanning: Vulnerability Scanning
Reconnaissance	T1590	Gather Victim Network Information
Credential Access	T1110.002	Brute Force: Password Cracking (Hydra)
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell
Credential Access	T1552.004	Unsecured Credentials: Private Keys
Credential Access	T1110.002	Brute Force: Password Cracking (JohnTheRipper)
Lateral Movement	T1021.004	Remote Services: SSH

8. RECOMENDACIONES Y MITIGACIONES (Actionable Intelligence)

8.1. Mitigaciones Inmediatas (Tácticas)

1. **Fortalecimiento de Contraseñas**: Gestionar el cambio inmediato de clave para la cuenta `jan`, implementando una política de contraseñas robustas (mínimo 16 caracteres, uso de símbolos, números y mayúsculas).
2. **Remoción de Permisos**: Restringir los permisos del directorio `/home/kay/.ssh` y sus archivos contenidos usando:

```
# Directorio
chmod 700 /home/kay/.ssh

# Archivo
chmod 600 /home/kay/.ssh
```

3. **Protección Contra Fuerza Bruta**: Implementar `fail2ban` en el servicio SSH para bloquear direcciones IP tras un límite de intentos fallidos.

8.2. Mitigaciones a Largo Plazo (Estratégicas)

1. *Deshabilitar Autenticación por contraseña SSH*: Configurar `PasswordAuthentication no` en el archivo `/etc/ssh/sshd_config` para uso exclusivo de llaves SSH con *"passphrase"* robusta.
2. *Auditoría periódica de archivos sensibles*: Implementar escaneos automatizados para verificar que ninguna clave o secreto quede almacenado con permisos de lectura para grupos o usuarios no autorizados (`other`)