

Sniffers

Lab Assignment (Module 8)

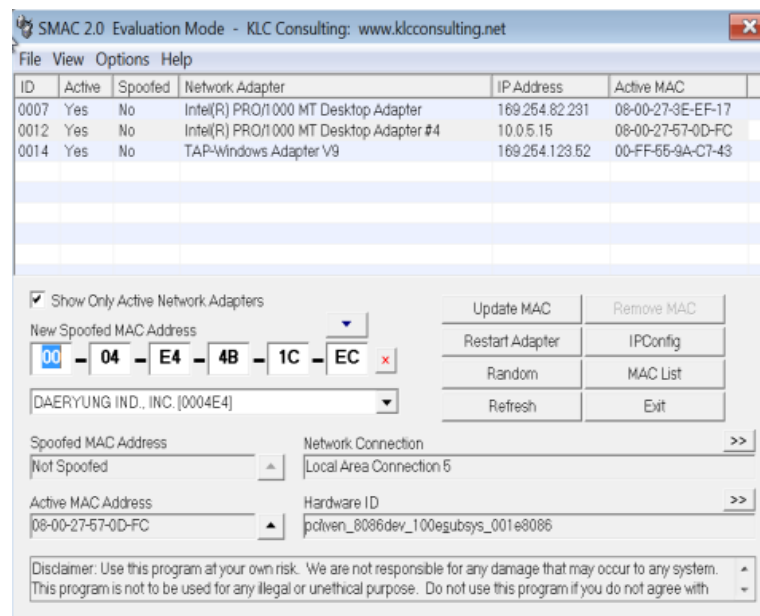
Name: Sachin Saj T K

Roll No: CB.EN.P2CEN18012

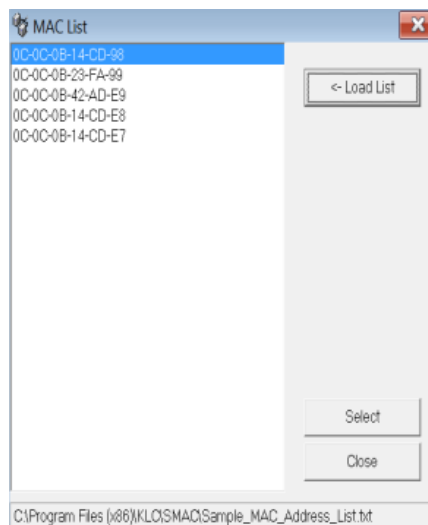
Date of Submission: 10/06/2019

Spoofing MAC Address Using SMAC

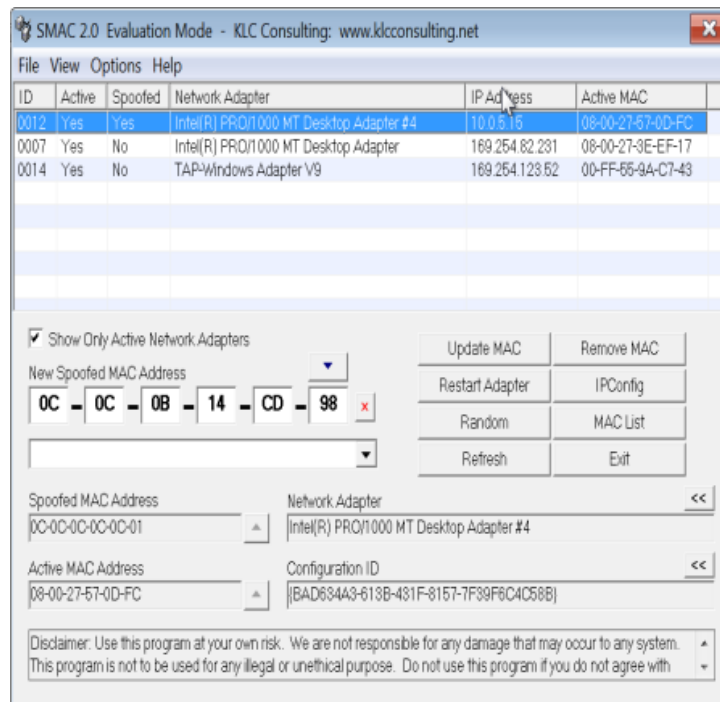
1. Smac



2. Loaded Mac list



3. Mac address spoofed

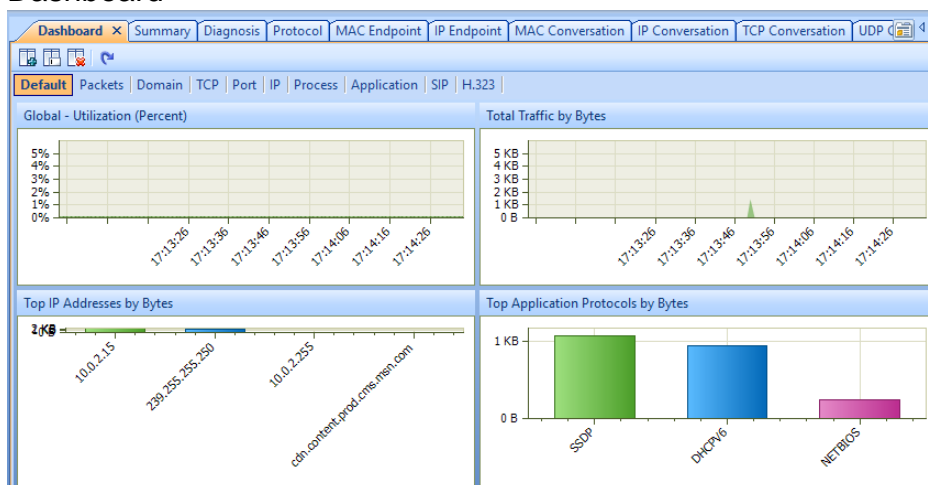


Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
SMAC	Host Name: Intel® PRO/1000 MT Desktop Adapter #4 Node Type: nil MAC Address: 08-00-27-57-0D-FC IP Address: 10.0.5.15

Analyzing a Network Using the Capsa Network Analyzer

1. Dashboard



2. Summary

Dashboard Summary X Diagnosis Protocol MAC Endpoint IP Endpoint MAC Conversation IP Conversation TCP Conversation UDP						
Full Analysis/Statistics:						67
Statistics Item						
Diagnosis						
Information Events						
Notice Events						
Warning Events						
Error Events						
Traffic						
Total	Bytes	Packets	Utilization	Average Utilization	bps	Av
Broadcast	5.11 KB	38	0.002%	0.000%	19.128 Kbps	31
Multicast	247.00 B	1	0.000%	0.000%	1.976 Kbps	2
