Workshop 1 : Preparation of the working environment and analysis of vulnerabilities

Goals

- Download and install Kali Linux on your PC.
- Install and download Nessus Tenable.
- Use some network scanning tools.
- Understand the procedures for identifying and remediating vulnerabilities.

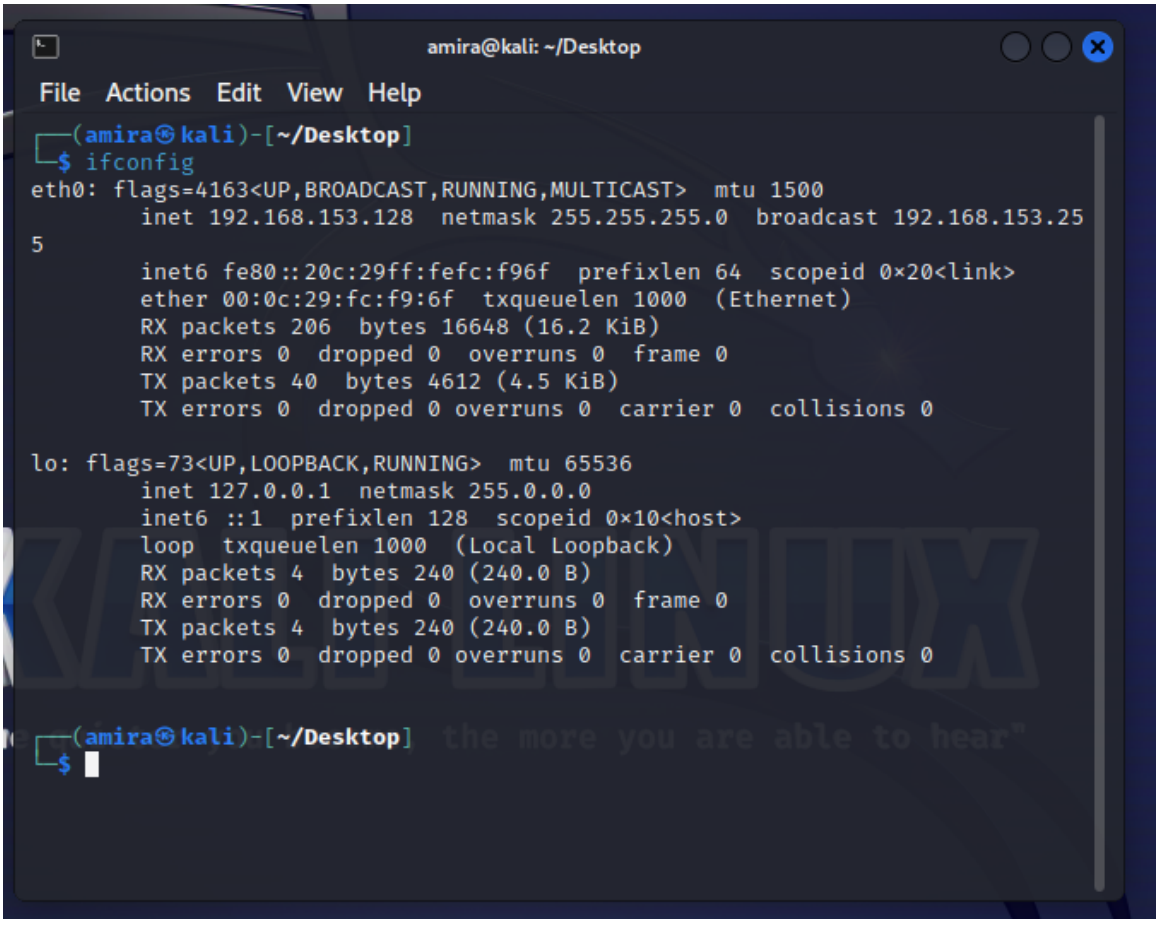
Part 1: Preparing the environment

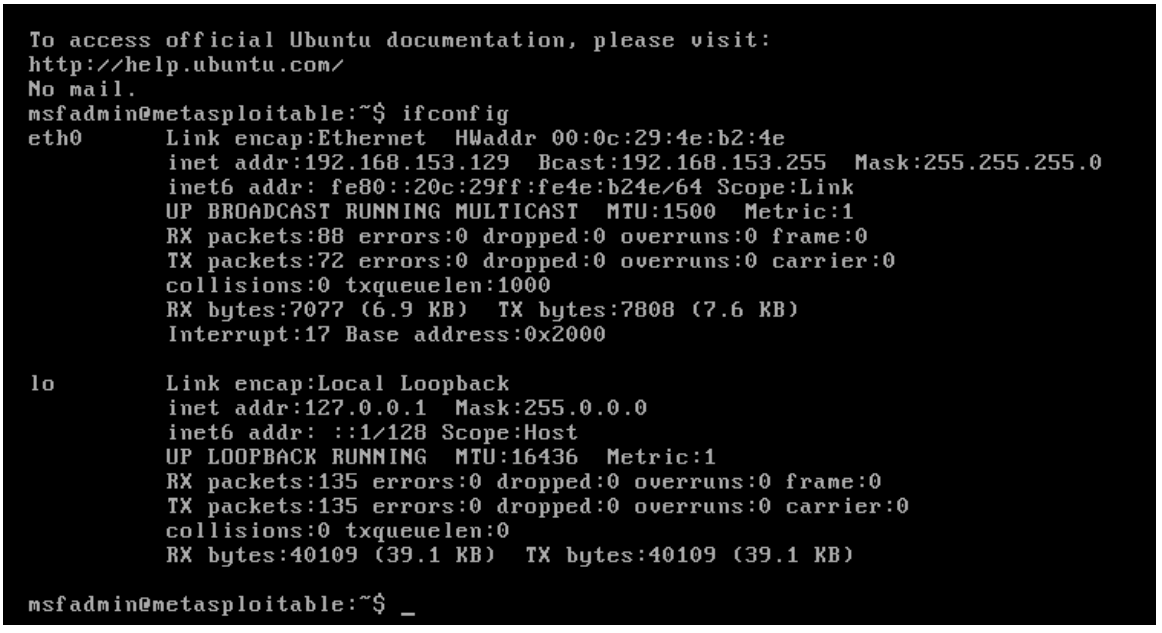
- [x] ~~1. Download and install Vmware~~
- [x] ~~2.Download and install Kali Linux machine~~
- [x] ~~3.Download and install Nessus Tenable~~
- [x] ~~4.Download and start the Metasploitable2 VM~~

Part 2: Nmap Scan

Nmap is an open source port scanner. It detects open ports, services hosted and information about the operating system of a target computer.

