ATACAR CON UN SNIFFER A UN FTP

1.-Instalamos el sniffer en este caso el Wireshark



2.-Una vez instalado entramos como root para que nos permita capturar el tráfico.

alumno@alumno-pc08:~\$ sudo wireshark

3.-Entramos al filezilla para hacer la prueba.

1	😣 🗉 Gestor de sitio	os						
ſ	Seleccione el sitio:		General	Avanzado	Opciones de	Transferencia		
	Mis sitios		Generat	Avail2000	opciones de			
rchi [,] Tamaño de Tij	📕 Nueva carpe	ta	Servidor:	abde2smr.herobo.com	Puerto:	isos Pro		
Dir	📕 Nuevo sitio		Protocolo:	FTP - Protocolo de Tr				
Dir			Cifrado:	Utilizar FTP simple	rvidor			
Dir								
Dir								
Dir								
Dir		😣 🗈 Gestor d	de sitios					
Dir		Seleccione el siti	io:					
d Dir		V Mis sitio	os	General	General Avanzado			
Dir	rchi [,] Tamaño de Tij	📁 Nueva	a carpeta	Servidor:	rvidor: abde2smr.herobo.com			
Dir	Dir	L Nuevo	o sitio	Protocolo:	Protocolo: FTP - Protocolo de Transf Cifrado: Utilizar FTP simple			
Dir	Nu			Cifrado:				
Dir	Dir				othizarrin	Surpre		
Dir	Dir			Modo de acceso	: Normal			
Dir	Dir			Usuasia	asio: a5267007			
Dir	Dir			USUAITO.	35507007			
Dire	ectc Dir			Contraseña:	•••••			
Dire	Dir			Cuenta:				
3 directorios. Tamai	no c Dir							

4.- Iniciamos el shark

th0 [W	liresh	ark 1.	6.7]				🐱 🖡 🕠 14:15 👤 a
	File	Edit	View Go	Capture Analyze Stat	istics Telephony Tools	Internals	5 Help
0				🏽 📔 🖉 🗙 C	😫 🔍 🔶 🤿 🕯	F	🛓 🗐 🕞 o o a 🕾 🖼 🕅 🕵 🔀 🥝
	Filter	r: 🗌	Show the ca	pture options	▼ Expres	sion Cl	Elear Apply
	No.	Т	ime	Source	Destination	Protocol	l Length Info
		10	.000000	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
		2 2	.019904	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
		3 4	.041877	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
		4 6	.049194	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
M		57	.716203	CadmusCo_9f:14:b0	Broadcast	ARP	60 Who has 192.168.3.1? Tell 192.168.3.139
		68	.059826	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
		79	.726919	192.168.3.139	239.192.152.143	UDP	161 Source port: plysrv-https Destination port: plysrv-https
		89	.726930	192.168.3.139	239.192.152.143	UDP	161 Source port: plysrv-https Destination port: plysrv-https
		9 1	0.069741	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
		10 1	1.980397	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
Z		11 1	3.989134	PlanetTe_37:03:e6	Spanning-tree-(for-br	STP	60 Conf. Root = 32768/0/00:30:4f:37:03:dc Cost = 0 Port = 0x800a
		12 1	5.671216	192.168.3.139	224.0.0.251	MDNS	<pre>117 Standard query SRV alumno@alumno-pc12presencetcp.local, "QM</pre>
100		13 1	5.671805	192.168.3.144	224.0.0.251	MDNS	169 Standard query response A, cache flush 192.168.3.144 SRV, cache
	▶ Fra	me 1:	60 bytes	on wire (480 bits), 6	0 bytes captured (480	bits)	
	▶ IEE	E 802	.3 Ethern	et	a Barrier (7 ann gar an 2 a 2 Agus a saos an 2 Agus a saos		
62	Log	ical-	Link Cont	rol			
	Spa	nning	Tree Pro	tocol			
000							
Se a							

5.- Observamos que ha capturado la contraseña de la conexión entre cliente-servidor esto es debido a que el wireshark aprovecha que FTP lo pone en texto plano sin encritptación.

eth0 [V	Wiresh	ark 1.6.7]															\sim	i ti	■)) 1	13:57
	File	Edit Vie	w Go	Capture Analy	ze Stati	stics Te	lephony	Tools	Internals	Help										
0		i		94 📔 💆	× C		Q (~) Ŧ	↓ [ф		1	•	¥ 🗹 (6	< (?	
	Filter	r:					~	Expres	sion Cl	ear Aj	pply									
	No.	Time		Source		Destinat	ion		Protocol	Lengt	h Info									
		24 17.11	13239	213.4.106.164		192.168	.3.109		HTTP	7	9 Continu	ation	or no	n-HTTI	∙ trafi	fic				
		25 17.11	13258	192.168.3.109		213.4.1	06.164		ТСР	5	4 44920 >	http-	alt [RST] S	Seq=2 V	/in=0 Ler	n=0			
		26 17.61	1871	213.4.106.164		192.168	.3.109		FTP	32	6 Respons	se: 220)		Welcom	ne to Pui	e-FTP	d [pr	ivsep]	
		27 17.61	1891	192.168.3.109		213.4.1	06.164		тср	6	6 44922 >	http-	alt [ACK] S	Seq=97	Ack=300	Win=1	5744	Len=0	TSval:
		28 17.61	L2059	192.168.3.109		213.4.1	06.164		FTP	8	1 Request	: USER	₹ a536	7007						
		29 17.71	12650	213.4.106.164		192.168	.3.109		TCP	6	6 http-al	.t > 44	922 [ACK] S	Seq=306) Ack=112	2 Win=	65535	Len=0) TSva
		30 17.78	35285	213.4.106.164		192.168	.3.109		FTP	10	7 Respons	e: 331	User	a536	7007 0	(. Passwo	ord re	quire	d	
		31 17.78	35451	192.168.3.109		213.4.1	06.164	-	FTP	8	1 Request	: PASS	abde	1993						
		32 17.91	1412	213.4.106.164		192.168	.3.109		TCP	6	6 http-al	.t > 44	922 [ACK] S	Seq=341	Ack=127	/ Win=	65535	Len=0	TSva
		33 18.01	L0168	PlanetTe_37:03	3:e6	Spannin	g-tree-	(for-br	STP	6	0 Conf. R	Root =	32768	/0/00	:30:4f:	37:03:do	Cos	t = 0	Port	: = 0x8
17		34 18.37	75269	192.168.3.125		192.168	.3.255		NBNS	9	2 Name qu	ery NB	SU.F	F.AVAS	ST.COM«	<00>				
······		35 19.12	25730	192.168.3.125		192.168	.3.255		NBNS	9	2 Name qu	ery NB	SU.F	F.AVAS	ST.COM<	<00>				
23%		36 19.88	36112	192.168.3.125		192.168	.3.255		NBNS	9	2 Name qu	ery NB	SU.F	F.AVAS	ST.COM<	<00>				
	▶ Fra	me 1: 60	bytes	on wire (480 b	its), 60	bytes	captured	d (480	bits)											
	▶ IEE	E 802.3 E	Ethern	et																
62	Logical-Link Control																			
1	▶ Spa	nning Tre	ee Pro	tocol																
000																				