



ENVENENAR Y/O SUPLANTAR SERVICIOS

Jordi Masó Pla

ÍNDICE

1	CAPTURAS RELEVANTES	2
1.1	ARP	2
1.2	SERVICIO FTP	2
1.3	SERVICIO TELNET	2
1.4	SERVICIO SAMBA	2
1.5	CAPTURA TRAFICO NAVEGADOR WEB	3
2	CAPTURA DE CREDENCIALES	3
2.1	SERVICIO FTP	3
2.2	SERVICIO TELNET	3
2.3	CREDENCIALES CAPTURADAS DE SERVICIOS WEB	4

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.

101	11.896778049	VWware_3b:ea:f0	VWware_8a:0f:f8	ARP	60	10.0.1.131	is at	00:0c:29:3b:ea:f0	
102	11.896778369	VWware_fa:dd:2a	VWware_8a:0f:f8	ARP	60	10.0.1.135	is at	00:0c:29:fa:dd:2a	
153	20.362642236	VWware_8a:0f:f8	VWware_fa:dd:2a	ARP	42	10.0.1.131	is at	00:0c:29:8a:0f:f8	
154	20.362699124	VWware_8a:0f:f8	VWware_3b:ea:f0	ARP	42	10.0.1.135	is at	00:0c:29:8a:0f:f8	duplicate use of 10.0.1.131 detected!

1.2 SERVICIO FTP

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

Time	Source	Destination	Protocol	Length	Info
21	10.0.1.135	10.0.1.131	FTP	74	Response: 220 (vsFTPD 2.3.4)
24	10.0.1.135	10.0.1.131	FTP	64	Request: AUTH TLS
27	10.0.1.135	10.0.1.131	FTP	92	Response: 530 Please login with USER and PASS.
29	10.0.1.135	10.0.1.131	FTP	64	Request: AUTH SSL
			FTP	92	Response: 530 Please login with USER and PASS.

1.3 SERVICIO TELNET

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

Time	Source	Destination	Protocol	Length	Info
12483	1505.727390351	10.0.1.135	TELNET	66	Telnet Data ...
12485	1505.737270492	10.0.1.131	TELNET	60	Telnet Data ...
12488	1505.745163829	10.0.1.135	TELNET	60	Telnet Data ...
12491	1505.753255295	10.0.1.131	TELNET	63	Telnet Data ...
12497	1505.804721251	10.0.1.131	TELNET	63	Telnet Data ...
12498	1505.804787719	10.0.1.135	TELNET	66	Telnet Data ...
12503	1505.824750552	10.0.1.131	TELNET	70	Telnet Data ...
12506	1505.836941586	10.0.1.135	TELNET	66	Telnet Data ...
12509	1505.844887346	10.0.1.131	TELNET	60	Telnet Data ...
12513	1505.900857088	10.0.1.131	TELNET	63	Telnet Data ...
12516	1505.909095939	10.0.1.135	TELNET	60	Telnet Data ...
12519	1505.917025852	10.0.1.131	TELNET	60	Telnet Data ...
12521	1505.928867085	10.0.1.135	TELNET	674	Telnet Data ...
12523	1505.936942492	10.0.1.131	TELNET	60	Telnet Data ...
12529	1509.451106181	10.0.1.131	TELNET	60	Telnet Data ...
12532	1509.452791099	10.0.1.135	TELNET	60	Telnet Data ...

