cat Writeup

Resumen

Breve descripción de la máquina:

- Nombre: Cap
- Direccion utilizada: 10.10.10.245
- Dificultad: Fácil
- Sistema Operativo: Linux
- Resumen: La maquina expone un servidor web vulnerable a IDOR que permite acceder a capturas de red de otros usuarios, revelando credenciales. Luego, una capability de Linux mal configurada permite escalar privilegios a root.

Enumeracion

Nmap

nmap -p- –min-rate=1000 -Pn -T4 10.10.10.245 nmap -p21,22,80 -Pn -sC -sV 10.10.10.245

Resultados: - 21/tcp - FTP (sin acceso anónimo) - 22/tcp - OpenSSH (password capturada con Wireshark) - 80/tcp - Gunicorn HTTP server (Python-based)

Explotacion (Foothold)

HTTP

- Acceso al panel web con varias funciones administrativas (ifconfig, netstat, capturas).
- La funcionalidad de captura genera archivos accesibles por IDOR: /data/ID
- Descargando /data/0 obtuvimos un .pcap con tráfico FTP

PCAP

- En Wireshark se identifican credenciales FTP: *Usuario*: nathan *Password*: Buck3tH4TF0RM3!

SSH

- Las credenciales encontradas en PCAP son validas para ingresar por SSH

Escalada de privilegios

LinPEAS

- Se encontro que python tiene capabilities vulnerables: cap_setuid, cap_net_bind_service=eip
- Esto permite ejecutar Python con UID 0 y escalar a root:

import os os.setuid(0) os.system("/bin/bash")

- Resultado: shell root

Flags

- user.txt (encontrada ni bien ingresar al ssh
- root.txt (encontrada al escalar privilegios con python, en la carpeta root)

Notas finales

- Vulnerabilidades explotadas:
  - IDOR (Insecure Direct Object Reference)
  - Linux capability mal configurada (cap_setuid)
- Aprendizaje: Importancia de proteger endpoints y manejar capacidades de binarios correctamente

Recomendaciones

- Validar accesos en el servidor web, impedir acceso directo a recursos por IDOR.
- Evitar capabilities innecesarias en binarios criticos.