Sniff ICMP traffic (10 + 10 = 20 points)

Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping

Internal Kali.

a. Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic.

🖳 Kali	- Internal Workstation on BPEAR003 - Virtual Machine Connection	- 0	×
File	Action Media Clipboard View Help		
┣ @	● ● ● ○ II II B 5 🗄 🔠		
Appli	cations 🔻 🛛 Places 🔻 📶 Wireshark 👻 🛛 🛛 🗤 💶 🚺	🖬 💉 📢 🖰	-
	*eth0	• •	×
	<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp		
	표 🖉 🕲 🖬 🔛 🛇 🗢 + २ २ 🖉 🖬 🗇 🕲 🖉 🔳 📐		
	licmp	Expression	+
	No. Time Source Destination Protocol Length Info		
9	226 117.847050500 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable	e (Port unreach	
5	228 117.847051400 192.106.10.13 192.106.10.2 ICMP 109 DESEMATION UNFERCHADI 230 117 847066900 192 168 10 13 192 168 10 2 ICMD 109 DESEMATION UNFERCHADI	e (Port unreach e (Port unreach	
	232 117.847071400 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable	e (Port unreach	
_	234 117.847076400 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable	e (Port unreach	
	236 117.847080200 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable	e (Port unreach	
	515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable	e (Port unreach	
	516 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable	e (Port unreach	
_	51/11/.550/52200 192.106.10.10 192.106.10.2 ICMP 102 Destination unreachable	e (Port unreach e (Port unreach	
M		, (Fort unreach	-
.	Frame 234: 109 hytes on wire (872 hits) 109 hytes cantured (872 hits) on interface 0		
	Ethernet II, Src: Microsof 40:57:03 (00:15:5d:40:57:03), Dst: Microsof 40:57:1e (00:15:5d:40:57:1e)		
	→ Internet Protocol Version 4, Src: 192.168.10.13, Dst: 192.168.10.2		
×	▶ Internet Control Message Protocol		
<u>S</u>			
6			
	k.		
7			
	0000 00 15 5d 40 57 10 00 15 5d 40 57 02 00 00 45 c0 104 104 5		
	0020 0a 02 03 03 92 9d 00 00 00 00 45 00 00 43 8d 58 ·································		
<u> </u>	0030 00 00 40 11 57 f2 c0 a8 0a 02 c0 a8 0a 0d 00 35 @ W · · · · · · 5		
•••	0050 ac cd 00 2T 5/ b2 d0 09 81 82 00 01 00 00 00/W	1	
::::	0060 03 6e 74 70 03 6f 72 67 00 00 01 00 01 00 01 01 01 01 01 01 01	dows	
	Go to Settings to	activate Windows.	

b. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM.