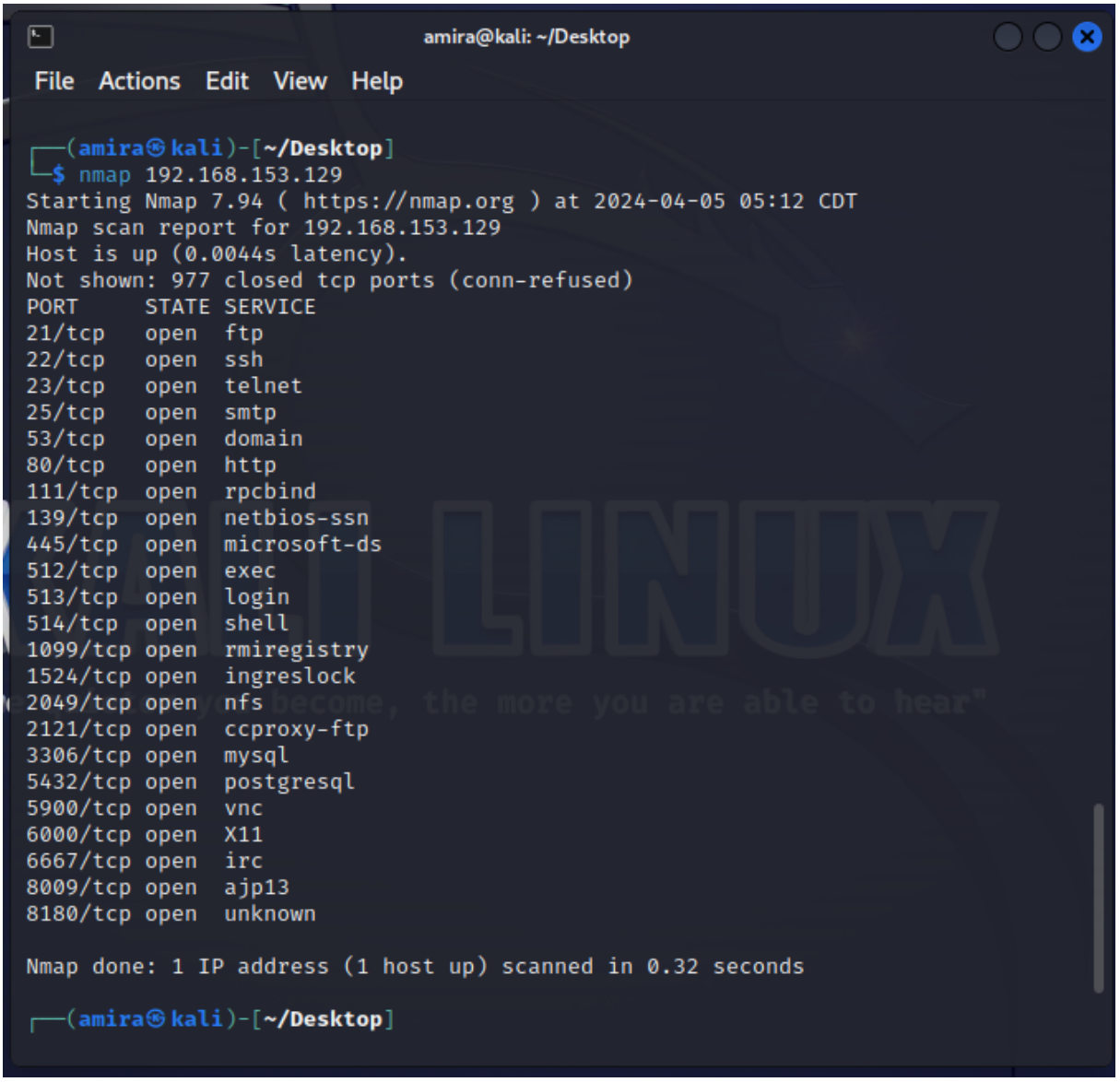
1. Run a quick machine scan. Use the "Ifconfig" command to get the IP address and network mask.



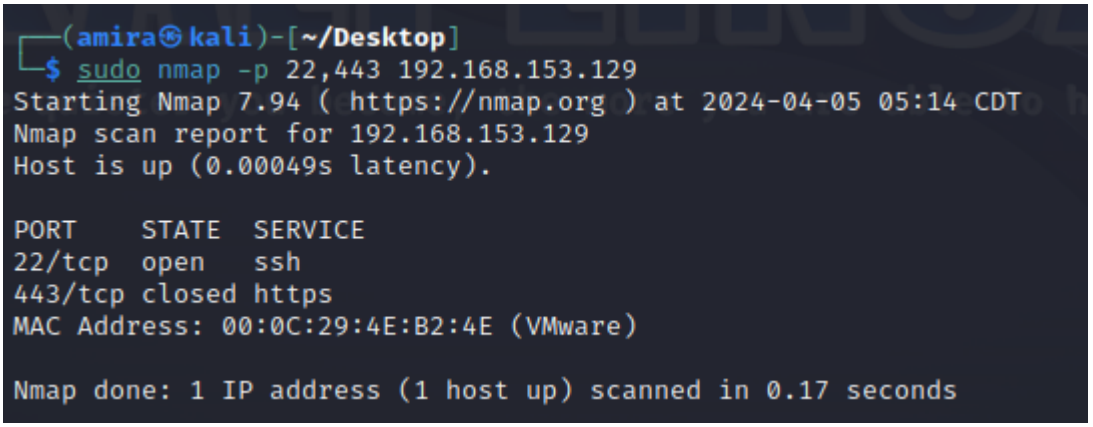


2.Identify the operating systems of a target machine.

3.Scan all ports of a target machine.

