

#### LAB MANUAL ON A PRACTICAL APPROACH TO NETWORK SNIFFING



ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

**PREPARED BY:** 

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

#### **Table of Contents**

INTRODUCTION TO NETWORK SNIFFING	2
CAIN AND ABEL TOOL	3
NETWORK SNIFFING WITH CAIN AND ABEL TOOL	4
COUNTERMEASURES	22
REFERENCES	26

# **MANUAL-2**: **A Practical Approach to** Network Sniffing

# INTRODUCTION TO NETWORK SNIFFING

- Network sniffing is a process to sniff the network traffic in real-time.
- It works by capturing and analyzing packets of data that flow through a particular network.
- Figure 1 shows the process of network sniffing where data is travelling through a network in the form of packets. The sniffer intercepts the network traffic and captures the raw data packets.
- The captured data packet is analyzed by the packet sniffing software and presented to the network administrators.



Figure 1: Process of network sniffing

### CAIN AND ABEL TOOL

- The Cain and Abel tool [1] is a password recovery and network sniffing tool which is freely available for Windows operating system.
- This tool is useful for network administrators, teachers, security consultants/professionals, forensic staff, security software vendors, professional penetration tester and everyone else that plans to use it for ethical reasons.
- This tool contains features such as Arp Poison Routing (APR) which enables sniffing on switched LANs and wireless network.
- The sniffer can also analyze protocols such as HTTP, SSH-1 and HTTPS and contains filters to capture credentials from a wide range of authentication mechanisms.



Figure 2: Cain & Abel tool

# NETWORK SNIFFING WITH CAIN AND ABEL TOOL

Before downloading and installing Cain & abel tool, it is advised to turn off the Windows firewall and anti-virus tool. The network sniffing can be performed with Cain and abel tool with following steps:

**Step 1:** Search for Cain & Abel in a searching engine and download the tool as shown in Figure 3 and Figure 4 respectively.

Google	cain and abel tool download X 🎍 Q
	Q All ▶ Videos 🖾 Images 🗉 News 🟈 Shopping 🗄 More Settings Tools
	About 3,79,000 results (0.45 seconds)
	www.filehorse.com > Firewalls and Security 💌
	Cain & Abel Download (2020 Latest) for Windows 10, 8, 7
	Aug 22, 2019 - Download Cain & Abel for Windows PC from FileHorse. 100% Safe and Secure
	√ Free Download (32-bit/64-bit) Latest Version 2020.
	★★★★ Rating: 8.1/10 - 55 votes - Free - Windows - Security
	cain_abel.en.downloadastro.com
	Cain & Abel - latest version 2019 free download
	Cain & Abel 0.1733912037037037 free download. Get new version of Cain & Abel. A
	Multipurpose password recovery and security tool for all Microsoft OS
	You've visited this page 2 times. Last visit: 17/9/19
	softfamous.com > > Password Recovery 💌
	Cain & Abel Download Free for Windows 10, 7, 8 (64 bit / 32 bit)
	Jan 23, 2019 - Download Cain & Abel (2020) for Windows PC from SoftFamous. 100% Safe and Secure. Free Download (64-bit / 32-bit).
	Figure 3: Search Cain and abel tool



Figure 4: Download Cain and abel tool

**Step 2:** Download WinPcap for Windows operating system. Figure 5 shows WinPcap for Windows 10 operating system and Figure 6 shows WinPcap for rest of the versions of Windows operating system.

win10pcap.org		New Wind	Pcap-based packet cap	oture library for	r x By Daiyau	Nobori
	Win10Pc	cap driver mo	del. Supports IEEE802	1Q VLAN tags.	University	of Tsukuba, Japan
Overview	Download	How to use	Source code	SDK	License	Japanese
Vin10Pcap is a new Win Inlike original WinPcap, vith Windows 10. Win10 Vin10Pcap has the binau Vireshark or other WinP Vin10Pcap DLLs, instead Vin10Pcap is written as cience of University of 1 Download How to use Source code SDK	Pcap-based Ethernet pac Win10Pcap is compatibl DPcap also supports captury- ry-compatibility with the Pcap-compatible applicati d of original WinPcap. a personal project by Da Tsukuba, Japan. The man	ket capture library. e with NDIS 6.x driver mo uring IEEE802.1Q VLAN ta original WinPcap DLLs. Y ions with Win10Pcap by s iyuu Nobori, a Ph.D stude y parts of Win10Pcap was	edel to work stably igs, ou can run imply installing ent of Computer s from WinPcap.	Appring two flowed (Minutes 102) (a) you go Capton Body you The Save 20 - 2073400 on 1, 00, 1-04 20 - 2074400 on 1, 00, 1-04 20 - 2074400 on 1, 00, 1-04 20	(4123-9-9174c)1 form moder 1.5() Intro. Mayberg Cont Harris (94) The State of the	C      C

