ENVENENAR Y/O SUPLANTAR SERVICIOS

Jordi Masó Pla

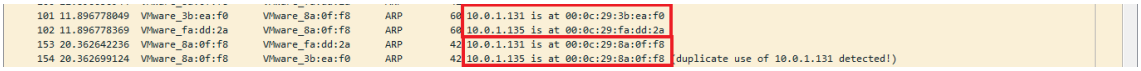
ÍNDICE

1 CAPTURAS RELEVANTES

Una vez tenido el tráfico capturado con Wireshark, analizamos los paquetes que tenemos. Podemos comprobar el envenenamiento de las tablas arp, los inicios de sesión en diferentes servicios, como ftp, telnet, páginas web.

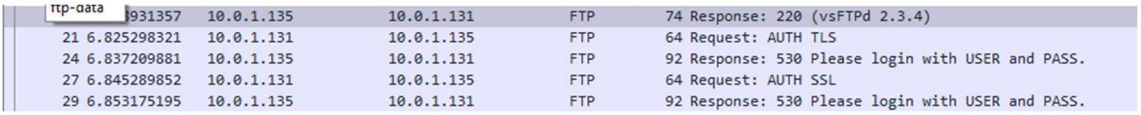
1.1 ARP

En Wireshark comprobamos como el envenenamiento se ha producido correctamente en las dos ips con la dirección MAC de la maquina atacante.



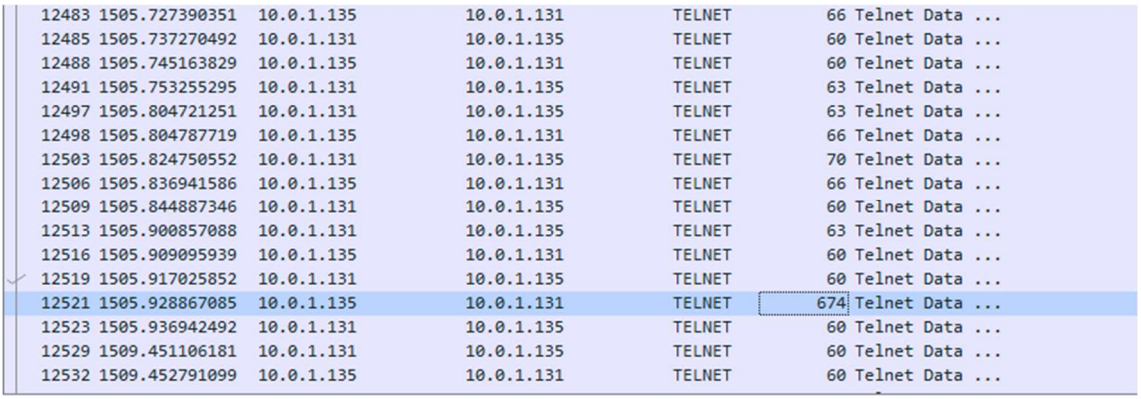
1.2 SERVICIO FTP

Capturamos el trafico del servicio ftp con las conexiones solicitadas por parte de cada máquina.



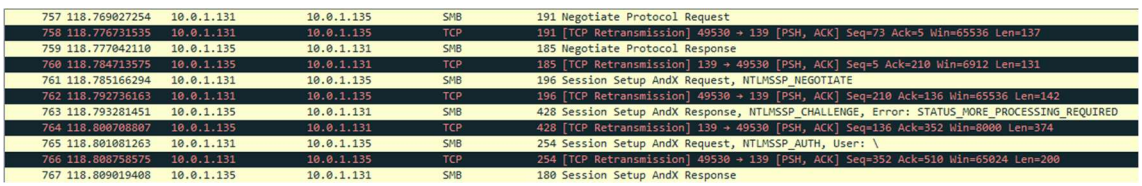
1.3 SERVICIO TELNET

Captura de trafico del servicio telnet del la maquina Windows a Metasplotable 2.