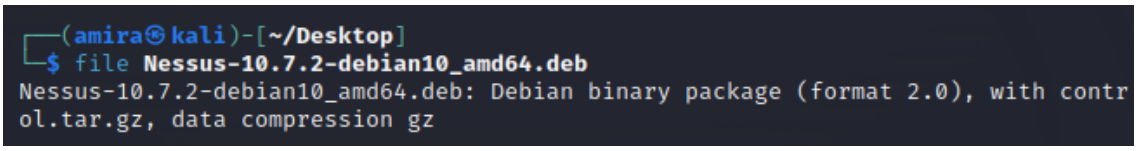


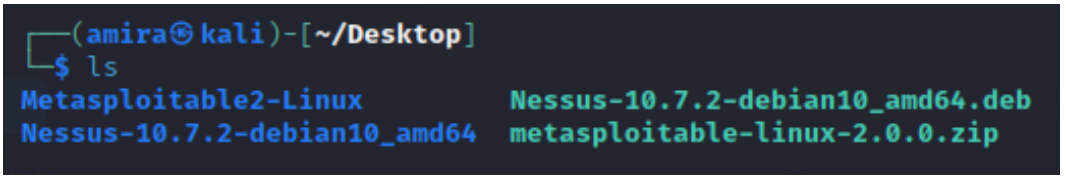
4.Check the status of ports 22 and 443 on network machines.



Part 3: Nessus Vulnerability Scanner on Kali Linux

1.Download the package and confirm that it is locally available for installation.

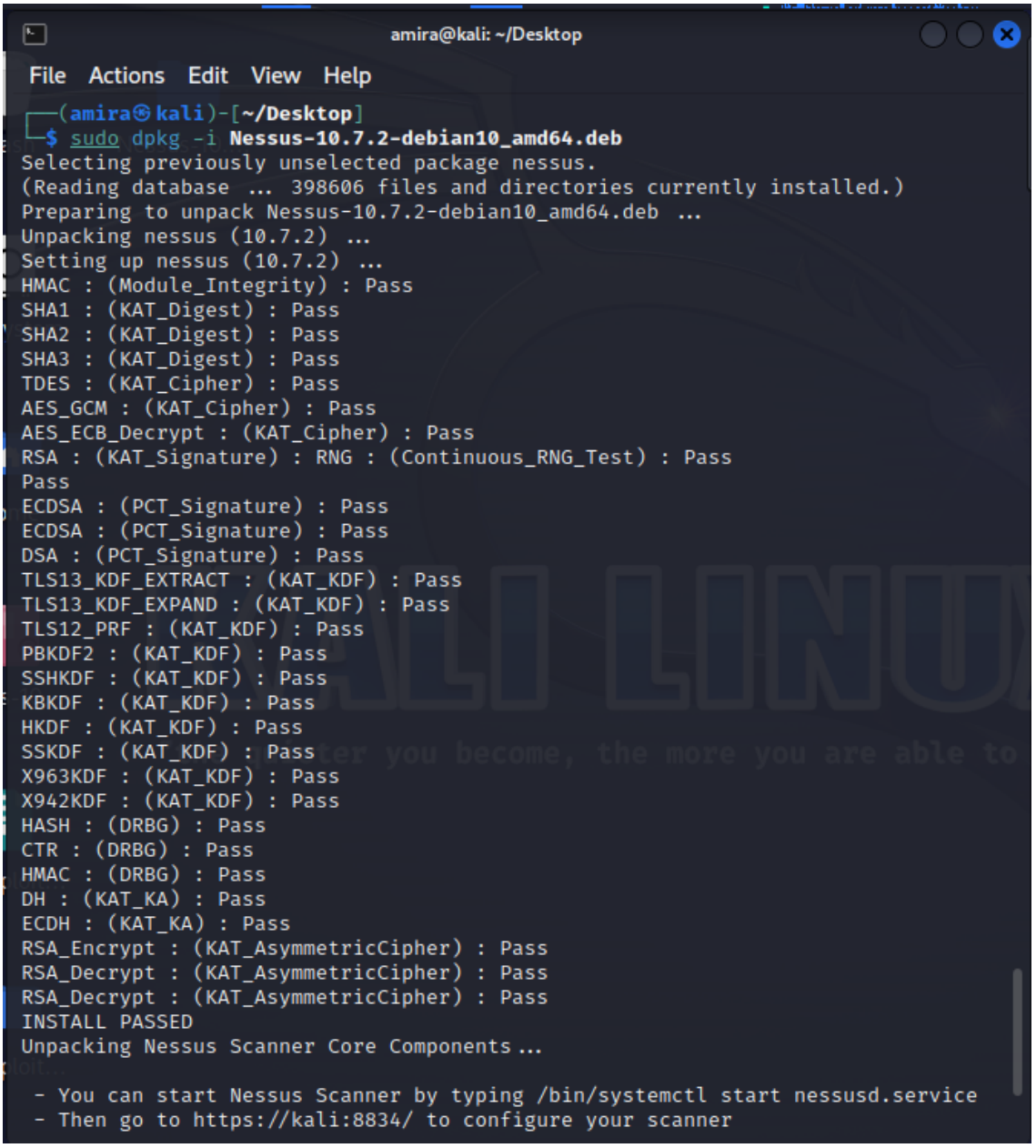




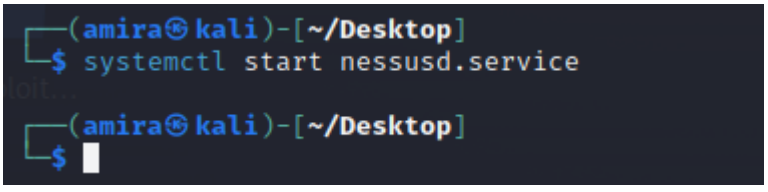
2.Install Nessus Vulnerability scanner on Kali Linux the command below:

cd /home/kali/Downloads/

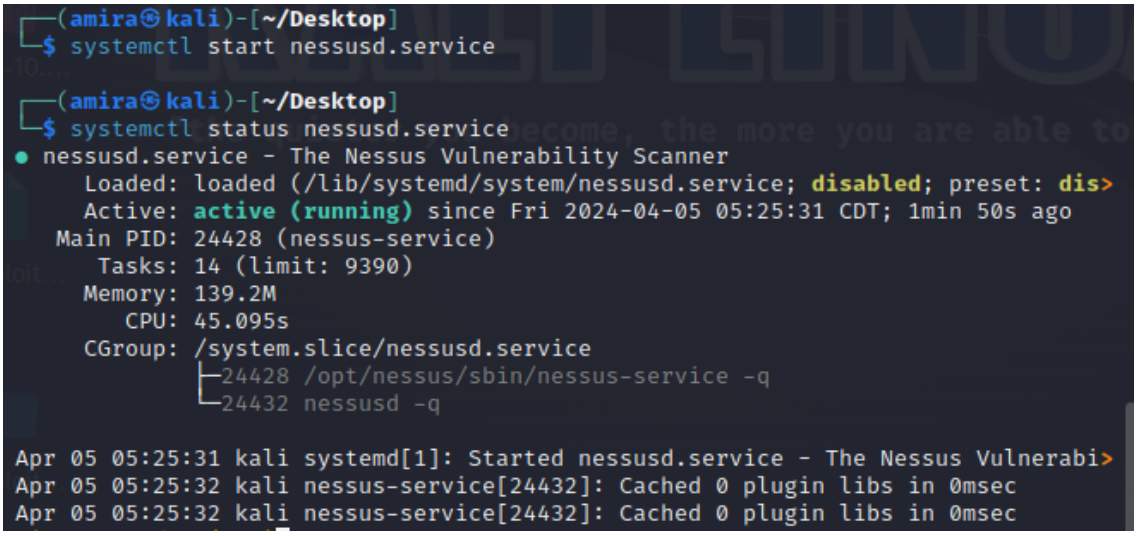
sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb



3.Start the service required to run Nessus vulnerability scanner.

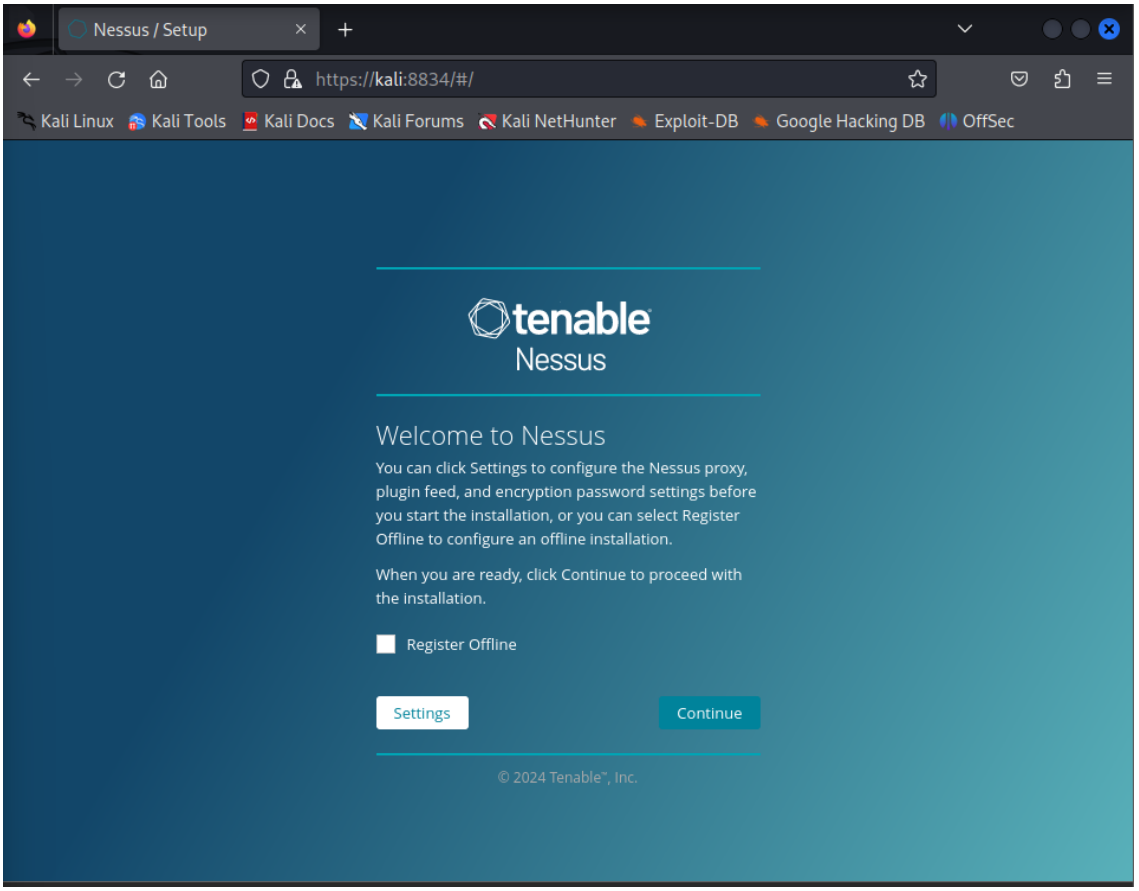


4.Confirm that nessusd is started and running

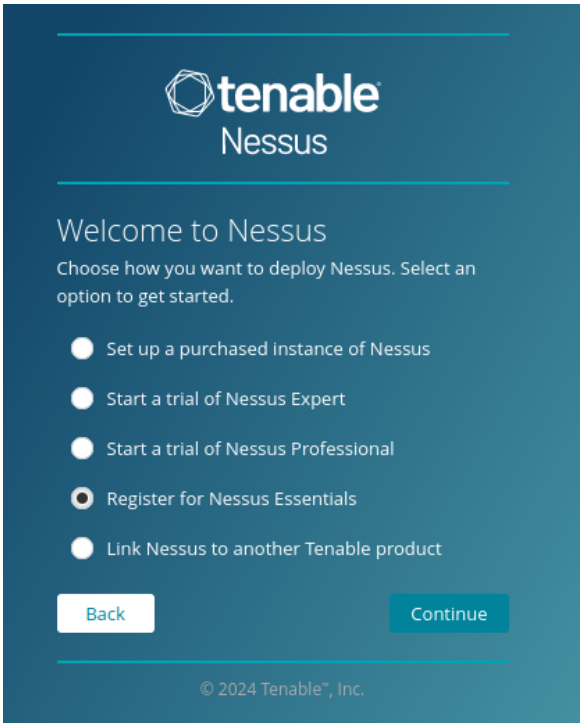


5.Visit your Nessus web interface on your server IP address, hostname port 8834 to complete Nessus installation and activation.