#### Figure 5: Download WinPcap for Windows 10 operating system

• winpcap.org/install/	
WiFi Capture Adapter for Windows	
WinPcap Has Ceased Development The WinPcap project has ceased development and WinPcap and WinDump are no longer maintained. We recommend using Np	cap instead.
If you do insist upon using WinPcap, be aware that its installer was built with an old version of NSIS and as a result is vulnerable	to DLL hijacking.
The last official WinPcap release was 4.1.3 For the list of changes, refer to the changelog. Version 4.1.3 Installer for Windows Driver +DLLs	
Supported platforms: • Windows NT4/2000 • Windows XP/2003/Vista/2008/Win7/2008R2/Win8 (x86 and x64)	
MD5 Checksum: a11a2f0cfe6d0b4c50945989db6360cd SHA1 Checksum: e2516fcd1573e70334c8f50bee5241cdfdf48a00	
This executable file installs WinPcap on your machine.	

Figure 6: Download WinPcap for Windows NT/XP/..../Win8 operating system

# **<u>Step 3</u>**: Figure 7 shows icon of Cain & Abel tool on Desktop of Windows operating system after installation.

Recycle Bio	OpenOffice 4111		
powed80			
Slager	1		
(Milware Weaksiteitien	0111ce 2013		
Google	diadiga		

Figure 7: Cain & Abel tool on Windows operating system

**<u>Step 4</u>**: Double click on this icon to open Cain & Abel tool as shown in Figure 8.

File View Configure	Tools Help
Cached Passwords	Press the + button on the toolbar to dump the Protected Storage

Figure 8: Opening Cain & Abel tool

**Step 5:** Click the sniffer tab and press "configure" to open configuration dialog. Select an adapter from the configuration dialog box and click "ok" as shown in Figure 9.

x <mark>en</mark>	
File View Configure Tools Help	
🔄 🏟 🕹 👬 🎆 🎆 🖳 🕂 🥹 😼 🖪 🛯	n 🛤 🖬 🖬 😋 😵 🚺 ? j
🚨 🖉 Decoders 👰 Network 🙀 Sniffer 🥑 Cracker 🔕 Tracer	eroute 🔝 CCDU % Wireless 🚯 Query
Configuration Dialog	ost name B   B   B8   Gr   M0   M1   M3
Challenge Spoofing     Filters and ports     HTTP Fields       Traceroute     Certificate Spoofing     Certificates Collector       Sniffer     APR (Ap Poison Routing)     APR-SSL Options       Adapter     IP address     Subnet Mask       Imp_Ubevice/NIPF_ABEE09     172.16.40.76     255.255.0.0	Image: Section of the section of th
Winpcap Version 4.1.0.2980	
Current Network Adapter \Device\NPF_(ABEE0901-0D79-49E8-8B72-115B93C9E774}	
WARNING !!! Only ethemet adapters supported Options Start Sniffer on startup Start APR on startup	
OK Cancel Apply Help	

Figure 9: Opening configuration dialog to select the router

**Step 6:** Turn on the sniffer and click the "+"icon to select all host in the subnet or give a range of IP address. Click "ok" as shown in Figure 10.