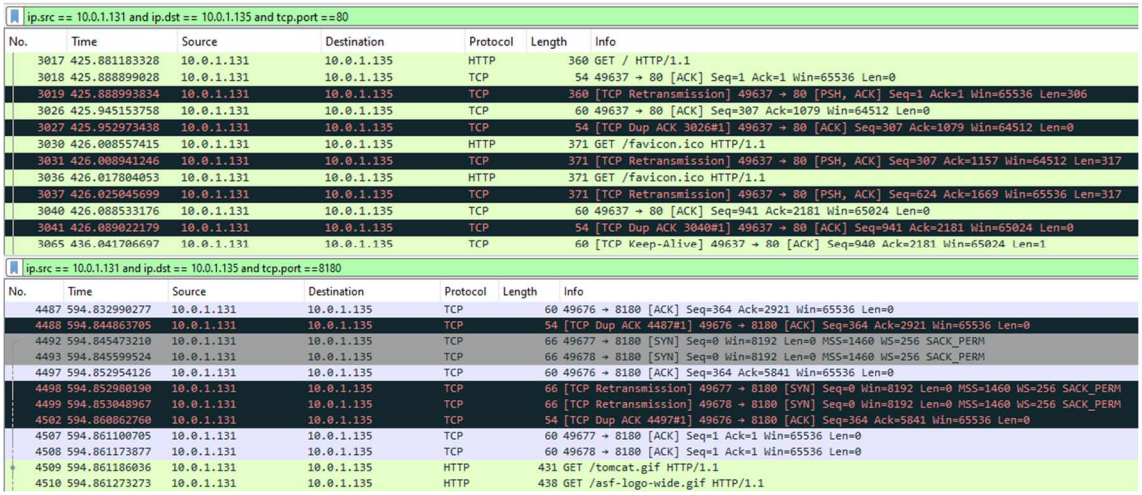
1.4 SERVICIO SAMBA

Captura de trafico con el servicio samba de la maquina Windows para la compartición de ficheros.



1.5 CAPTURA TRAFICO NAVEGADOR WEB

Examinado los paquetes capturados con Wireshark, podemos ver que desde el navegador web ha accedido a diferentes servicios, en el puerto 80 y el puerto 8180.



ip.src == 10.0.1.131 and ip.dst == 10.0.1.135 and tcp.port ==80

No.	Time	Source	Destination	Protocol	Length	Info
3017	425.881183328	10.0.1.131	10.0.1.135	HTTP	360	GET / HTTP/1.1
3018	425.888899028	10.0.1.131	10.0.1.135	TCP	54	49637 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
3019	425.888993834	10.0.1.131	10.0.1.135	TCP	360	[TCP Retransmission] 49637 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=306
3026	425.945153758	10.0.1.131	10.0.1.135	TCP	60	49637 → 80 [ACK] Seq=307 Ack=1079 Win=64512 Len=0
3027	425.952973438	10.0.1.131	10.0.1.135	TCP	54	[TCP Dup ACK 3026#1] 49637 → 80 [ACK] Seq=307 Ack=1079 Win=64512 Len=0
3030	426.008557415	10.0.1.131	10.0.1.135	HTTP	371	GET /favicon.ico HTTP/1.1
3031	426.008941246	10.0.1.131	10.0.1.135	TCP	371	[TCP Retransmission] 49637 → 80 [PSH, ACK] Seq=307 Ack=1157 Win=64512 Len=317
3036	426.017804053	10.0.1.131	10.0.1.135	HTTP	371	GET /favicon.ico HTTP/1.1
3037	426.025045699	10.0.1.131	10.0.1.135	TCP	371	[TCP Retransmission] 49637 → 80 [PSH, ACK] Seq=624 Ack=1669 Win=65536 Len=317
3040	426.088533176	10.0.1.131	10.0.1.135	TCP	60	49637 → 80 [ACK] Seq=941 Ack=2181 Win=65024 Len=0
3041	426.089022179	10.0.1.131	10.0.1.135	TCP	54	[TCP Dup ACK 3040#1] 49637 → 80 [ACK] Seq=941 Ack=2181 Win=65024 Len=0
3065	436.041706697	10.0.1.131	10.0.1.135	TCP	60	[TCP Keep-Alive] 49637 → 80 [ACK] Seq=940 Ack=2181 Win=65024 Len=1

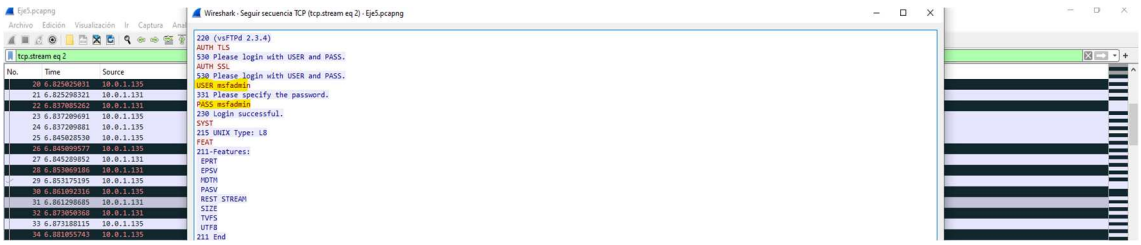
ip.src == 10.0.1.131 and ip.dst == 10.0.1.135 and tcp.port ==8180