Average Packet Size	3.25 KB	19	0.002%	0.000%	16.512 Kbps	25
Pkt Size Distribution						
<58	Bytes	Packets	Utilization	Average Utilization	bps	Av
58-63	0.00 B	0	0.000%	0.000%	0.000 bps	0
64-127	350.00 B	6	0.000%	0.000%	0.000 bps	0
128-255	598.00 B	9	0.000%	0.000%	640.000 bps	4
256-511	3.89 KB	22	0.002%	0.000%	18.488 Kbps	26
512-1023	304.00 B	1	0.000%	0.000%	0.000 bps	0
1024-1518	0.00 B	0	0.000%	0.000%	0.000 bps	0

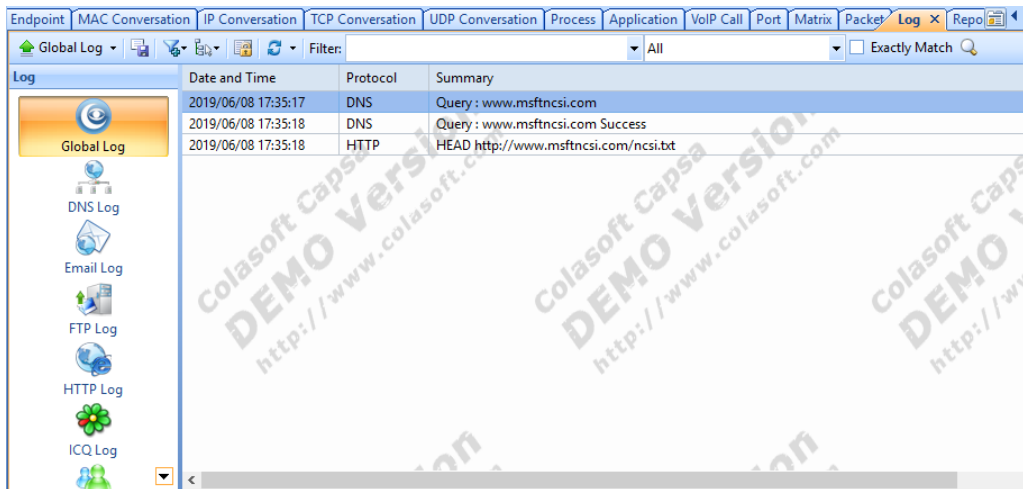
3. Diagnosis

Dashboard		Summary		Diagnosis X		Protocol		MAC Endpoint		IP Endpoint		MAC Conversation		IP Conversation		TCP Conversation		UDP								
Events										Addresses																
										Full Analysis\Diagnostic Item: 1												Full Analysis\Diagnosis Address: 0				
Name					Count					Name					MAC address					IP Address					0	
All Diagnosis					0					There are no items to show in this view.																
Details																										
										Full Analysis\Details: 0																
Severity				Type		Layer		Event Summary						Source IP Address						S						
There are no items to show in this view.																										