aín						) 🕅
File	View Configure	Tools Help				 
~ • •	♦ CHALL CHALL TWO					
🔤 👪 🖌	AUTH RESET NTLH		🔛 🎦 🔛			
Context Decoders	🍳 Network 🏼 🏙	Sniffer 🦪 Cracker 🔕 Tracero	ute 🔝 CCD	J 🕅 Wireless 🗟 Ouerv		
ID address	MAC address		est name	MAC Address Scanner	M2	_
170.16.00.0	MAC address	Dellare	ostname			 -
172.10.20.9	2417ED A 7E70A	Dell Inc.		Target		
172 16 55 20	2/17EDA7E15A	Dell Inc PCDA Test		<ul> <li>All hosts in my subnet</li> </ul>		
172.10.33.20	2/17EDA7ETEE	Dell Inc PCBA Test		C Bange		
172.10.33.3	3417EBA7E020	Dell Inc PCBA Test		- From		
72 16 55 9	3417EBA68128	Dell Inc PCBA Test				
72 16 55 12	3417EBA7E1E5	Dell Inc PCBA Test		172 . 16 . 0 . 1		
72 16 55 13	3417EBA7E5A5	Dell Inc PCRA Test		- To		
72.16.55.66	3417EBA7456B	Dell Inc PCBA Test				
72.16.80.15	002564C6FF43	Dell Inc.		172 . 16 . 255 . 254		
72.16.80.49	D4BED994502C	Dell Inc				
72.16.80.54	2C44FD25459B	Hewlett Packard		Promiscuous-Mode Scanner		
72.16.80.84	9890969C0DA7			🔲 ARP Test (Broadcast 31-bit)		
72.16.80.85	989096AB6118			ARP Test (Broadcast 16-bit)		
72.16.80.65	90B11C94D84D	Dell Inc.		ARP Test (Broadcast 8-bit)		
72.16.80.70	008CFAADC0F0	Inventec Corporation		ARP Test (Group bit)		
72.16.80.99	2C44FD25080C	Hewlett Packard		ARP Test (Multicast group 0)		
72.16.50.19	782BCB835A97	Dell Inc		ARP Test (Multicast group 1)		
72.16.50.22	D4BED98CE55C	Dell Inc		ARP Test (Multicast group 3)		
72.16.50.23	D4BED98CEEB4	Dell Inc		🗖 All Tests		
72.16.50.21	782BCB834975	Dell Inc				
72.16.50.25	00219BD92745	Dell Inc		OK Cancel		
72.16.50.29	D4BED9944FA5	Dell Inc				
72.16.50.11	002511C08210	ELITEGROUP COMPUTER SY			1	
72.16.50.50	989096AB5DAD					
72.16.50.56	9890969C14B3					
70 16 50 62	000006ADA3CD					 

Figure 10: MAC address scanner

**<u>Step 7</u>**: Select the IP address of target host (172.16.55.9) from the list of hosts as shown in Figure 11.

								_	
n .									
File View Configur	e Tools Help								
A NTLM SPOOF SPOOF	3 📕 🖓 🙀 B. 🗞	🕅 📖 🖬 🚍 🧰 🗐	10	<b>?</b>	-				
AUTH RESET NTLH			• •	•   -					
Decoders 🔮 Network 🗳	🕽 Sniffer 🥑 Cracker 🗕 🍳 Tr	aceroute 🔝 CCDU 🕅 W	reless 🚯	Query	]				
ddress MAC address	OUI fingerprint	Host name	B B	B8	Gr	M0 M1	M3		
16.20.9 002564C6FABE	3 Dell Inc.			_					 
16.55.22 3417EBA7E79A	Dell Inc PCBA Test								
16.55.20 3417EBA7E1EE	Dell Inc PCBA Test								
16.55.5 3417EBA7E5DE	3 Dell Inc PCBA Test								
16.55.8 3417EBA7E024	Dell Inc PCBA Test								
16.55.9 3417EBA68128	Dell Inc PCBA Test			_					
16.55.12 3417EBA7E1F5	Dell Inc PCBA Test								
16.55.13 3417EBA7E5A5	Dell Inc PCBA Test								
16.55.66 3417EBA7456B	Dell Inc PCBA Test								
16.80.15 002564C6FF43	Dell Inc.								
16.80.49 D4BED9945020	Dell Inc								
16.80.54 2C44FD25459E	B Hewlett Packard								
16.80.84 9890969C0DA	7								
16.80.85 989096AB6118									
6.80.65 90B11C94D84E	Dell Inc.								
16.80.70 008CFAADC0F	0 Inventec Corporation								
16.80.99 2C44FD250800	Hewlett Packard								
16.50.19 782BCB835A97	7 Dell Inc								
16.50.22 D4BED98CE55	C Dell Inc								
16.50.23 D4BED98CEEB	4 Dell Inc								
16.50.21 782BCB834975	Dell Inc								
16.50.25 00219BD92745	Dell Inc								
16.50.29 D4BED9944FA	5 Dell Inc								
16.50.11 002511C08210	ELITEGROUP COMPUTER SY								
16.50.50 989096AB5DA	D								
16.50.56 9890969C14B3									
16 50 62 000006 A D A 2 C	D								
losts 🚯 APR 🕂 Routin	g 🚯 Passwords 🛭 🚳 VolP								
1									
ackets: 0%									

Figure 11: Selecting a target

**Step 8:** Select APR tab and perform ARP route poisoning to poison the route and sniff the network packets. Select the IP address of router on left side of the table and IP address of the target host (or we can select all IP addresses) on the right side of the table as shown in Figure 12 and Figure 13 respectively.