No.	Time	Source	Destination	Protocol	Length	Info
4487	594.832990277	10.0.1.131	10.0.1.135	TCP	60	49676 → 8180 [ACK] Seq=364 Ack=2921 Win=65536 Len=0
4488	594.844863705	10.0.1.131	10.0.1.135	TCP	54	[TCP Dup ACK 4487#1] 49676 → 8180 [ACK] Seq=364 Ack=2921 Win=65536 Len=0
4492	594.845473210	10.0.1.131	10.0.1.135	TCP	66	49677 → 8180 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4493	594.845599524	10.0.1.131	10.0.1.135	TCP	66	49678 → 8180 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4497	594.852954126	10.0.1.131	10.0.1.135	TCP	60	49676 → 8180 [ACK] Seq=364 Ack=5841 Win=65536 Len=0
4498	594.852980190	10.0.1.131	10.0.1.135	TCP	66	[TCP Retransmission] 49677 → 8180 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4499	594.853048967	10.0.1.131	10.0.1.135	TCP	66	[TCP Retransmission] 49678 → 8180 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
4502	594.860862760	10.0.1.131	10.0.1.135	TCP	54	[TCP Dup ACK 4497#1] 49676 → 8180 [ACK] Seq=364 Ack=5841 Win=65536 Len=0
4507	594.861100705	10.0.1.131	10.0.1.135	TCP	60	49677 → 8180 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4508	594.861173877	10.0.1.131	10.0.1.135	TCP	60	49678 → 8180 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4509	594.861186036	10.0.1.131	10.0.1.135	HTTP	431	GET /tomcat.gif HTTP/1.1
4510	594.861273273	10.0.1.131	10.0.1.135	HTTP	438	GET /asf-logo-wide.gif HTTP/1.1

2 CAPTURA DE CREDENCIALES

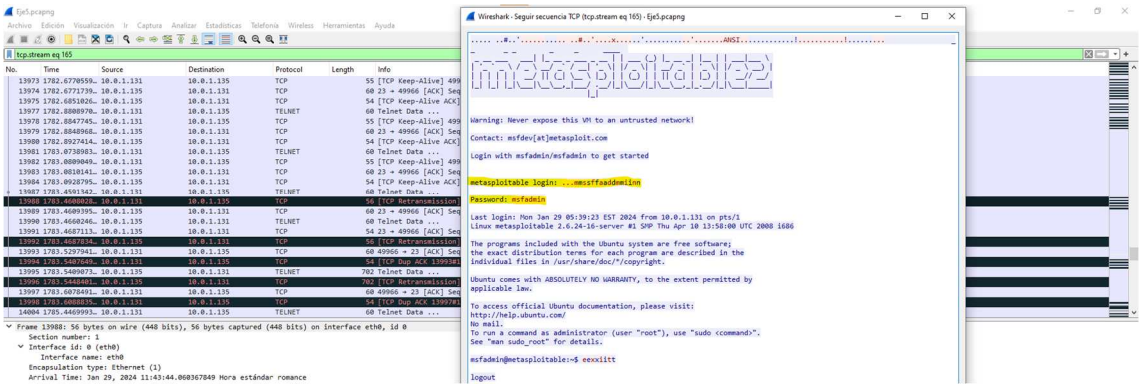
2.1 SERVICIO FTP

Observando los paquetes con Wireshark y filtrando vemos que las credenciales de acceso al servicio ftp están en texto claro y están capturadas. Las credenciales son usuario msfadmin y contraseña msfadmin.



2.2 SERVICIO TELNET

El servicio telnet en desuso por sus vulnerabilidades y que las credenciales viajan por la red en texto claro, por lo tanto, se pueden ver sin mucha dificultad. Las credenciales son usuario msfadmin y contraseña msfadmin.



2.3 CREDENCIALES CAPTURADAS DE SERVICIOS WEB

Al navegar por páginas web y acceder a logins de estas mismas webs, si no están bien diseñadas, las credenciales de pueden viajar por la red en texto claro y ser capturadas. En el puerto 80 hay un servicio DVWA con un login mal configurado, emos podidos capturar las credenciales, que son usuario admin y contraseña password.

En el puerto 8180 hay un servicio tomcat con un login que también emos podidos capturar las credenciales en texto claro. Usuario tomcat contraseña tomcat.