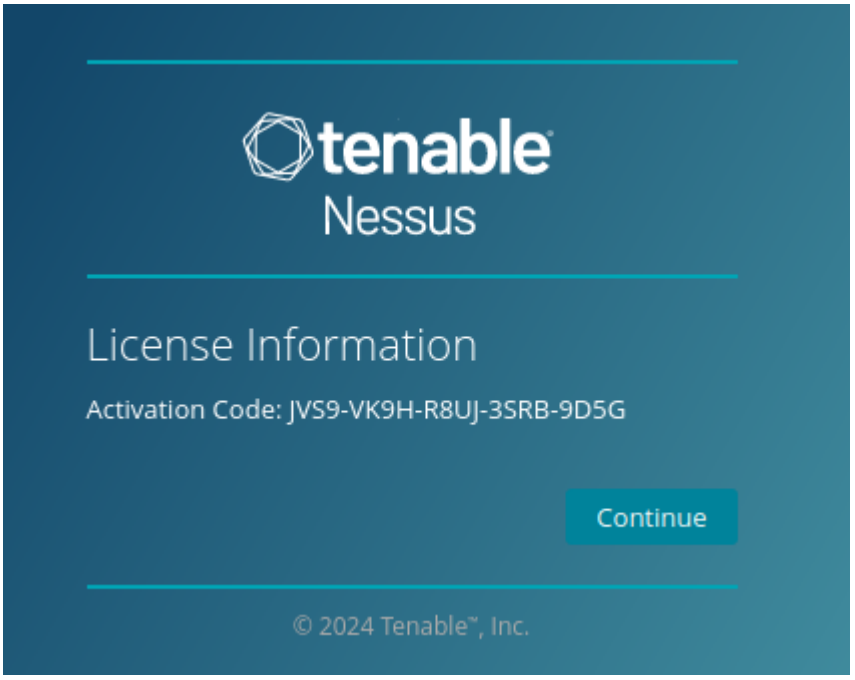
https://kali:8834/



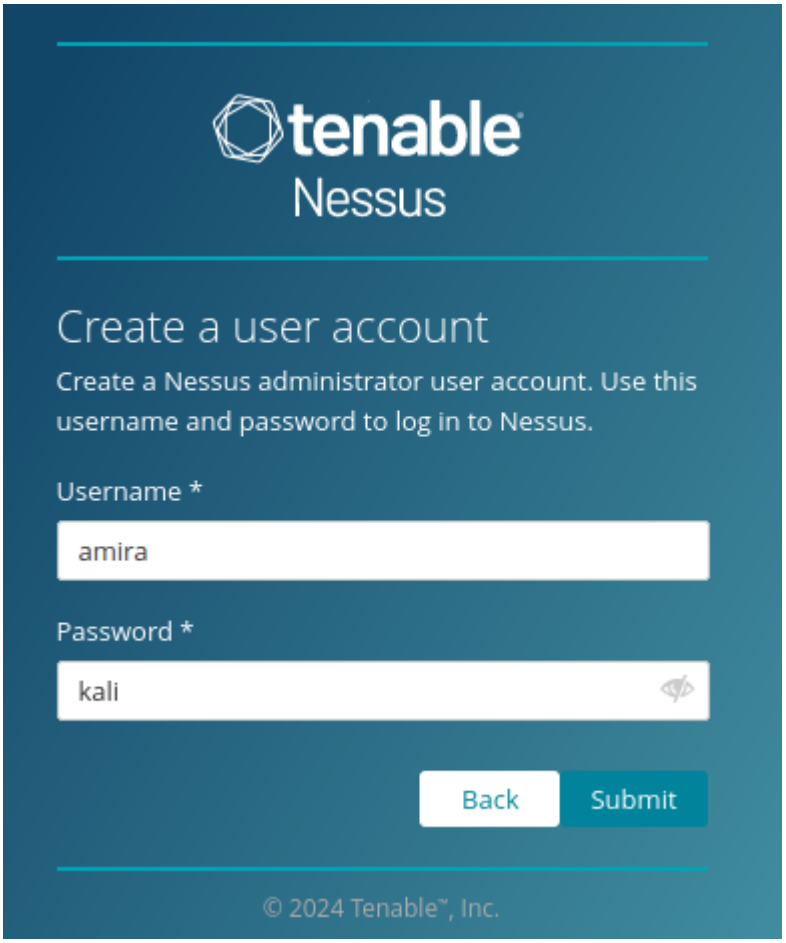
6.Activate product: Nessus Essentials license