File View Confi	gure Tools Help	B, 1 .	I 📟 🚾 🗉	3 (	) % Ø Ø	? 1			
& Decoders 🔮 Network	🙀 Sniffer 🥑 Cra	cker 🔕 Tracer	oute 🔝 CCI	DU	😵 Wireless 🛱	) Query			
APR			New ARF	Poi	ison Routing			x	^
APR-DNS APR-SSH-1 (0) APR-HTTPS (0) APR-ProxyHTTPS (0) APR-RDP (0) APR-RDP (0) APR-FTPS (0) APR-POP3S (0)	APR enables you to directions. If a selec machine has not the all other hosts on yo	hijack IP traffic bet ted host has routing same performance ur LAN.	ween the selecte capabilities WAN of a router you c	/ARN d hos l traff ould c	IING !!! t on the left list and a ic will be intercepted cause DoS if you set.	II selected hosts on th as well. Please note th APR between your De	e right list in both nat since your efault Gateway a	nd	
APR-IMAPS (0) APR-LDAPS (0) APR-SIPS (0)	IP address           17216.39.59           17216.39.124           172.16.02           172.16.0.2           172.16.0.3           172.16.0.1           172.16.0.7           172.16.0.14           172.16.0.50	MAC 90B11C94D837 989096900F83 Ad03C10C21D7 18A9057344F8 9848E1632850 28841C048401 80C166684B28 78E7D1560570 80C16E68327C C8D3A3254D25	Hostname	^	IP address           172 16.201.0           172 16.204.204           172 16.5510           172 16.201.32           172 16.201.32           172 16.201.35           172 16.201.35           172 16.201.35           172 16.201.35           172 16.201.35           172 16.201.35           172 16.201.37           172 16.201.37           172 16.201.37           172 16.201.37	MAC 1C3E845730A7 BC7737B115ED 3417EBA7E820 40F02F602C1 A41731E8FA6D 30483A084C43 B4CEF673C5D6 D0534933F68F 9042E535FAD4 ACE010829641	Hostname		
< > APR 🔶 Rou	Configuration / I uting R Passwords	Routed Packets			,	OK.	Cance	1	

Figure 12: ARP route poisoning

Decoders	📮 🛛 🕂 📎	😼 📴 🕅	route 🕅 CC	🗃 🚺	🕽 📽 💋 🤞	<b>?</b>			
APR	]- <b>3</b>		New AR	P Po	ison Routing	0		x	
APR-DNS APR-SSH-1 (0) APR-HTTPS (0) APR-ProxyHTTPS (0) APR-RDP (0) APR-FTPS (0)	APR enables yo directions. If a se machine has not all other hosts or	u to hijack IP traffic be lected host has routin the same performance your LAN.	tween the select g capabilities W4 e of a router you	WARN ed hos AN traff could (	ING !!! t on the left list and ic will be intercepte cause DoS if you se	all selected hosts on th d as well. Please note t t APR between your Do	e right list in both hat since your efault Gateway a	nd	
APR-POPS3 (0)	IP address           172 16.33,59           172 16.33,124           172 16.025           172 16.0,2           172 16.0,3           172 16.0,1           172 16.0,1           172 16.0,14           172 16.0,13           172 16.0,13           172 16.0,14           172 16.0,15           172 16.0,16           172 16.0,17	MAC 90811C34D837 980965C0F83 A0D3C10C21D7 184905734F8 9848E1632850 28841C048401 80C16E684828 78E7D1560570 80C16E68327C C8D3A3254D25	Hostname	<b>^</b>	IP address 172165566 172165513 172165519 17216559 17216558 17216555 17216552 17216552 17216552 1721629 4	MAC 3417EBA74568 3417EBA7E5A5 3417EBA7E155 3417EBA7E158 3417EBA7E024 3417EBA7E024 3417EBA7E508 3417EBA7E73A 002564C6FABB	Hostname	*	
	Configuration	/ Routed Packets					Canc	el	

Figure 13: Selecting IP address of router and target host

**Step 9:** As shown in Figure 14, the IP address of the target host (172.16.55.9) is displayed with the IP address of the router (172.16.0.1)

