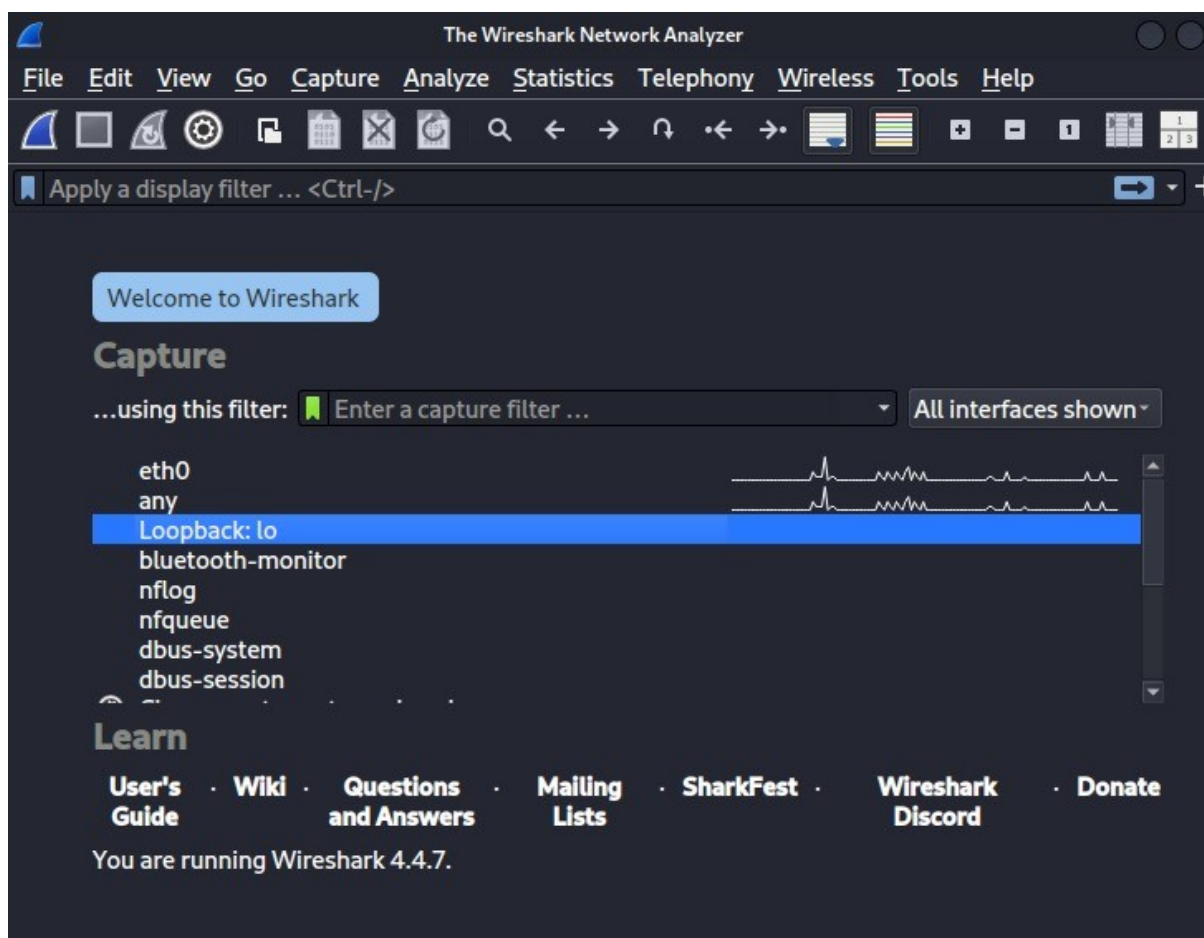


WIRESHARK



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.126.128	34.107.243.93	TLSv1.2	93	App l
2	0.000592351	34.107.243.93	192.168.126.128	TCP	60	443
3	0.001055580	192.168.126.128	34.107.243.93	TLSv1.2	78	App l
4	0.002051618	34.107.243.93	192.168.126.128	TCP	60	443
5	0.002114749	192.168.126.128	34.107.243.93	TCP	54	5388
6	0.002602443	34.107.243.93	192.168.126.128	TCP	60	443
7	0.052621843	34.107.243.93	192.168.126.128	TCP	60	443
8	0.052663315	192.168.126.128	34.107.243.93	TCP	54	5388
9	11.180404586	192.168.126.128	192.46.210.39	NTP	90	NTP

Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface eth0
Ethernet II, Src: VMware_e1:b1:d9 (00:0c:29:e1:b1:d9), Dst: 34:107:243:93 (08:00:27:10:72:43)
Internet Protocol Version 4, Src: 192.168.126.128, Dst: 34.107.243.93
Transmission Control Protocol, Src Port: 443, Dst Port: 443
Transport Layer Security

0000 00 50 56 ed 60 56 00 0c 29 e1 b1 d9
0010 00 4f 17 f0 40 00 40 06 cd c7 c0
0020 f3 5d d2 80 01 bb 4f d8 21 24 58
0030 f7 45 55 33 00 00 17 03 03 00 22
0040 b3 09 6a cc 39 85 57 af 67 c0 7b
0050 80 83 24 03 1c 4d 3c 63 43 90 d9



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :

Password :

You can also
Signup disabled

This connection is not secure.
Logins entered here could be
compromised. [Learn More](#)

password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

RESULT:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
http							
No.	Time	Source	Destination	Protocol	Length	Info	
138	207.463847972	34.36.137.203	192.168.126.128	TCP	60	443	
139	207.463882587	192.168.126.128	34.36.137.203	TLSv1.3	252	App	
140	207.464415864	34.36.137.203	192.168.126.128	TCP	60	443	
141	207.483198854	34.36.137.203	192.168.126.128	TLSv1.3	672	App	
142	207.483915380	192.168.126.128	34.36.137.203	TLSv1.3	85	App	
143	207.484693777	34.36.137.203	192.168.126.128	TCP	60	443	
144	207.497536596	34.36.137.203	192.168.126.128	TLSv1.3	85	App	
145	207.540743970	192.168.126.128	34.36.137.203	TCP	54	410	
146	207.759725248	34.36.137.203	192.168.126.128	TLSv1.3	2563	App	
147	207.759768867	192.168.126.128	34.36.137.203	TCP	54	410	
148	207.760508683	192.168.126.128	34.36.137.203	TLSv1.3	93	App	
149	207.760836832	34.36.137.203	192.168.126.128	TCP	60	443	
150	210.598204424	34.107.243.93	192.168.126.128	TLSv1.2	78	App	
151	210.598593877	192.168.126.128	34.107.243.93	TLSv1.2	82	App	
152	210.599426631	34.107.243.93	192.168.126.128	TCP	60	443	
153	210.894328126	192.168.126.128	192.46.210.39	NTP	90	NTP	
154	210.932962197	192.46.210.39	192.168.126.128	NTP	90	NTP	

Frame 1: 90 bytes on wire (720 bits), 60 bytes captured (480 bits) on interface 0	0000	00 50 56 ed 60 56 00 0c 29 e1 b1
Ethernet II, Src: VMware_e1:b1:d9 (00:0c:29:e1:b1:d9), Dst: 192.168.126.128 (08:00:27:d0:91:00)	0010	00 4c a8 b3 40 00 40 11 bf b6 c0
Internet Protocol Version 4, Src: 192.168.126.128, Dst: 192.46.210.39	0020	d2 27 d0 91 00 7b 00 38 d1 c8 23
User Datagram Protocol, Src Port: 53393, Dst Port: 123	0030	00 00 00 00 00 00 00 00 00 00 00
Network Time Protocol (NTP Version 4, Mode: Client)	0040	00 00 00 00 00 00 00 00 00 00 00
	0050	00 00 fc c9 fb 71 c6 0d 2e 90