<pre>File Action Media Clipboard View Help Action Places Places Wireshark Wed03:47</pre>	•
Image: Image	•
Applications Places Wireshark *eth0 *eth0 *eth0 File Edit View Go Capture Analyze Statistics Telephony Wireless Iools Help Image: Statistics Telephony Help Image: Statistics Telephon	•
*eth0 Fle Edit Yiew Go Capture Analyze Statistics Telephony Wireless Tools Help Image: Statistic Statistics Telephony Wireless Tools Help Image: Statistic Statistics Telephony Wireless Tools Help Image: Statistic Statistic Statistics Telephony Wireless Tools Help Image: Statistic Statistic Statistics Telephony Wireless Tools Help Image: Statistic Statistic Statistic Statistics Telephony Wireless Tools Help Image: Statistic Statistic Statistic Statistics Telephony Protocol Length Info Expression Image: Statistic S	8
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Image: Statistics Telephony Help Image: Statististics Telephony Help <tr< th=""><th></th></tr<>	
Image: Image	
Applya display filter <ctrl.></ctrl.> Expression No. Time Source Destination Protocol Length Info 228 117.847061400 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable (Port unreach 226 117.847061400 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable (Port unreach 762 183.762745300 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 761 183.762745300 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 520 117.850755800 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 519 117.850754700 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 517 117.850752200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachabl	
No. Time Source Destination Protocol Length Info 228 117.847061400 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable (Port unreachable 226 117.847050500 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable (Port unreachable 762 183.762745300 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreachable	+
228 117.847061400 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable (Port unreach 226 117.847050500 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable (Port unreach 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 56 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 520 117.850755800 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 519 117.850754700 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 519 117.850754700 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 517 117.850752200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 1102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.8507516.0 0.15.5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e)	F
226 117.847050500 192.168.10.13 192.168.10.2 ICMP 109 Destination unreachable (Port unreach 762 183.762745300 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 761 183.762745300 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 520 117.850755800 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 519 117.850754700 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 519 117.850754700 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 517 117.850752200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 11	
 102 163.76273900 192.166.10.10 192.166.10.2 104 102 Destination unreachable (Port unreach 520 117.850755800 192.168.10.10 192.168.10.2 104 113 Destination unreachable (Port unreach 519 117.850753400 192.168.10.10 192.168.10.2 104 113 Destination unreachable (Port unreach 518 117.850753400 192.168.10.10 192.168.10.2 104 113 Destination unreachable (Port unreach 516 117.850753400 192.168.10.10 192.168.10.2 104 113 Destination unreachable (Port unreach 516 117.850752200 192.168.10.10 192.168.10.2 104 102 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 104 104 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 104 104 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 105 117.850740600 192.168.10.10 192.168.10.2 104 104 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 104 104 Destination unreachable (Port unreach 516 117.850740600 192.168.10.10 192.168.10.2 104 113 Destination unreachable (Port unreach 516 117.850740600 192.168.10.10 192.168.10.2 104 113 Destination unreachable (Port unreach 516 117.850740600 192.168.10.10 192.168.10.2 105 117.850740600 192.168.10.10 105 117.850740600 192.168.10.10	
 520 117.850755800 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 519 117.850753400 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 518 117.850753400 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 517 117.850752200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.8507540600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10, Dst: 192.168.10.2 Frame 762: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0 Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:1e) Internet Control Message Protocol 	
 519 117.850754700 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 518 117.850753400 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 517 117.85075200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10, Dst: 192.168.10.2 Frame 762: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0 Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e) Internet Control Message Protocol 	
518 117.850753400 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreachable (P	
517 117.850752200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 516 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 Image: Non- 113 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 Image: Non- 515 117.850740600 192.168.10.10 Image: Non- 515 117.850740600 192.168.10.10 192.168.10.2 Image: Non- State State S	
516 117.850751200 192.168.10.10 192.168.10.2 ICMP 102 Destination unreachable (Port unreach 515 117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreach Image: Signal and Signa	
515117.850740600 192.168.10.10 192.168.10.2 ICMP 113 Destination unreachable (Port unreachable (Po	
Frame 762: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0 Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e) Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.2 Internet Control Message Protocol	•
<pre>> Frame 762: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0 > Ethernet II, Src: Microsof_40:57:0c (00:15:5d:40:57:0c), Dst: Microsof_40:57:1e (00:15:5d:40:57:1e) > Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.10.2 > Internet Control Message Protocol</pre>	_
<pre>internet Control Version 4, Src: 192.168.10.10, Dst: 192.168.10.2 Internet Control Message Protocol </pre>	
Internet Control Message Protocol	
■ 0000 00 15 5d 40 57 1e 00 15 5d 40 57 0c 08 00 45 c0 ···]@W····E·	
0010 00 58 e1 90 00 00 40 01 02 f8 c0 a8 0a 0a c0 a8 ·X····@·······	
0020 0a 02 03 03 92 93 00 00 00 00 45 00 00 3c eb 7e	
111 0000 00 00 03 62 74 70 06 75 62 75 66 74 75 03 63 65, ntrue buntu co	
0060 6d 00 00 01 00 01 m	
Go to Settings to activate windows.	