File View Conf	igure Tools H	lelp						
📇 🚓 🗘 NTLM SPOOF SPOO	i 🖾 📕 🕼	) 🖬 В 🍕	) 🛲 📟 🚾 📾	a 🥅 🥨	0 6 9			
AUTH RESET NTL	"∓∐" <	Ø   ⊡w≉   64 ⊔						
🚴 Decoders 🔮 Network	🙀 Sniffer 🥑	🕻 Cracker   🔕 1	raceroute 🔝 CC	DU 🐒 Wire	eless	uery		
🔂 APR	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	<u>^</u>
🗠 🔛 APR-Cert (4)	åldle	172.16.0.1	288A1C0A8401	0	0	002564C6FABB	172.16.20.9	
🖳 🚉 APR-DNS	aldle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E79A	172.16.55.22	
	aldle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E1EE	172.16.55.20	
APR-HTTPS (0)	aldle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E5DB	172.16.55.5	
APR-ProxyHTTPS (0)	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA68128	172.16.55.9	
	aldle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E024	172.16.55.8	
APR-FTPS (0)	aldle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E5A5	172.16.55.13	
APR-POP3S (0)	åldle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E1F5	172.16.55.12	
APR-IMAPS (0)	aldle	172.16.0.1	288A1C0A8401	0	0	3417EBA7456B	172.16.55.66	
APR-I DAPS (0)	aldle	172.16.0.1	288A1C0A8401	0	0	002564C6FF43	172.16.80.15	
	aldle	172.16.0.1	288A1C0A8401	0	0	D4BED994502C	172.16.80.49	
	aldle	172.16.0.1	288A1C0A8401	0	0	2C44FD25459B	172.16.80.54	
	dle	172.16.0.1	288A1C0A8401	0	0	989096AB6118	172.16.80.85	
	aldle	172.16.0.1	288A1C0A8401	0	0	9890969C0DA7	172.16.80.84	
	dle	172.16.0.1	288A1C0A8401	0	0	90B11C94D84D	172.16.80.65	
	åldle	172.16.0.1	288A1C0A8401	0	0	008CFAADC0F0	172.16.80.70	
	Å Idle	172.16.0.1	288A1C0A8401	0	0	2C44FD25080C	172.16.80.99	¥
	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
	_							
< >	🚱 Configurat	tion / Routed Pack	ets					
📕 Hosts 🕹 APR 🕂 Ro	uting 🕅 Pass	words 🔏 VolP						
Lost packets: 0%	•	•	_					1.



**Step 10:** Now open an HTTP website on the target host machine (172.16.55.9) and create an account on that website as shown in Figure 15 and Figure 16 respectively.

€ -}	C	hackforums.net/index.php			ත් <b>(</b> )
ł	Welco	ome to HackForums.net		Curre	ent time: 10-26-2015, 04:44 AM
		Packets,	Punks, and Posts		
		a a a a a a a a a a a a a a a a a a a			
		Home Upgrade Search Members Extras V	Viki Help Follow Contact		
	Hello	There, Guest! (Login — Register)			
	Hack F	Forums mmon Hack Tech Code Game Groups Web GFX Market Money			
	Hack	Forums Official Information			
	Forum	 1		Threads/Posts	s Last Post
	?	Rules, Announcements, News, and Feedback This is where site rules and important announcements about the site are made. Please read carefully before you join. Also you car Moderated By: Mentors Suggestions and Ideas HF News	n leave us feedback or ask site questions here.	44,093 598,400	Server Move and Bugs Today 04:39 AM by Fourteen
	Hack	Forums Open Discussion			
	Forum			Threads/Posts	Last Post
	Ř	The Lounge For great discussions on various subjects and to have some fun relaxed topics you can enter our Lounge. Read the rules in the for allowed. Moderated By: Mentors Sports World Tinychat, Join.me, Skype, and Other	ums as trolling, spamming, or flaming are not Chat Invites	440,895 6,250,790	H <b>F, what Anti-Virus do yo</b> Today 04:43 AM by <b>bigwo</b> o
	3	Personal Life Our personal life topics sections are all under subforums of this category. Education Nation Health Wise Nices Bragging Rights		47,509 671,100	<b>I woke up with this!</b> Today 04:44 AM by Truth Hurts

