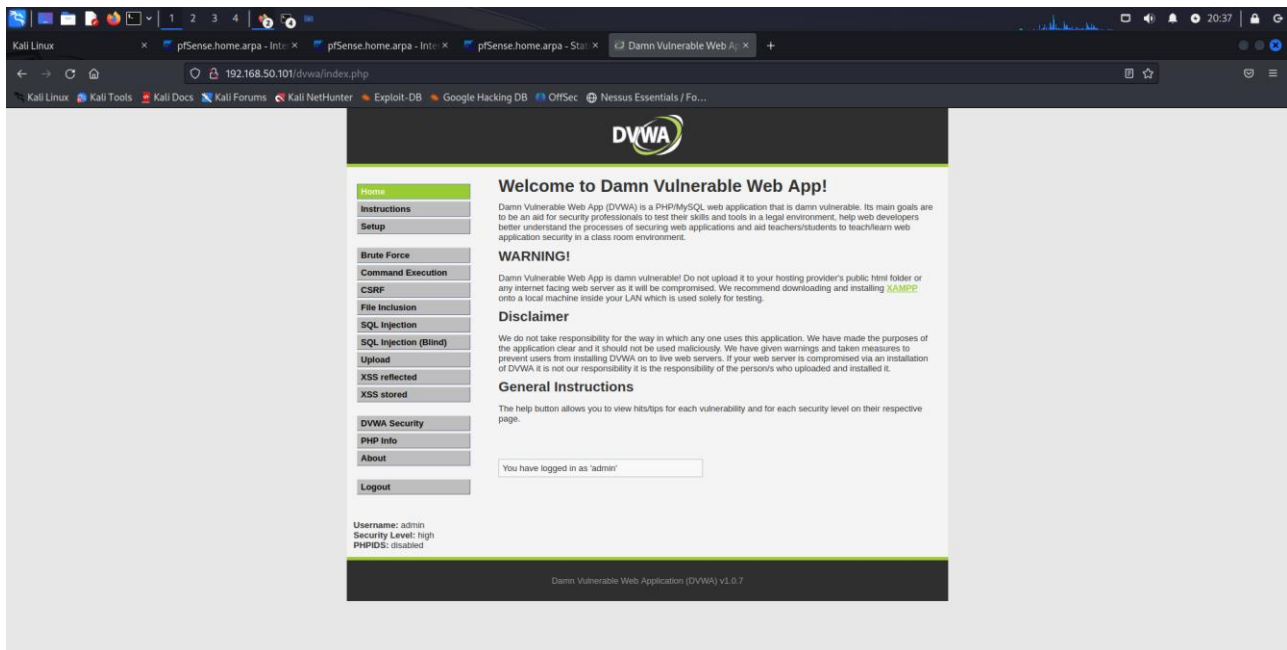
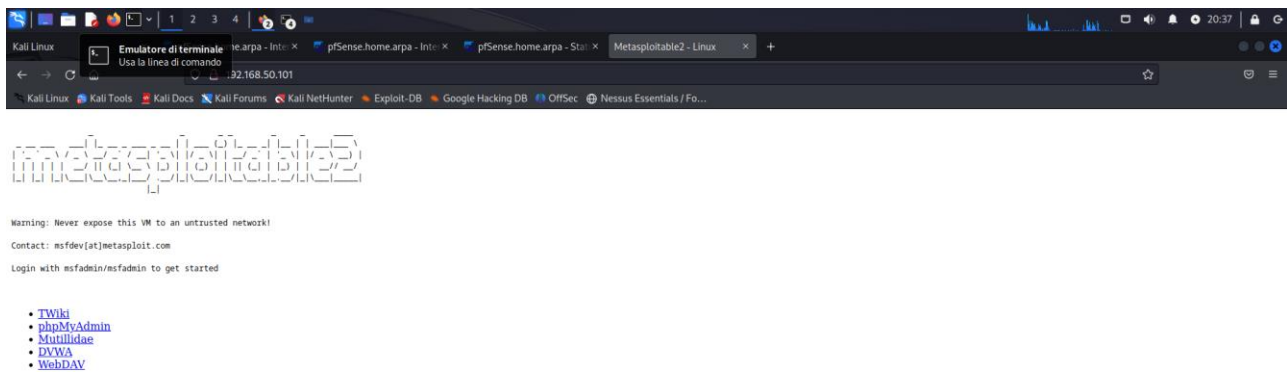


In questo screen si può vedere che Kali può accedere alla DVWA



Qui vediamo i pacchetti che passano durante la connessione sulla DVWA

Kali Linux

Firefox ESR
Esplora il web

pfSense.home.arpa - Int...
pfSense.home.arpa - Sta...
pfSense.home.arpa - Sta...
Dann Vulnerable Web A...
any