2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to

use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu

VM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.

TALLACKET Kall - External Workstation on BPEARoos - Virtual Machine Connection	2	Attacker Kali -	External Workstation	on BPEAR003 -	Virtual Machine Connection	
--	---	-----------------	----------------------	---------------	----------------------------	--



:::

b. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.

🖳 Kali	- Internal	Workstation on	BPEAR003 - V	irtual Machine	Connection						-	- 0	×
File	Action	Media Clipb	ooard View	Help									
₽ ©	. 🔳 🧿	🕲 🔢 🕨	ל 🖏	2 🔠									
Applie	cations	 Places 	👻 📶 W	/ireshark -			Wed 04:02				1 🗯	, ≰ ∎))	، گ
							*eth0					•	• •
	<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apt	ure <u>A</u> naly	ze <u>S</u> tatistic	s Telephon <u>y W</u> irele	ess <u>T</u> ools <u>H</u>	lelp					
		1	0	XC	Q 🔹 🖬	📕 (+ +) 🐛	€	ର୍ ପ୍	3 6				
	ftp										E E	xpressio	n +
	No	Time		Source		Destination	D	rotoco 4	length Info				
2	140.	266 108.64	45063300	192.168.	10.10	192,168,217.	3 F	TP	80 Response: 2	21 Goodb	ve.		
		265 108.64	42769000	192.168.	217.3	192.168.10.1	0 F	TP	72 Request: QL	IT			
\$		252 102.23	31388600	192.168.	10.10	192.168.217.	3 F	TP	85 Response: 2	15 UNIX	Type: L8		
-		250 102.22	28708500	192.168.	217.3	192.168.10.1	0 F	TP	72 Request: SY	ST			
		248 102.22	22860100	192.168.	10.10	192.168.217.	3 F	TP	89 Response: 2	30 Login	successful		
		239 102.13	31493400	192.168.	217.3	192.168.10.1	0 F	TP	81 Request: PA	SS passw	ord		
		226 96.198	8400000	192.168.	10.10	192.168.217.	3 F	TP	100 Response: 3	31 Pleas	e specify t	he pass	sword.
		224 96.190	5226000	192.168.	217.3	192.168.10.1	0 F		80 Request NUS	ER CYSE3	01 Dd 2 0 2)		
		209 91.41	3330900	192.100.	10.10	192.100.217.	з г	IP	oo kespolise: 2	20 (VSFI	Pu 3.0.3)		
M	4												
. 🖤	- Tra	anemiesion	Control	Protoco	Src Por	t. 18956 Det Po	rt·21 Se	a. 1	Ack: 21 Len: 14				
		Source Por	t: 48956	i 1100000.	, 510 101	c. 40000, D3C F0	10.21,00	ч· ±,	ACK. 21, LCII. 14				
		Destinatio	n Port:	21									
		[Stream in	dex: 22]										
1		TCP Segme	nt Len:	14]									
		Sequence n	umber: 1	(rel	ative sequ	uence number)							
		[Next sequ	ence num	ber: 15	(relat:	ive sequence numb	er)]						
5	- I	Acknowledg	ment num	ber: 21	(relat:	ive ack number)							
		1000	= Header	Length:	32 bytes	(8)							
5		⊢lags: ⊍x⊍	18 (PSH,	ACK)									
	· ·	VINDOW SIZ	e varue:	229	22121								
			u window	, 3120. 2	1001								Ψ.
	0000	00 15 50	40 57 0	9c 00 15	5d 40 57	1e 08 00 45 10	· ·]@W · · ·]@W··	·E·				
	0010	00 42 48	ad 40 0	00 3T 06	8e 9a c0	a8 d9 03 c0 a8	· BH · @ · ? ·	~	· · · ·				
$\boldsymbol{\Lambda}$	0020	00 e5 96	30 00 1 30 00 6	10 US 0a	07 30 33	98 a7 65 59 Ab	=		eY.				
	0040	52 3b 55	5 53 45 5	52 20 63	79 73 65	33 30 31 0d 0a	R;USER c	vse30	1				
:::							,	,		ctivate \	Nindows		
··· _									r (o to Settin	rs to activate V		
											gs to activate v		

Went into the internal kali and filtered to ftp. Looking at the request and responds you can see the password and usernames used. To commfrim that password and usernames that say login successful to cimfimt that the password and username used allowed entrance.