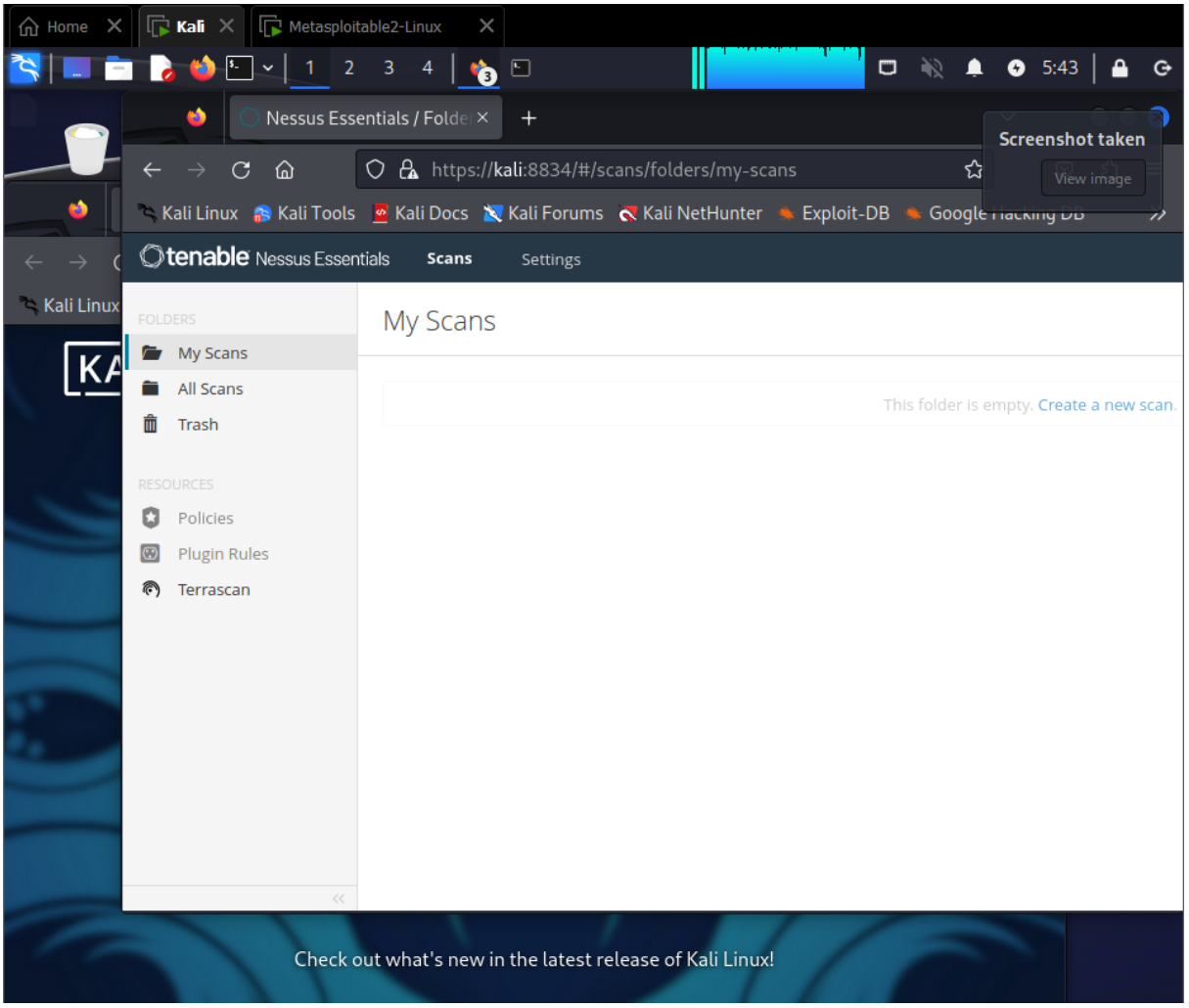
7. Register Nessus now by entering the activation code received by email.
JVS9-VK9H-R8UJ-3SRB-9D5G



8.Create a Nessus administrator account



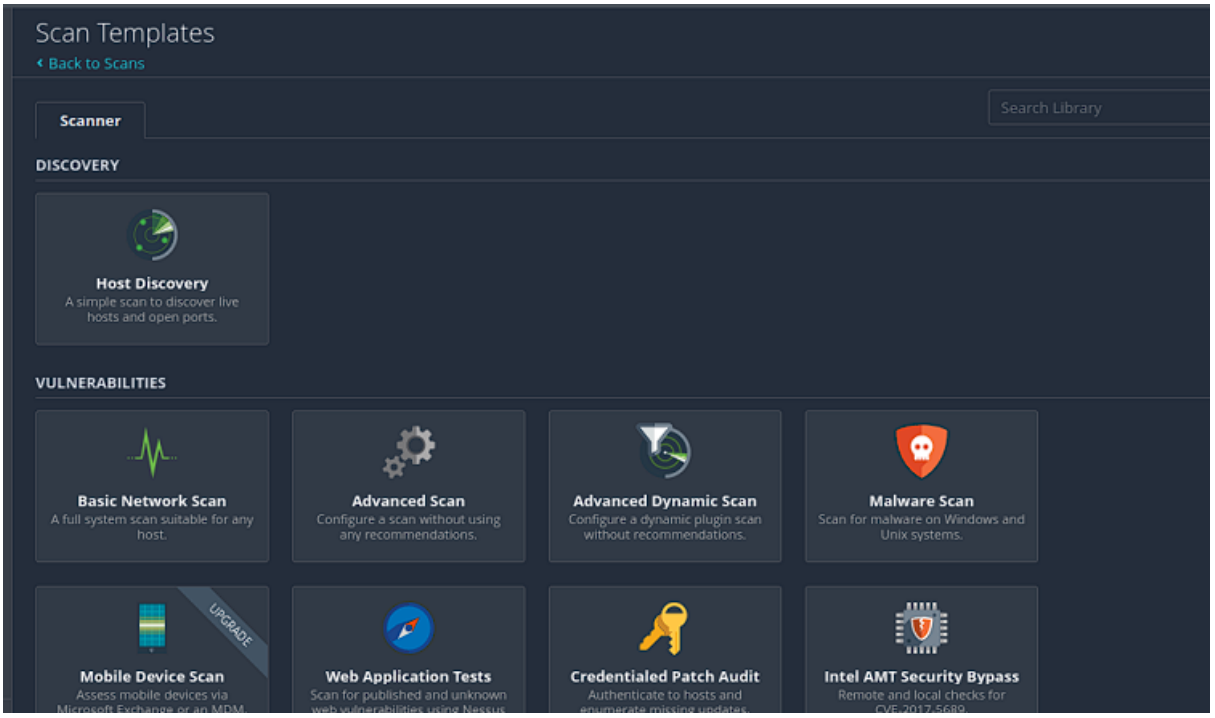
9.The default Nessus page when logging in should look like the one below:

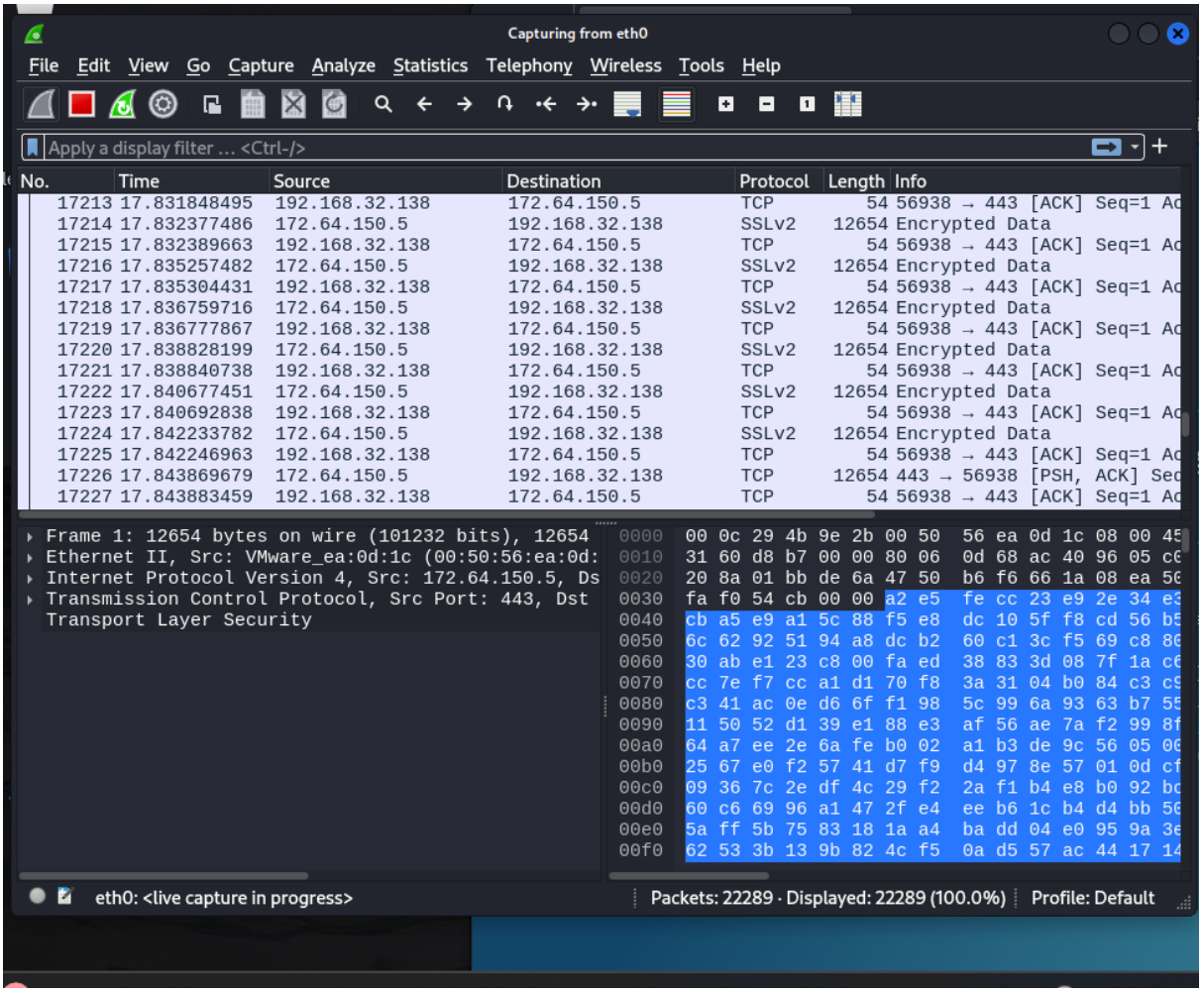


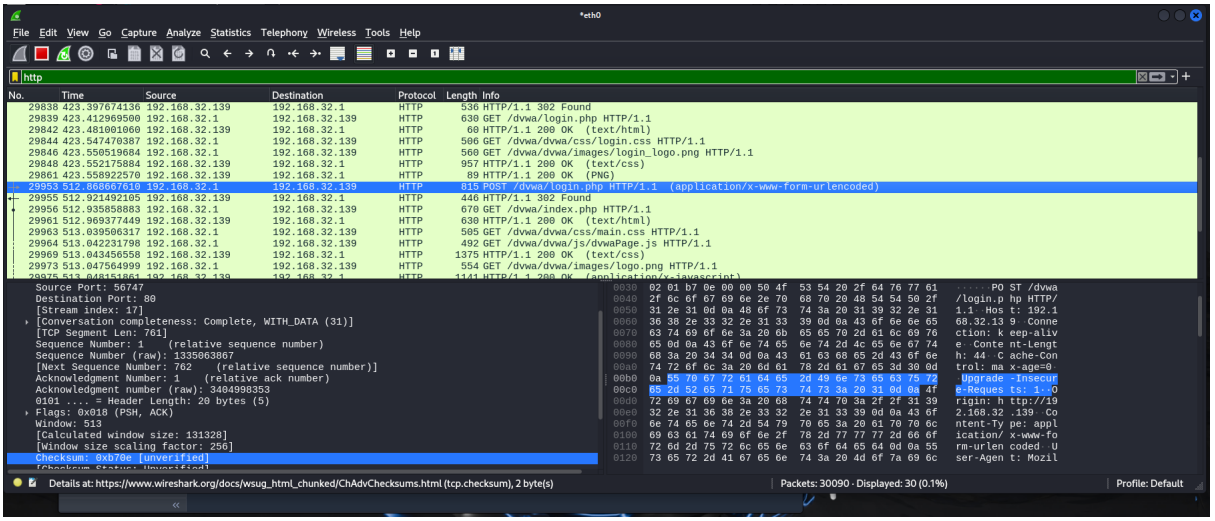
Part 4: Run a Nessus Vulnerability Scan

To create an agent analysis:

1. From the top navigation bar, choose Scans.
2. Choose the New scan.
3. Click on the scan template you want to use.
4. Configure scan settings.
5. Scan immediately: Nessus saves and starts the scan


Scan Templates
Back to Scans
Scanner
Search Library
DISCOVERY
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.
UPGRADE
Mobile Device Scan
Assess mobile devices via
Web Application Tests
Scan for published and unknown
Credentialed Patch Audit
Authenticate to hosts and
Intel AMT Security Bypass
Remote and local checks for