4. Protocol

Dashboard Summary Diagnosis Protocol MAC Endpoint IP Endpoint MAC Conversation IP Conversation TCP Conversation UDP						
Filter:		All	<input type="checkbox"/> Exactly Match			
Name	Bytes	Packets	bps	pps		
Ethernet II	1.88 KB	19	1.952 Kbps	4		
IP	1.88 KB	19	1.952 Kbps	4		
TCP	1.37 KB	16	1.952 Kbps	4		
HTTP	592.00 B	3	0.000 bps	0		
UDP	528.00 B	3	0.000 bps	0		
MAC Endpoint IP Endpoint						
Filter:		All	<input type="checkbox"/> Exactly Match			
Name	Bytes	Packets	Bytes Received	Packets Received	Bytes S	
Local Segment	3.51 KB	37	1.63 KB	18	1.88	
Local Host	1.88 KB	19	862.00 B	9	1.04	
PCS Systemtechnik Gm...	1.88 KB	19	862.00 B	9	1.04	
10.0.2.15	1.88 KB	19	862.00 B	9	1.04	
52:54:00:12:35:02	1.63 KB	18	804.00 B	9	862.0	
Broadcast Addresses	262.00 B	1	262.00 B	1	0.0	

5. Logs



Tool/Utility	Information Collected/Objective Achieved
Capsa Network Analyzer	Diagnosis: <ul style="list-style-type: none"> • Name: nil • Physical Address: nil • IP Address: nil
	Packet Info: <ul style="list-style-type: none"> • Packet Number:7 • Packet Length: 80 • Captured Length: 76
	Ethernet Type: <ul style="list-style-type: none"> • Destination Address: 172.17.18.2:53 • Source Address: 10.0.2.15:65015 • Protocol: DNS_QUERY • Physical Endpoint: nil • IP Endpoint: 172.17.18.4
	Conversations: <ul style="list-style-type: none"> • Physical Conversation:10.0.2.15:59741 – 172.17.18.2.53 • IP Conversation: 10.0.2.15 – 172.17.18.4 • TCP Conversation: 10.0.2.15 – www.msftncsi.com • UDP Conversation: 10.0.2.15 – 172.17.18.4
	Logs: <ul style="list-style-type: none"> • Global Log: 2019/06/08 – DNS • DNS Log: 2019/06/08 -10.0.2.15 • Email Log: nil

	<ul style="list-style-type: none"> • FTP Log: nil • HTTP Log: nil • MSN Log: nil • Yahoo Log: nil
--	---

Sniffing Passwords Using Wireshark

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a sequence of packets, with packet 28 selected, which is an HTTP GET request for /success.txt. The packet details pane shows the structure of the HTTP request, including the Host, User-Agent, and Accept headers. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
28	28.822750	10.0.2.15	23.33.185.9	HTTP	347	GET /success.txt HTTP/1.1
30	28.897707	23.33.185.9	10.0.2.15	HTTP	438	HTTP/1.1 200 OK (text/plain)
102	31.593986	10.0.2.15	172.217.167.227	OCSP	434	Request
103	31.594375	10.0.2.15	172.217.167.227	OCSP	434	Request
134	31.745072	172.217.167.227	10.0.2.15	OCSP	755	Response
135	31.759938	172.217.167.227	10.0.2.15	OCSP	755	Response
145	31.870814	10.0.2.15	172.217.167.227	OCSP	434	Request

Frame 28: 347 bytes on wire (2776 bits), 347 bytes captured (2776 bits) on interface 0
 Ethernet II, Src: PcsCompu_07:69:ca (08:00:27:07:69:ca), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 23.33.185.9
 Transmission Control Protocol, Src Port: 1595, Dst Port: 80, Seq: 1, Ack: 1, Len: 293
 Hypertext Transfer Protocol

```

0000  52 54 00 12 35 02 08 00 27 07 69 ca 08 00 45 00  RT..S...'.i...E.
0010  01 4d 52 68 40 00 80 06 cb 09 0a 00 02 0f 17 21  .MRh@... ..!
0020  b9 09 06 3b 00 50 e4 35 9f 6d 01 aa c2 02 50 18  ...;.P.5 .m....P.
0030  fa f0 57 72 00 00 47 45 54 20 2f 73 75 63 63 65  ..Wr..GE T /succe
0040  73 73 2e 74 78 74 20 48 54 54 50 2f 31 2e 31 0d  ss.txt H TTP/1.1.
0050  0a 48 6f 73 74 3a 20 64 65 74 65 63 74 70 6f 72  .Host: d etectpor
0060  74 61 6c 2e 66 69 72 65 66 6f 78 2e 63 6f 6d 0d  tal.fire fox.com.
0070  0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a  .User-Ag ent: Moz
0080  69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77  illa/5.0 (Window
0090  73 20 4e 54 20 31 30 2e 30 3b 20 57 4f 57 36 34  s NT 10. 0; WOW64
00a0  3b 20 72 76 3a 36 37 2e 30 29 20 47 65 63 6b 6f  ; rv:67. 0) Gecko
00b0  2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f  /2010010 1 Firefo
  
```

wireshark_3A126F2A-1148-45B6-92A5-D66F15D68E92_20190608202000_a00104 | Packets: 5889 · Displayed: 54 (0.9%) · Dropped: 0 (0.0%) | Profile: Default

Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
Wireshark	Time: 28.822750 Source: 10.0.2.15 Destination: 23.33.185.9 Protocol: HTTP Length: 347 Info: GET/ success.txt HTTP/1.1