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these "secrets" from the attacker VM, which is Internal Kali.

	Capturing fro	om eth0			Ξ	• ×	
File Edit View Go Capture Apply	Statistics Telephony Wireless Tool	le Help)		
	root@CS	52APenTest:	~ •	• •			
File Edi	t View Search Terminal Help						_
Apply a display filter <ctrl- bi<="" td="" using=""><td>nary mode to transfer files.</td><td></td><td></td><td>–</td><td> Express </td><td>ion +</td><td></td></ctrl->	nary mode to transfer files.			–	 Express 	ion +	
ftp> exi	.t						alion
747 133 251657500 1 0000	Ibye.			(Dod	ect for	host)	
748 133 251663000 1 Connoctd	APeniest: # 110 192.108.10.10			(Red	ect for	host)	
749 133.251665000 1220 (vs	TPd 3 0 3)			(Red	ect for	host)	IR an
750 134.247325900 1 Name (19	2 168 10 10:root) bpear003			id=0:	861, sec	=1351/:	
751 134.253100300 1331 Plea	ise specify the password.			(Red	ect for	host)	
752 134.253150000 1 Password				(Red	ect for	host)	
753 134.253153500 1 <mark>530 Log</mark> i	n ⁷ incorrect. ^{192.168.217.3}			(Red.	ect for	host)	SSWO
754 134.253155600 1Login fa	iled. 192.168.217.3			(Red.	ect for	host)	13500
755 135.248511000 1 ftp> exi	t/.3 192.186.10.10			1d=01	861, seq	=1352/:	
750 135.250230800 1221 Good	bye.			(Red.	ect for	nost)	
757 135.250291400 1 root@C52	APenTest:~# ttp 192.168.10.10			(Red.	ect for	host)	-
759 135 250296500 1220 (ven	d to 192.168.10.10.			(Red	ect for	host)	
760 136 257451400 1 Name (19	1Pd 3.0.3)			id=01	861 sec	=1353/	
761 136.260983800 1331 Plea	se specify the password			(Red	ect for	host)	
762 136.261029500 1 Password	192.168.217.3			(Red.	ect for	host)	
763 136.261032400 1530 Logi	n7incorrect.192.168.217.3			(Red:	ect for	host)	
764 136.261034700 1Login fa	iled. 192.168.217.3			(Red:	ect for	host)	
765 137.259429500 1 ftp> exi	t7.3 192.186.10.10			id=0:	861, seq	=1354/:	
766 137.261545900 1 <mark>221 Good</mark>	lbye. 192.168.217.3			(Red:	ect for	host)	
767 137.261590600 1 root@CS2	APenTest:~# 92.168.217.3			(Red.	ect for	host)	
768 137.261593100 192.168.2	17.2 192.168.217.3	ICMP	126 Redirect	(Redin	rect for	host)	
769 137.201595200 192.108.2	17.2 192.108.217.3	ICMP	126 Redirect	(RedI)		HOSE)	
771 128 265062700 192.100.2	17.3 192.100.10.10	TCMP	126 Podiroct	(Dodin	set for	-13557.	
772 138 265109600 192 168 2	17.2 192.100.217.3	TCMP	126 Redirect	(Redi)	rect for	host)	
112 1001200100000 102110012	1021100121110	2011	120 110021 000	(11042)	000 101	noo c /	·

