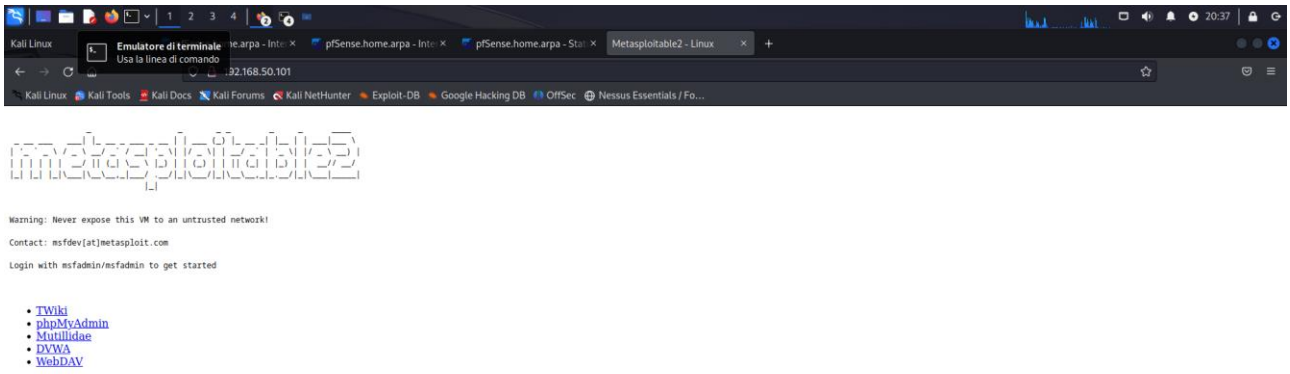
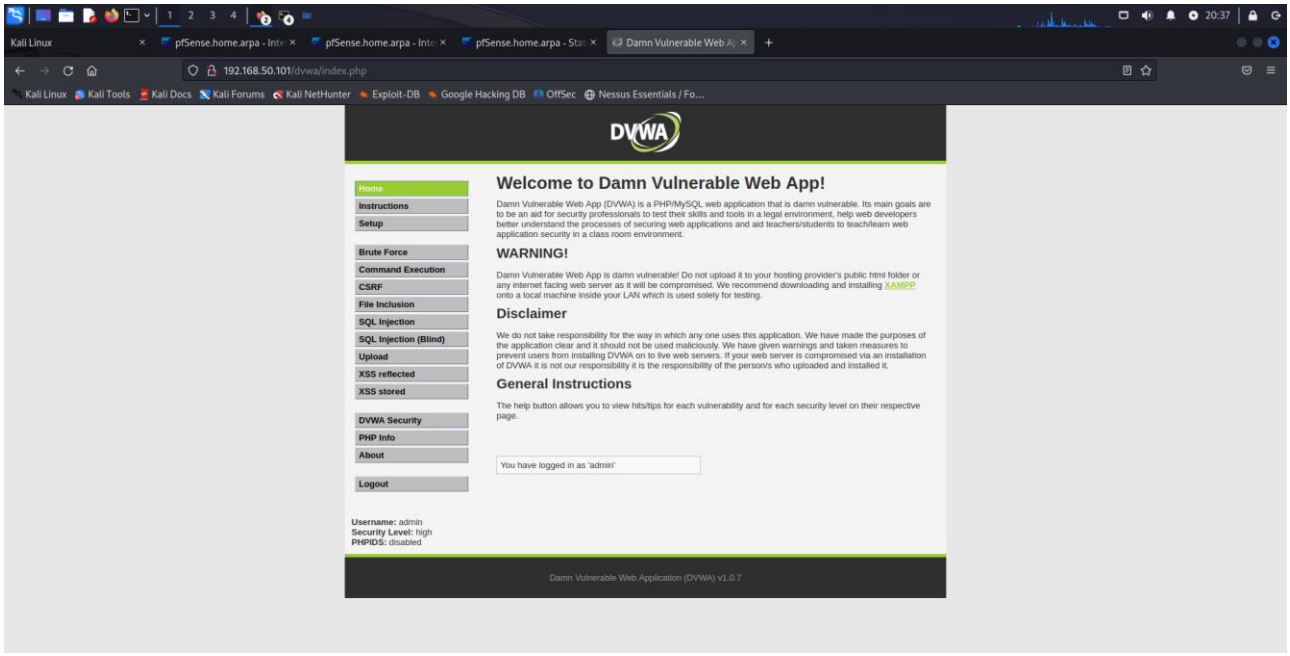
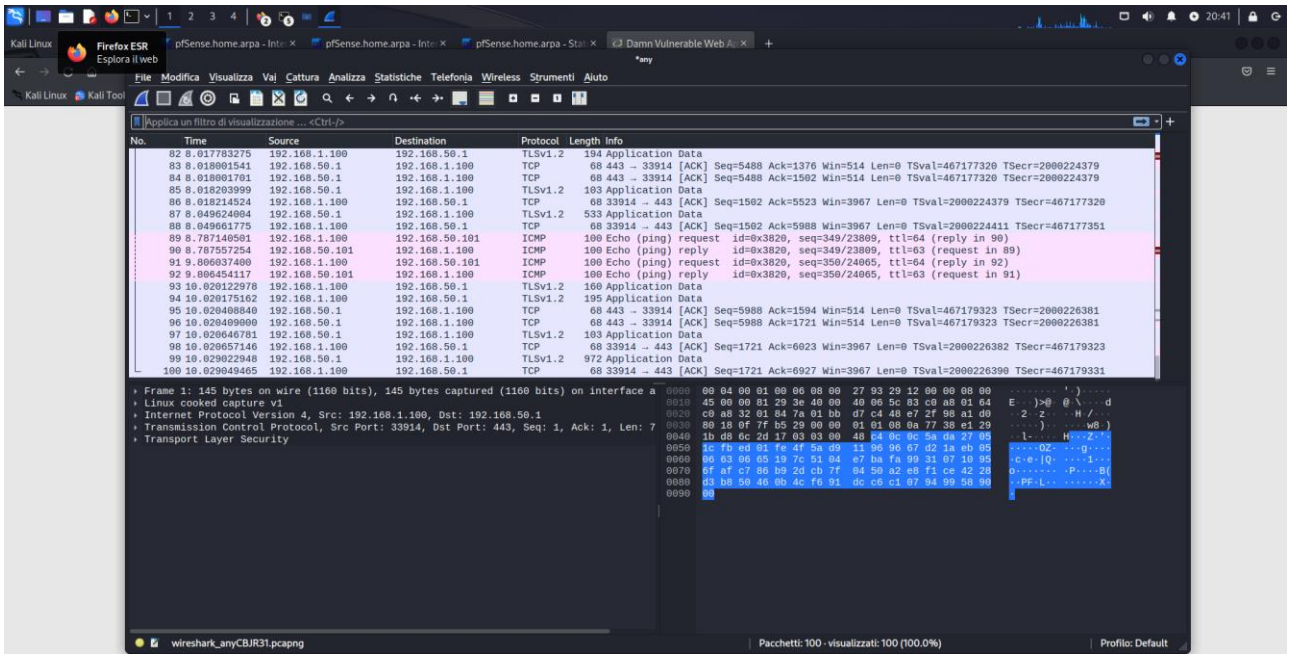
In questo screen si può vedere che Kali può accedere alla DVWA

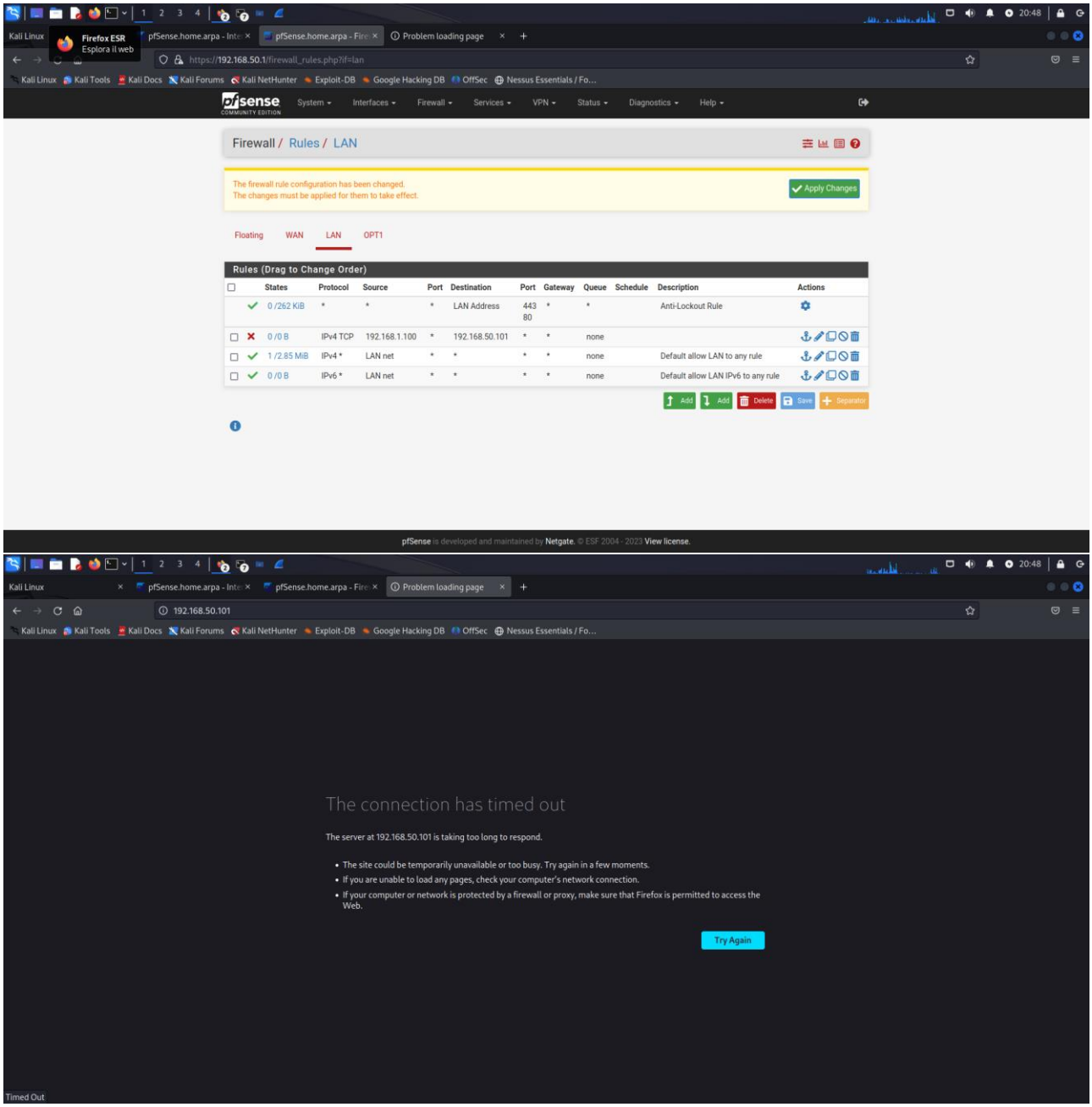




Qui vediamo i pacchetti che passano durante la connessione sulla DVWA


Kali Linux
Firefox ESR
Esplora il web
pfSense.home.arpa - Inte
pfSense.home.arpa - Inte
pfSense.home.arpa - Stat
Damn Vulnerable Web Ap
*any
File Modifica Visualizza Vai Cattura Analizza Statistiche Telefonia Wireless Strumenti Aiuto
Applica un filtro di visualizzazione ... <Ctrl-/>
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 8.018214524 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=0x3820, 