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
17213 17.831848495 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
17214 17.832377486 172.64.150.5 192.168.32.138 SSLv2 12654 Encrypted Data
17215 17.832389663 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
17216 17.835257482 172.64.150.5 192.168.32.138 SSLv2 12654 Encrypted Data
17217 17.835304431 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
17218 17.836759716 172.64.150.5 192.168.32.138 SSLv2 12654 Encrypted Data
17219 17.836777867 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
17220 17.838828199 172.64.150.5 192.168.32.138 SSLv2 12654 Encrypted Data
17221 17.838840738 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
17222 17.840677451 172.64.150.5 192.168.32.138 SSLv2 12654 Encrypted Data
17223 17.840692838 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
17224 17.842233782 172.64.150.5 192.168.32.138 SSLv2 12654 Encrypted Data
17225 17.842246963 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
17226 17.843869679 172.64.150.5 192.168.32.138 TCP 12654 443 → 56938 [PSH, ACK] Seq
17227 17.843883459 192.168.32.138 172.64.150.5 TCP 54 56938 → 443 [ACK] Seq=1 Ac
Frame 1: 12654 bytes on wire (101232 bits), 12654
Ethernet II, Src: VMware_ea:0d:1c (00:50:56:ea:0d:
Internet Protocol Version 4, Src: 172.64.150.5, Ds
Transmission Control Protocol, Src Port: 443, Dst
Transport Layer Security
0000 00 0c 29 4b 9e 2b 00 50 56 ea 0d 1c 08 00 45
0010 31 60 d8 b7 00 00 80 06 0d 68 ac 40 96 05 c0
0020 20 8a 01 bb de 6a 47 50 b6 f6 66 1a 08 ea 50
0030 fa f0 54 cb 00 00 a2 e5 fe cc 23 e9 2e 34 e3
0040 cb a5 e9 a1 5c 88 f5 e8 dc 10 5f f8 cd 56 b5
0050 6c 62 92 51 94 a8 dc b2 60 c1 3c f5 69 c8 86
0060 30 ab e1 23 c8 00 fa ed 38 83 3d 08 7f 1a c0
0070 cc 7e f7 cc a1 d1 70 f8 3a 31 04 b0 84 c3 c9
0080 c3 41 ac 0e d6 6f f1 98 5c 99 6a 93 63 b7 55
0090 11 50 52 d1 39 e1 88 e3 af 56 ae 7a f2 99 8f
00a0 64 a7 ee 2e 6a fe b0 02 a1 b3 de 9c 56 05 00
00b0 25 67 e0 f2 57 41 d7 f9 d4 97 8e 57 01 0d cf
00c0 09 36 7c 2e df 4c 29 f2 2a f1 b4 e8 b0 92 bc
00d0 60 c6 69 96 a1 47 2f e4 ee b6 1c b4 d4 bb 56
00e0 5a ff 5b 75 83 18 1a a4 ba dd 04 e0 95 9a 3e
00f0 62 53 3b 13 9b 82 4c f5 0a d5 57 ac 44 17 14
eth0: <live capture in progress>
Packets: 22289 · Displayed: 22289 (100.0%)
Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
29838 423.397674136 192.168.32.139 192.168.32.1 HTTP 536 HTTP/1.1 302 Found
29839 423.412969500 192.168.32.1 192.168.32.139 HTTP 630 GET /dvwa/login.php HTTP/1.1
29842 423.481001060 192.168.32.139 192.168.32.1 HTTP 60 HTTP/1.1 200 OK (text/html)
29844 423.547470387 192.168.32.1 192.168.32.139 HTTP 506 GET /dvwa/dvwa/css/login.css HTTP/1.1
29846 423.550519684 192.168.32.1 192.168.32.139 HTTP 560 GET /dvwa/dvwa/images/login_logo.png HTTP/1.1
29848 423.552175884 192.168.32.139 192.168.32.1 HTTP 957 HTTP/1.1 200 OK (text/css)
29861 423.558922570 192.168.32.139 192.168.32.1 HTTP 89 HTTP/1.1 200 OK (PNG)
29953 512.868667610 192.168.32.1 192.168.32.139 HTTP 815 POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
29955 512.921492105 192.168.32.139 192.168.32.1 HTTP 446 HTTP/1.1 302 Found
29956 512.935858883 192.168.32.1 192.168.32.139 HTTP 670 GET /dvwa/index.php HTTP/1.1
29961 512.969377449 192.168.32.139 192.168.32.1 HTTP 630 HTTP/1.1 200 OK (text/html)
29963 513.039506317 192.168.32.1 192.168.32.139 HTTP 505 GET /dvwa/dvwa/css/main.css HTTP/1.1
29964 513.042231798 192.168.32.1 192.168.32.139 HTTP 492 GET /dvwa/dvwa/js/dvwaPage.js HTTP/1.1
29969 513.043456558 192.168.32.139 192.168.32.1 HTTP 1375 HTTP/1.1 200 OK (text/css)
29973 513.047564999 192.168.32.1 192.168.32.139 HTTP 554 GET /dvwa/dvwa/images/logo.png HTTP/1.1
Source Port: 56747
Destination Port: 80
[Stream index: 17]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 761]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1335063867
[Next Sequence Number: 762 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 3404998353
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0xb70e [unverified]
0030 02 01 b7 0e 00 00 50 4f 53 54 20 2f 64 76 77 61 ..... PO ST /dvwa
0040 2f 6c 6f 67 69 6e 2e 70 68 70 20 48 54 54 50 2f /login.p hp HTTP/
0050 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 1.1 Hos t: 192.1
0060 36 38 2e 33 32 2e 31 33 39 0d 0a 43 6f 6e 6e 65 68.32.13 9 Conne
0070 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ction: k eep-aliv
0080 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 e Conte nt-Lengt
0090 68 3a 20 34 34 0d 0a 43 61 63 68 65 2d 43 6f 6e h: 44 C ache-Con
00a0 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d trol: ma x-age=0
00b0 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 Upgrade -Insecur
00c0 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 4f e-Reques ts: 1 O
00d0 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f 2f 31 39 rigin: h ttp://19
00e0 32 2e 31 36 38 2e 33 32 2e 31 33 39 0d 0a 43 6f 2.168.32 .139 Co
00f0 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c ntent-Ty pe: appl
0100 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f ication/ x-www-fo
0110 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 55 rm-urlen coded U
0120 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ser-Agen t: Mozil
Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (tcp.checksum), 2 byte(s)
Packets: 30090 · Displayed: 30 (0.1%)
Profile: Default