🖳 Kali	- Internal \	Workstation o	n BPEAR003 - V	/irtual Machine	Connection						- 0	×
File	Action	Media Cli	pboard View	Help								
₽ 0	• 0	0 II b	- 🔂 5 📲									
Applie	cations	 Place 	es 🔻 🛛 🛛 🛛	Vireshark 🔻			Wed 04:	08			1 😼 💉 🕬	с –
							*eth0				•	• •
	<u>F</u> ile	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> api	ture <u>A</u> naly:	ze <u>S</u> tatisti	ics Telephony	<u>N</u> ireless <u>T</u> ool	s <u>H</u> elp				
			• • •	XC	ଦ୍ 🔹	ا+ + ت. +		ହ ବ୍ ଦ୍	3			
	📕 ftp										Expressio	n +
	No.	Time		Source		Destination	ı	Protoco *	Length Info			-
9	1	724 563.	879437200	192.168.	217.3	192.168.	10.10	FTP	72 Request:	SYST		
	1	726 563.	879502600	192.168.	10.10	192.168.	217.3	FTP	104 Response:	530	Please login with USER	and I
		759 569.	386446000 087356500	192.108.	217.3	192.108.	10.10	FTP	72 Request: 80 Response:	221	Goodbye	
-		769 570.	836351900	192.168.	10.10	192.168.	217.3	FTP	86 Response:	220	(vsFTPd 3.0.3)	
	1	969 608.	466965200	192.168.	217.3	192.168.	10.10	FTP	81 Request:	USER	bpear003	
		971 608.	469563600	192.168.	10.10	192.168.	217.3	FTP	100 Response:	331	Please specify the pas	sword
		999 619.	2485/1100	192.168.	217.3	192.168.	10.10	FTP	81 Request:	PASS	01243149	
	2	003 622.	050166300	192.168.	217.3	192.168.	10.10	FTP	72 Request:	SYST	Login incorrect.	
M	4											•
V	▶ Fra	me 1969:	81 bytes	on wire	(648 bit	s), 81 bytes	captured (6	48 bits)	on interface 0			
1	→ Eth	ernet II	, Src: Mi	.crosof_40):57:1e (00:15:5d:40:5	7:1e), Dst:	Microsof	_40:57:0c (00:1	5:5d:4	10:57:0c)	
	→ Int	ernet Pr nemissio	otocol Ve n Control	Protocol	Src: 192	2.168.217.3, D ort: 48960 Ds	st: 192.168	.10.10 Sec: 1	Ack: 21 Len: 1	5		
1	S	ource Po	ort: 48960)	., 510 10	JIC. 40000, D3		JUQ. 1,	AGK. 21, LUII. 1	5		
<u> </u>	D	estinati	on Port:	21								
	[Stream i	ndex: 132	2]								
•		ICP Segn	number:	15] (re]:	ative se	uence number)						
_	l ï	Next sea	uence nur	ber: 16	(relat	tive sequence	number)]					
, , ,	Ā	cknowled	lgment num	nber: 21	(relat	tive ack numbe	er)					
	1	000	= Header	Length:	32 bytes	s (8)						-
	0000	00 15 5	5d 40 57 (9c 00 15	5d 40 5	7 1e 08 00 45	10 ···]@W	···]@W··	٠E٠			
_	0010	00 43 a	11 eb 40 (90 3f 06	35 5b c	0 a8 d9 03 c0	a8 ·C··@·	? 5[
A	0020	00 e5 b	0 40 00 . 0 47 00 (15 a7 97 90 01 01	82 57 6 08 0a 4	a 71 bu bo 80 c a0 78 75 de	e8 ···@··	··· ·wj··	1			
-	0040	b1 8a 5	55 53 45	52 20 62	70 65 6	1 72 30 30 33	0d ∙ USEF	b pear00	93·			
	0050	0a								Acti	vate Windows	
										Go to	Settings to activate Windows.	

Internal FTP search shows the username and passwords being used.