Figure 15: Open an HTTP website on target host

Velcome to HackForums.net		Current time: 10-26-2015, 05:07 Packets, Punks, and Posts				
	Home Upgrade Search Member	rs Extras Wiki Help Follow Contact				
Hello There, Guest! ( <b>Login — Register</b> )						
ack Forums / Register						
Registration	************					
-Account Details		Carteria Count Preferences:				
Username:		Receive emails from the Administrators.				
		Hide your email from other members.				
Complex passwords are at least 10 charact Complex Password:	rs with at least one digit and has both upper and lower case letter. Confirm Password:	<ul> <li>Receive private messages from other users.</li> <li>Alert me with a notice when I receive a Private Message.</li> </ul>				
Email:	Confirm Email:	<ul> <li>Notify me by email when I receive a new Private Message.</li> <li>Hide me from the Who's Online list.</li> </ul>				
		Default Thread Subscription Mode:				
-Referrer:		Do not subscribe				
If you were referred to these forums by an field blank.	ther member you can enter their name below. If not, simply leave this	Time Zone (DST correction excluded):				
		If you live in a time zone which differs to what this board is set at, you can select it from the list below.				

Figure 16: Creating an account in the website

**Step 11:** Now start poisoning the route to sniff the network packets by clicking the APR icon and the status will be changed from "Idle" to "Poisoning" as shown in Figure 17 and Figure 18 respectively.

/Stop APR	Sniffer 🥑	Cracker	Traceroute M CC	DU 😗 Wire	eless 👔 Q	uery		
Stat	tus	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
4)	dle	172.16.0.1	288A1C0A8401	0	0	002564C6FABB	172.16.20.9	
	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E79A	172.16.55.22	
(0)	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E1EE	172.16.55.20	
S (0)	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E5DB	172.16.55.5	
HTTPS (0)	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA68128	172.16.55.9	
)) 🕌	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E024	172.16.55.8	
0) 🛓	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E5A5	172.16.55.13	
S (0) 🛛 🎄 🖞	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA7E1F5	172.16.55.12	
S (0) 🛛 🎄 🖞	dle	172.16.0.1	288A1C0A8401	0	0	3417EBA7456B	172.16.55.66	
S (0)	dle	172.16.0.1	288A1C0A8401	0	0	002564C6FF43	172.16.80.15	
) 🛔	dle	172.16.0.1	288A1C0A8401	0	0	D4BED994502C	172.16.80.49	
` <u>الما</u>	dle	172.16.0.1	288A1C0A8401	0	0	2C44FD25459B	172.16.80.54	
	dle	172.16.0.1	288A1C0A8401	0	0	989096AB6118	172.16.80.85	
	dle	172.16.0.1	288A1C0A8401	0	0	9890969C0DA7	172.16.80.84	
	dle	172.16.0.1	288A1C0A8401	0	0	90B11C94D84D	172.16.80.65	
	dle	172.16.0.1	288A1C0A8401	0	0	008CFAADC0F0	172.16.80.70	
A.	dle	172.16.0.1	288A1C0A8401	0	0	2C44FD25080C	172.16.80.99	
Stat	tus	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	

Figure 17: Before poisoning the route

oders 🔮 Network	🔹 🕼 Sniffer	Cracker 🔇	Traceroute 🔝 CC	DU 🕅 Win	eless 🚯 Q	uery		
PD 6 . (42)	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
PR-Cert (12)	A Poisoning	172.16.0.1	288A1C0A8401	0	0	00193B9F4558	172.16.40.214	
PR-DNS	A Poisoning	172.16.0.1	288A1C0A8401	0	0	00193BA34B50	172.16.40.213	
PR-SSH-1 (0)	d Poisoning	172.16.0.1	288A1C0A8401	0	0	54B80A38A4D8	172.16.40.212	
PR-HTTPS (0)	di Poisoning	172.16.0.1	288A1C0A8401	0	0	4C0F6EDB4124	172.16.40.219	
PR-ProxyHTTPS (0)	d Poisoning	172.16.0.1	288A1C0A8401	0	0	00193B9F4548	172.16.40.216	
PR-RDP (0)	💑 Poisoning	172.16.0.1	288A1C0A8401	0	0	C4A81D953E10	172.16.40.221	
PR-FTPS (0)	💑 Poisoning	172.16.0.1	288A1C0A8401	0	0	C8CBB830374E	172.16.40.199	
PR-POP3S (0)	💑 Poisoning	172.16.0.1	288A1C0A8401	0	0	00193B9F4508	172.16.40.203	
PR-IMAPS (0)	뤒 Poisoning	172.16.0.1	288A1C0A8401	0	5615	00193BA34948	172.16.40.202	
PR-LDAPS (0)	뤒 Poisoning	172.16.0.1	288A1C0A8401	0	0	00193BEE4CCD	172.16.40.201	
PR-SIPS (0)	뤒 Poisoning	172.16.0.1	288A1C0A8401	57	0	C8CBB830387B	172.16.40.200	
	뤒 Poisoning	172.16.0.1	288A1C0A8401	0	0	00193B9F4560	172.16.40.207	
	뤒 Poisoning	172.16.0.1	288A1C0A8401	0	0	00193BEE4CCC	172.16.40.206	
	뤒 Poisoning	172.16.0.1	288A1C0A8401	0	0	00193B9F4540	172.16.40.205	
	뤒 Poisoning	172.16.0.1	288A1C0A8401	0	0	00193B9F4588	172.16.40.204	
	뤒 Poisoning	172.16.0.1	288A1C0A8401	0	0	10DDB1E2CAE7	172.16.40.247	
	Å Poisoning	172.16.0.1	288A1C0A8401	0	0	E83935309D2F	172.16.40.245	
	Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address	
	👶 Configurat	ion / Routed Pac	xets					