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=0x3820, seq=349/23809, ttl=63 (request in 89)
91 9.806037400 192.168.1.100 192.168.50.101 ICMP 100 Echo (ping) request id=0x3820, seq=350/24065, ttl=64 (reply in 92)
92 9.806454117 192.168.50.101 192.168.1.100 ICMP 100 Echo (ping) reply id=0x3820, seq=350/24065, ttl=63 (request in 91)
93 10.020122978 192.168.1.100 192.168.50.1 TLSv1.2 160 Application Data
94 10.020175162 192.168.1.100 192.168.50.1 TLSv1.2 195 Application Data
95 10.020408840 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 10.020409000 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 10.020646781 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 10.029022948 192.168.50.1 192.168.1.100 TLSv1.2 972 Application Data
100 10.029049465 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 93 29 12 00 00 08 00
0010 45 00 00 81 29 3e 40 00 40 06 5c 83 c0 a8 01 64
0020 c0 a8 32 01 84 7a 01 bb d7 c4 48 e7 2f 98 a1 d0
0030 80 18 0f 7f b5 29 00 00 01 01 08 0a 77 38 e1 29
0040 1b d8 6c 2d 17 03 03 00 48 64 0c 0c 5a da 27 05
0050 1c fb ed 01 fe 4f 5a d9 11 96 96 67 d2 1a eb 05
0060 06 63 06 65 19 7c 51 04 e7 ba fa 99 31 07 10 95
0070 6f af c7 86 b9 2d cb 7f 04 50 a2 e8 f1 ce 42 28
0080 d3 b8 50 46 0b 4c f6 91 dc c6 c1 07 94 99 58 90
0090 00
wireshark_anyCBJR31.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



A seguire la scansione su wireshark