CEH Labs Manual

Sniffers

Module 8

Lab

Performing Man-In-The-Middle Attack using Cain & Abel

22. Now, go to Windows 7 Virtual Machine and start FTP



FIGURE 9.16: Control panel in Windows 7

Credential Manager is a new SSO solution that Microsoft offers in Windows Server 2003 and Windows XP to provide a secured store for credential information. It allows you to input user names and passwords for various network resources and applications once, and then have the system automatically supply that information for subsequent visits to those resources without your intervention

Module 08 - Sniffers



FIGURE 9.17: Turn Windows features on or off feature window

23. Now access ftp://10.0.0.7 in Windows Server 2003

Back • 🔿 - 👔 🗍	Search 🜔 Fold	lers 🗟 🗴 🗙 🎝 🖽 -	
dress () 10://10.0.0.7	71		💌 🋃 Go Lini
lame ∽	Size	Type Modified	

FIGURE 9.18: Start ftp://10.0.0.7

24. Now, observe the tool listing out more packets exchange

	Cracker 1	maderoote 100 CC	00 0 10	eess D	Juery
Status	IP address	MAC address	Packets ->	<- Packets	MAC address
the osor and	10.0.0.7	001330482000	10	15	00133048200
4	1	=			1
Status	IP address	MAC address	Packets ->	<- Packets	MAC address
1.1					1
•					

FIGURE 9.19: Sniffer window with more packets exchanged

25. Click Password tab at bottom

This set of credentials is stored in the file \Documents and Settings\%Username%\Ap plication Data\Microsoft\Credentials \%UserSID%\Credentials

> Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

🙎 Decoders 🔮 Network	🛯 😰 Sniffer 🥑 Cracke	r 🔇 Tracerout	e 🛄 (CDU 🏷	Wireless 🚯	Query	
Passwords	Tinestamp	SMB server	Client	Username	Domain	Password
MAP (0) MAP (0) DDAP (0) SMB (1) Telnet (0) W(0) M(0)	4 by SMB			Administrator		

Figure 9.20: Cain and Abel Password tab

과 방 영 교육 전망 전] 가 생 140 % 1 가 같이 200 200 전 전 20 20 20 20 20 20 20 20 20 20 20 20 20						
Passwords	Timestamp	HTTP server	Client	Username	Password	URL.
🖕 FTP (0)	22/12/2010 - 10:24:07	59.151.145.115	192.168.0.100	4d1184390de12258	cain.ulst.ac.uk	http://s7.addthis.com/static
HTTP (24)	22/12/2010 - 10:28:38	209.85.153.154	192.168.0.100	1900989424.1292	http://www.asdf.co	http://www.asdf.com/what
IMAP (0)	22/12/2010 - 10:28:38	209.85.153.100	192.168.0.100	329990207	/whatisasdf.html	http://www.asdf.com/what
DAP (DAP (0)	22/12/2010 - 10:28:38	209.85.153.164	192.168.0.100	1900989424.1292	http://www.asdf.com	http://googleads.g.doublec
(h POP3 (n)	22/12/2010 - 10:28:38	209.85.151164	192.168.0.100	1900989424.1292	http://www.asdf.com	http://googleads.g.doublec
CALL (N)	22/12/2010 - 10:42:28	209.85.151100	192.168.0.100	951143343	/ds	http://www.gamestop.com/
Telest (0)	22/12/2010 - 10:42:30	66.235.131155	192.168.0.100	storefront: ds	Mozilla Default Plug	metrics.gamestop.com
Teinet (U)	22/12/2010 - 10:42:30	66.235.132155	192.168.0.100	storefront: ds	Mozilla Default Plug	metrics.gamestop.com
VNC (0)	22/12/2010 - 10:42:35	209.85.151100	192.168.0.100	2006659900	/Catalog/ProductDet	http://www.gamestop.com
TDS (0)	22/12/2010 - 10:42:35	209.85.153100	192.168.0.100	2006659900	/Catalog/ProductDet	http://www.gamestop.com
TN5 (0)	22/12/2010 - 10:42:35	173.222.5.115	192.168.0.100	4d1184390de12258	www.gamestop.com	http://s7.addthis.com/static
SMTP (0)	22/12/2010 - 10:42:37	66.235.132155	192.168.0.100	pdp: shirlock hol	Mozilla Default Plug	http://www.gamestop.com/
P NNTP (0)	22/12/2010 - 10:43:50	209.85.151100	192.168.0.100	1129859.51	/	http://mail.in.com/
DCE/RPC (0)	22/12/2010 - 10:45:57	209.85.153.100	192.168.0.100	1932716369	/	http://mail.in.com/
55 MSKerbS-PreAuth (0)	22/12/2010 - 10:50:33	209.85.151100	192.168.0.100	677234400		http://www.in.com/
Radius-Keys (0)	22/12/2010 - 10:51:15	202/54/15/152	192468.0.100	122022-044	1 shakora	http://www.in.com/
C Radius-Users (0)	22/12/2010 - 10:51:18	2023415/152	192.168.0.100	the second second	1	http://www.in.com/
100.00	22/12/2010 - 10:51:18	202.54.15/152	192.168.0.100	Contract of the second	1	http://www.in.com/
S INT DOW MA	22/12/2010 - 10:51:18	202.54.15/152	192.168.0.100	Contract of the second	1	http://www.in.com/
D INE-PSK (0)	22/12/2010 - 10:51:19	202.34.13/132	192.168.0.100	and a state of the second	1	http://www.in.com/
D WARD (0)	22/12/2010 - 10:51:20	209/03/15/162	102168.0100	Contract of Charges	1	http://www.in.com/
SNMP (0)	22/12/2010 - 10-51-20	202.54157152	192 168 0 100	Contract of Contract	1	http://www.in.com/
🐔 SIP (0)	22/12/2010 - 10-51-20	202 54 157 152	102 168 0 100	Contract of Contract	1	http://www.in.com/
GRE/PPP (0)	1	10	191.100.0.100	Contraction of the local division of the loc	·	indp://initialiconte
PPPoE (0)						
	HTTP					

Figure 9.21: Cain and Abel Password Extracted

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and "exposure" through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

- 1. Determine how you can defend against ARP Cache Poisoning in a network
- 2. How can you easily find the password captured in EDP MITM attack using only notepad or some other text editor?
- 3. How can one protect Windows Server against RDP MITM attacks?

Internet Connection Required				
□ Yes	☑ No			
Platform Supported				
☑ Classroom	🗹 iLabs			