Figure 18: After poisoning the route

**Step 12:** Select "HTTP" tab to check the username, password, and URL captured after sniffing the network as shown in Figure 19 and Figure 20 respectively.

MAUTH RESET N	nt 🌳 🛛 🕂 📎 🛛 🛚	B <sub>64</sub>	📟 🔀 🔳 🗖	9 😵 🙋 🧿	<b>1</b> 8			
Decoders	k 🎒 Sniffer 🥑 Crack	ter 🔇 Tracerou	te 🔝 CCDU 🖞	🕅 Wireless 🚯	Query			
asswords 🔺	Timestamp	HTTP server	Client	Username	Password	URL	UserField	
P FTP (0)	26/10/2015 - 17:05:44	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
HTTP (25)	26/10/2015 - 17:05:44	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
MAP (0)	26/10/2015 - 17:05:45	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
LDAP (0)	26/10/2015 - 17:05:52	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
	26/10/2015 - 17:05:55	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SMP (0)	26/10/2015 - 17:05:56	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SIVID (U)	26/10/2015 - 17:05:56	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
Telnet (0)	26/10/2015 - 17:05:58	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
VNC (0)	26/10/2015 - 17:06:02	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
) TDS (0)	26/10/2015 - 17:06:04	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
) TNS (0)	26/10/2015 - 17:06:10	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SMTP (0)	26/10/2015 - 17:06:27	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
NNTP (0)	26/10/2015 - 17:09:48	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
DCF/RPC (0)	26/10/2015 - 17:09:48	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
MCK-rbE DecAuth	26/10/2015 - 17:09:49	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
MSKerbo-PreAutr	26/10/2015 - 17:09:50	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
Radius-Keys (0)	26/10/2015 - 17:09:52	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
Radius-Users (0)	26/10/2015 - 17:09:55	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
ICQ (0)	26/10/2015 - 17:09:56	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
IKE-PSK (0)	26/10/2015 - 17:09:57	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
MvSQL (0)	26/10/2015 - 17:09:58	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SNMP (35)	26/10/2015 - 17:10:08	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SID (0)	26/10/2015 - 17:10:14	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
	26/10/2015 - 17:10:27	5/ 17/ 225 27	172 16 50 50	16/122	12067	http://onlinelibrany.wiley.com/doi/10.1002/eioc.201/02766/ab	an-	
ORE/PPP (U)	<							
> PPPoE (0) *	ы нттр							