File Modifica Visualizza Vai Cattura Analisi Statistiche Telefonia Wireless Strumenti Aiuto

Applica un filtro di visualizzazione... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
82	8.017783275	192.168.1.100	192.168.50.1	TLSv1.2	194	Application Data
83	8.018001541	192.168.50.1	192.168.1.100	TCP	68	443 - 33914 [ACK] Seq=5488 Ack=1376 Win=514 Len=0 TSval=467177320 TSecr=2000224379
84	8.018001701	192.168.50.1	192.168.1.100	TCP	68	443 - 33914 [ACK] Seq=5488 Ack=1502 Win=514 Len=0 TSval=467177320 TSecr=2000224379
85	8.018203999	192.168.50.1	192.168.1.100	TLSv1.2	103	Application Data
86	8.019214524	192.168.1.100	192.168.50.1	TCP	68	33914 - 443 [ACK] Seq=1502 Ack=5523 Win=3967 Len=0 TSval=2000224379 TSecr=467177320
87	8.049624004	192.168.50.1	192.168.1.100	TLSv1.2	533	Application Data
88	8.049661775	192.168.1.100	192.168.50.1	TCP	68	33914 - 443 [ACK] Seq=1502 Ack=5988 Win=3967 Len=0 TSval=2000224411 TSecr=467177351
89	8.787140501	192.168.1.100	192.168.50.101	ICMP	100	Echo (ping) request id=8x3820, seq=349/23809, ttl=64 (reply in 90)
90	8.787557254	192.168.50.101	192.168.1.100	ICMP	100	Echo (ping) reply id=8x3820, seq=349/23809, ttl=63 (request in 89)
91	9.086037400	192.168.1.100	192.168.50.101	ICMP	100	Echo (ping) request id=8x3820, seq=350/24065, ttl=64 (reply in 92)
92	9.086454117	192.168.50.101	192.168.1.100	ICMP	100	Echo (ping) reply id=8x3820, seq=350/24065, ttl=63 (request in 91)
93	10.020122978	192.168.1.100	192.168.50.1	TLSv1.2	100	Application Data
94	10.020175102	192.168.1.100	192.168.50.1	TLSv1.2	195	Application Data
95	10.020400840	192.168.50.1	192.168.1.100	TCP	68	443 - 33914 [ACK] Seq=5988 Ack=1594 Win=514 Len=0 TSval=467179323 TSecr=2000226381
96	10.020400900	192.168.50.1	192.168.1.100	TCP	68	443 - 33914 [ACK] Seq=5988 Ack=1721 Win=514 Len=0 TSval=467179323 TSecr=2000226381
97	10.020640781	192.168.50.1	192.168.1.100	TLSv1.2	103	Application Data
98	10.020657146	192.168.1.100	192.168.50.1	TCP	68	33914 - 443 [ACK] Seq=1721 Ack=6023 Win=3967 Len=0 TSval=2000226382 TSecr=467179323
99	10.020622948	192.168.50.1	192.168.1.100	TLSv1.2	972	Application Data
100	10.02040405	192.168.1.100	192.168.50.1	TCP	68	33914 - 443 [ACK] Seq=1721 Ack=6927 Win=3967 Len=0 TSval=2000226390 TSecr=467179331

Frame 1: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface a
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.50.1
Transmission Control Protocol, Src Port: 33914, Dst Port: 443, Seq: 1, Ack: 1, Len: 7
Transport Layer Security

0000 00 04 00 01 00 06 08 00 27 83 29 12 00 00 08 00
0010 45 00 00 01 29 3e 40 00 40 06 5c 83 c0 a8 01 64
0020 c0 a8 32 01 84 7a 01 b5 d7 c4 4b e7 2f 98 a1 00
0030 80 1b 0f 7f b5 29 00 00 01 01 08 0a 77 3b c1 29
0040 1b d8 6c 2d 17 03 03 00 48 c4 90 9c 5a 0a 27 85
0050 3c fb ed 61 fe 4f 5a 09 11 90 90 67 02 1a eb 05
0060 06 03 06 05 19 7c 03 0a e7 ba fa 99 3a 07 40 85
0070 6f 9f c7 86 d9 2d cb 7f 04 59 a2 e9 71 ce 42 28
0080 d3 b8 50 a6 8b 4c f6 91 dc c6 c1 07 94 99 50 80
0090 00

wireless_arkanyCBJR31.pcapng

Pacchetti: 100 - visualizzati: 100 (100.0%)

Profilo: Default

Configurando questa regola sul firewall di pfsense osserviamo che la DVWA non è più raggiungibile da browser

The image consists of two screenshots from a Kali Linux system. The top screenshot shows the pfSense web interface for configuring firewall rules on the LAN interface. A yellow notification bar at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." Below this, the "Rules (Drag to Change Order)" table is visible. It contains three rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓ 0/262 KiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/> ✗ 0/0 B	IPv4 TCP	192.168.1.100	*	192.168.50.101	*	*	none			
<input type="checkbox"/> ✓ 1/2.85 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> ✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom of the table are buttons for "Add", "Delete", "Save", and "Separator".