1.4 SERVICIO SAMBA

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

Time	Source	Destination	Protocol	Length	Info
757	118.769027254	10.0.1.131	SMB	191	Negotiate Protocol Request
758	118.776731535	10.0.1.131	TCP	191	[TCP Retransmission] 49530 → 139 [PSH, ACK] Seq=73 Ack=5 Win=65536 Len=137
759	118.777042110	10.0.1.135	SMB	185	Negotiate Protocol Response
760	118.784713575	10.0.1.131	TCP	185	[TCP Retransmission] 139 → 49530 [PSH, ACK] Seq=5 Ack=210 Win=6912 Len=131
761	118.785166294	10.0.1.131	SMB	196	Session Setup AndX Request, NTLMSSP_NEGOTIATE
762	118.792736163	10.0.1.131	TCP	196	[TCP Retransmission] 49530 → 139 [PSH, ACK] Seq=210 Ack=136 Win=65536 Len=142
763	118.793281451	10.0.1.131	SMB	428	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
764	118.800708807	10.0.1.135	TCP	428	[TCP Retransmission] 139 → 49530 [PSH, ACK] Seq=136 Ack=352 Win=8000 Len=374
765	118.801081263	10.0.1.131	SMB	254	Session Setup AndX Request, NTLMSSP_AUTH, User: \
766	118.808758575	10.0.1.131	TCP	254	[TCP Retransmission] 49530 → 139 [PSH, ACK] Seq=352 Ack=510 Win=65024 Len=200
767	118.809019408	10.0.1.135	SMB	188	Session Setup AndX Response

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.

The screenshot shows two sections of a Wireshark packet capture. The first section is filtered for traffic to port 80, and the second section is filtered for traffic to port 8180. The table below summarizes the visible packets.

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	425.888993334	10.0.1.131	10.0.1.135	TCP	360	[TCP Retransmission] 49637 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=360
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

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	594.861106705	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

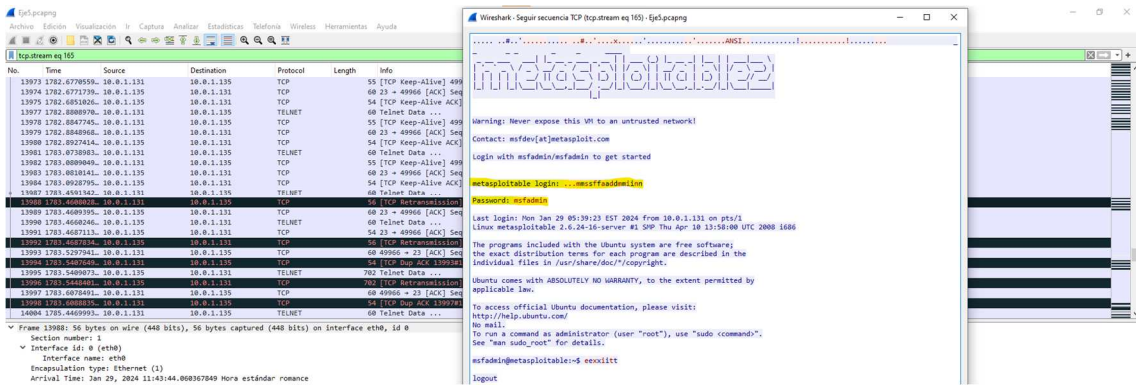
2.1 SERVICIO FTP

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.



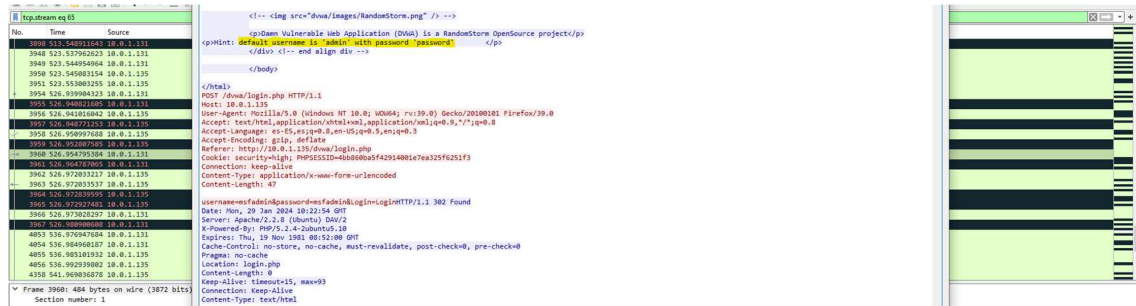
2.2 SERVICIO TELNET

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.