Figure 19: Selecting HTTP tab

AUTH RESET N	₩₩	B <sub>64</sub> <sup>№</sup> ] IIII	📟 🔀 🔲 🗖	9 🛯 🖉	? <u>1</u>			
Decoders 🔮 Networ	k 🏟 Sniffer 🥑 Crack	er 🔇 Tracerou	te 🔝 CCDU 🎙	🖞 Wireless 🚯	Query		1	_
asswords 🔨	Timestamp	HTTP server	Client	Username	Password	URL	UserField	
2 FTP (0)	26/10/2015 - 17:05:44	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
HTTP (25)	26/10/2015 - 17:05:44	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
IMAP (0)	26/10/2015 - 17:05:45	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
LDAP (0)	26/10/2015 - 17:05:52	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
POP3 (0)	26/10/2015 - 17:05:55	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SMB (0)	26/10/2015 - 17:05:56	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
Telest (0)	26/10/2015 - 17:05:56	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
reinet (0)	26/10/2015 - 17:05:58	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
VNC (0)	26/10/2015 - 17:06:02	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
) TDS (0)	26/10/2015 - 17:06:04	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
) TNS (0)	26/10/2015 - 17:06:10	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SMTP (0)	26/10/2015 - 17:06:27	52.21.116.233	172.16.50.50	10380	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
NNTP (0)	26/10/2015 - 17:09:48	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
DCE/RPC (0)	26/10/2015 - 17:09:48	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
MSKerb5-DreAuth	26/10/2015 - 17:09:49	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
Padius Kaus (0)	26/10/2015 - 17:09:50	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
Radius-Reys (0)	26/10/2015 - 17:09:52	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
Radius-Users (0)	26/10/2015 - 17:09:55	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
ICQ (0)	26/10/2015 - 17:09:56	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
i IKE-PSK (0)	26/10/2015 - 17:09:57	141.101.121.9	172.16.55.9	shweta	Hacking123	http://hackforums.net/member.php	username=	
MySQL (0)	26/10/2015 - 17:09:58	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SNMP (35)	26/10/2015 - 17:10:08	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
SIP (0)	26/10/2015 - 17:10:14	54.174.225.37	172.16.50.50	16433	12967	http://onlinelibrary.wiley.com/doi/10.1002/ejoc.201402766/ab	an=	
GRE/PPP (0)	26/10/2015 - 17:10:27	5/ 17/ 225 27	172 16 50 50	16/22	12067	http://onlinelihran.wiley.com/doi/10.1002/eioc.201/02766/ah	an-	
								_

Figure 20: Captured username and password on host machine

**Step 13:** Now login the website with captured username and password on your host machine as shown in Figure 21 and Figure 22 respectively.

→ C 🗋 hackforums.net/member.php?action=login	公 🔮
Welcome to HackForums.net	Current time: 10-26-2015, 05:43 AM
	Packets, Punks, and Posts
Home Upgrade Sea	rch Members Extras Wiki Help Follow Contact
Hello There, Guest! ( <b>Login – Register</b> )	
Hack Forums / Login	
Login	
Username/Email:	shweta
Password: Please note that passwords are case sensitive.	(Lost your password?)
<b>Gauth</b> Enter your 2-factor authentication code. Ignore this field if you have it disabled.	(More Info)
	🛛 Remember me
	Login
Contact Us   Hack F	orums   Lite (Archive) Mode   Staff   Awards   Legal Policies   Top

Figure 21: Typing the captured username and password



Figure 22: Successfully authenticated

#### COUNTERMEASURES

The following countermeasures must be followed to prevent sniffing of usernames and passwords:

- Use HTTPS websites: Always make account on HTTPS website. In HTTPS, 'S' stands for security which implies the passwords are stored in encrypted form.
- Don't make accounts in HTTP websites: The passwords stored in HTTP websites are in plain text and are not

encrypted. That's why they are easily readable by the hackers.

- Wrong Policy: While developing a website, an error message of wrong username should not be displayed as "incorrect username" as shown in Figure 23 because hackers can get an idea that the password is correct while the user name is incorrect. Similarly, an error message of wrong password should not be displayed as "incorrect password" as shown in Figure 24 and Figure 25 because hackers can get an idea that the password is incorrect while the username is correct.
- Correct policy: The correct policy of showing an error message is- "incorrect username or password" as shown in Figure 25. This will increase the permutation and combination computations of hackers because they need to spend more time to get the username and password.





← → C	https://www.gliffy.com/go/ologin			୍ଲ ପ୍କୁ ପ୍କୁ
	∜gliffy		Login +	
	Products - Examples Support	Abod •		
	Log In Your e-mail address: Bessionet Passionet Response Log in now Forget your passiond?	Log In With Facebook, Google+	, or Microsoft Live	
	∳gliffy	<b>Useful Links</b> Support Desk User Manual	<b>Use Citify As</b> Flow chart Schware Network Gaczan Schware	

Figure 24: Wrong policy-II

ResearchGate
Sorry, the password you entered is
incorrect.
Email 💿
Password Forgot password?
Password
✓ Keep me logged in
Log in
or log in with
() () ()
No account? Size up
No account? Sign up

Figure 25: Wrong policy-III

The user name or password is	s incorrect
	Member Login
E-Mail Address or Username	🚨 login
Password	
Remember my password?	
	Login
Fi	gure 25: Correct policy

#### REFERENCES

[1] Darknet, "Cain And Abel Download – Windows Password Cracker," 2017. https://www.darknet.org.uk/2007/01/cain-and-abel-download-windows-passwordcracker/ (accessed Apr. 11, 2020).