The bottom screenshot shows a web browser window with the address bar set to "192.168.50.101". The page content displays a "Timed Out" error:

The connection has timed out

The server at 192.168.50.101 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

A "Try Again" button is located at the bottom right of the error message.

A seguire la scansione su wireshark

The image shows a Wireshark capture of network traffic on a Kali Linux system. The capture is filtered by the IP address 192.168.50.101. The packet list on the left shows a series of TCP and ICMP packets. The selected packet (No. 153) is an ICMP Echo (ping) request from 192.168.50.101 to 192.168.1.100. The packet details pane on the right shows the structure of the ICMP Echo request, including the type (8), code (0), and identifier (0x3820). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
145	17.031963587	192.168.1.100	192.168.50.1	TLSv1.2	200	Application Data
146	17.032207975	192.168.50.1	192.168.1.100	TCP	68	443 -> 33914 [ACK] Seq=11932 Ack=2911 Win=514 Len=0 TSval=467369677 TSecr=2000416643
147	17.032208145	192.168.50.1	192.168.1.100	TCP	68	443 -> 33914 [ACK] Seq=11932 Ack=3043 Win=513 Len=0 TSval=467369677 TSecr=2000416643
148	17.032408505	192.168.50.1	192.168.1.100	TLSv1.2	103	Application Data
149	17.032410730	192.168.1.100	192.168.50.1	TCP	68	33914 -> 443 [ACK] Seq=3043 Ack=11967 Win=3967 Len=0 TSval=2000416644 TSecr=467369677
150	17.046760251	192.168.50.1	192.168.1.100	TLSv1.2	1338	Application Data
151	17.046760707	192.168.1.100	192.168.50.1	TCP	68	33914 -> 443 [ACK] Seq=3043 Ack=13237 Win=3967 Len=0 TSval=2000416650 TSecr=467369691
152	17.404150911	192.168.1.100	192.168.50.101	ICMP	100	Echo (ping) request id=0x3820, seq=536/6146, ttl=64 (reply in 153)
153	17.404500448	192.168.50.101	192.168.1.100	ICMP	100	Echo (ping) reply id=0x3820, seq=536/6146, ttl=63 (request in 152)
154	18.033599890	192.168.1.100	192.168.50.1	TLSv1.2	145	Application Data
155	18.033645417	192.168.1.100	192.168.50.1	TLSv1.2	194	Application Data
156	18.033893272	192.168.50.1	192.168.1.100	TCP	68	443 -> 33914 [ACK] Seq=13237 Ack=3120 Win=514 Len=0 TSval=467370679 TSecr=2000417645
157	18.033893312	192.168.50.1	192.168.1.100	TCP	68	443 -> 33914 [ACK] Seq=13237 Ack=3246 Win=514 Len=0 TSval=467370679 TSecr=2000417645
158	18.034176041	192.168.50.1	192.168.1.100	TLSv1.2	103	Application Data
159	18.034180464	192.168.1.100	192.168.50.1	TCP	68	33914 -> 443 [ACK] Seq=3246 Ack=13272 Win=3967 Len=0 TSval=2000417646 TSecr=467370679
160	18.067091309	192.168.50.1	192.168.1.100	TLSv1.2	532	Application Data
161	18.067124953	192.168.1.100	192.168.50.1	TCP	68	33914 -> 443 [ACK] Seq=3246 Ack=13736 Win=3967 Len=0 TSval=2000417678 TSecr=467370711
162	18.427900116	192.168.1.100	192.168.50.101	ICMP	100	Echo (ping) request id=0x3820, seq=537/6402, ttl=64 (reply in 163)
163	18.428306205	192.168.50.101	192.168.1.100	ICMP	100	Echo (ping) reply id=0x3820, seq=537/6402, ttl=63 (request in 162)

Frame 153: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface a
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.50.101, Dst: 192.168.1.100
Internet Control Message Protocol

0000 00 00 00 01 00 00 08 00 27 45 bc 02 00 00 08 00 ... 'P ...
0010 45 00 00 54 55 33 00 00 3f 01 71 5c c0 a8 32 65 ... E T U 3 ? q \ 2e
0020 c0 a8 01 64 00 00 eb 5a 38 20 02 18 99 d9 42 64 ... d Z 8 B d
0030 00 00 00 00 33 5c 0c 00 00 00 00 00 10 11 12 13 ... 3 \
0040 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 ! *
0050 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 ... \$ % ' () * + , - . / 0 1 2 3
0060 34 35 36 37 4567