Universidad Autónoma de Chiapas

Act. 3.2 Práctica Protección de Directorio al Servidor Apache de la aplicación DVWA

Materia:

Análisis de Vulnerabilidades.

Alumnos:

Cedrick Marcial Quintero.

Cristian Gutierrez Hernandez.

Lugar:

Tuxtla Gutiérrez, Chiapas.

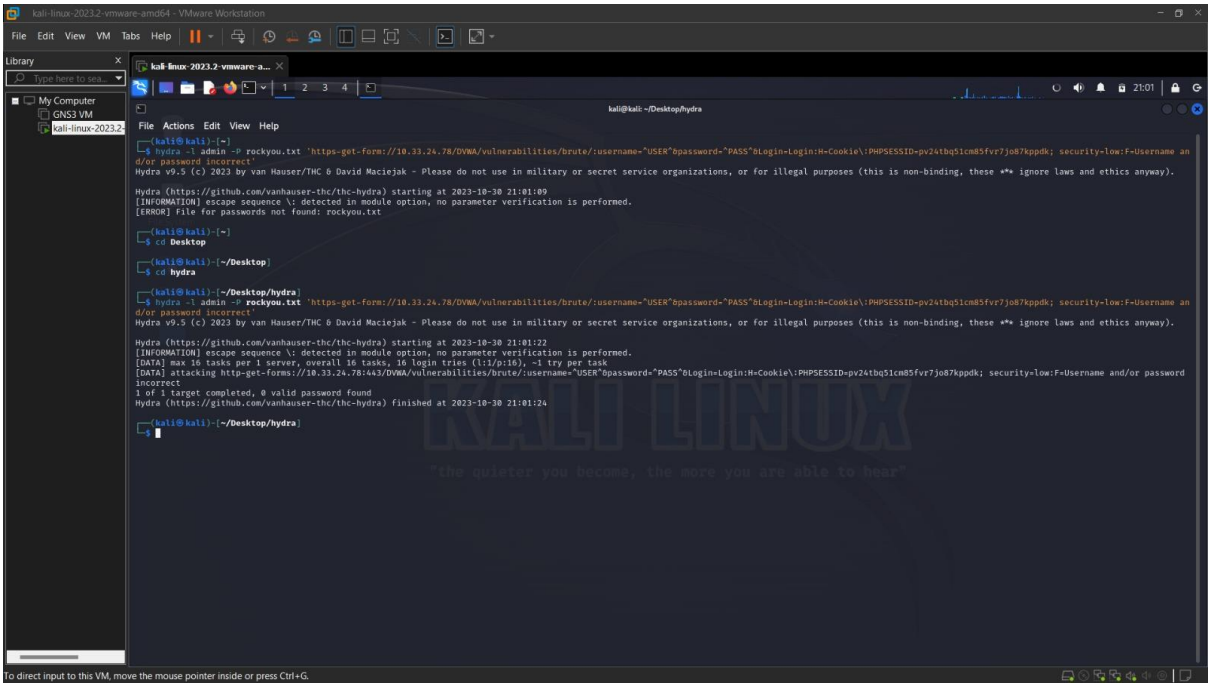
Profesor:

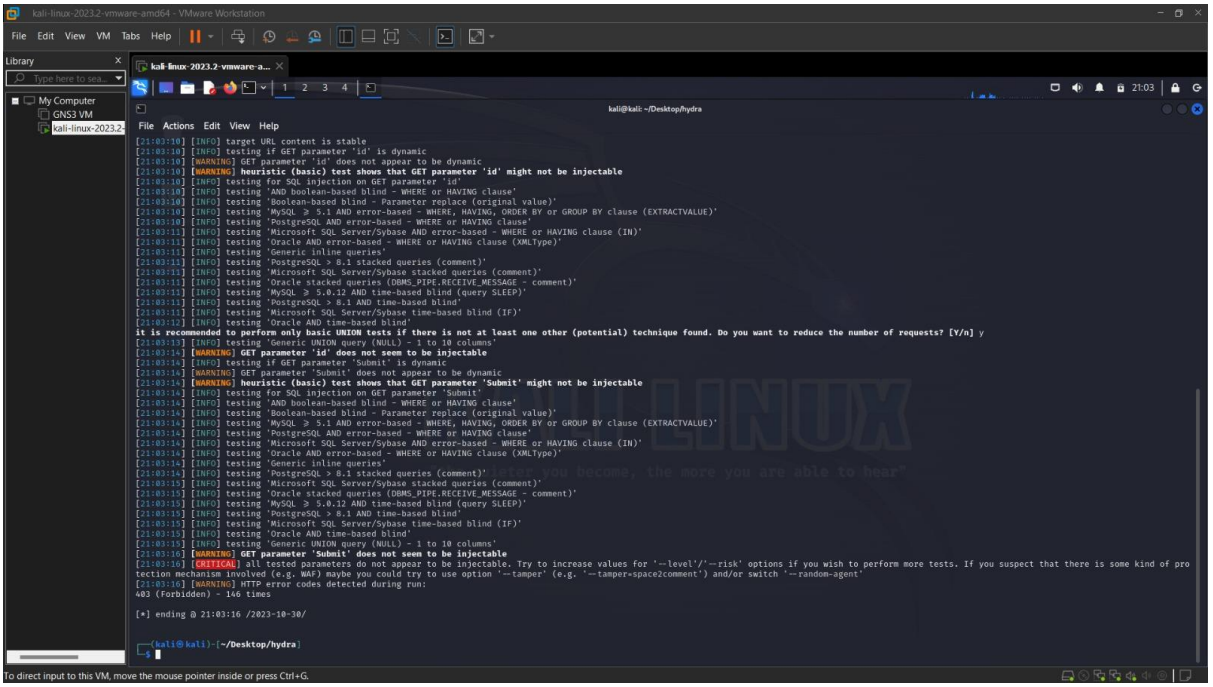
GUTIERREZ ALFARO LUIS.

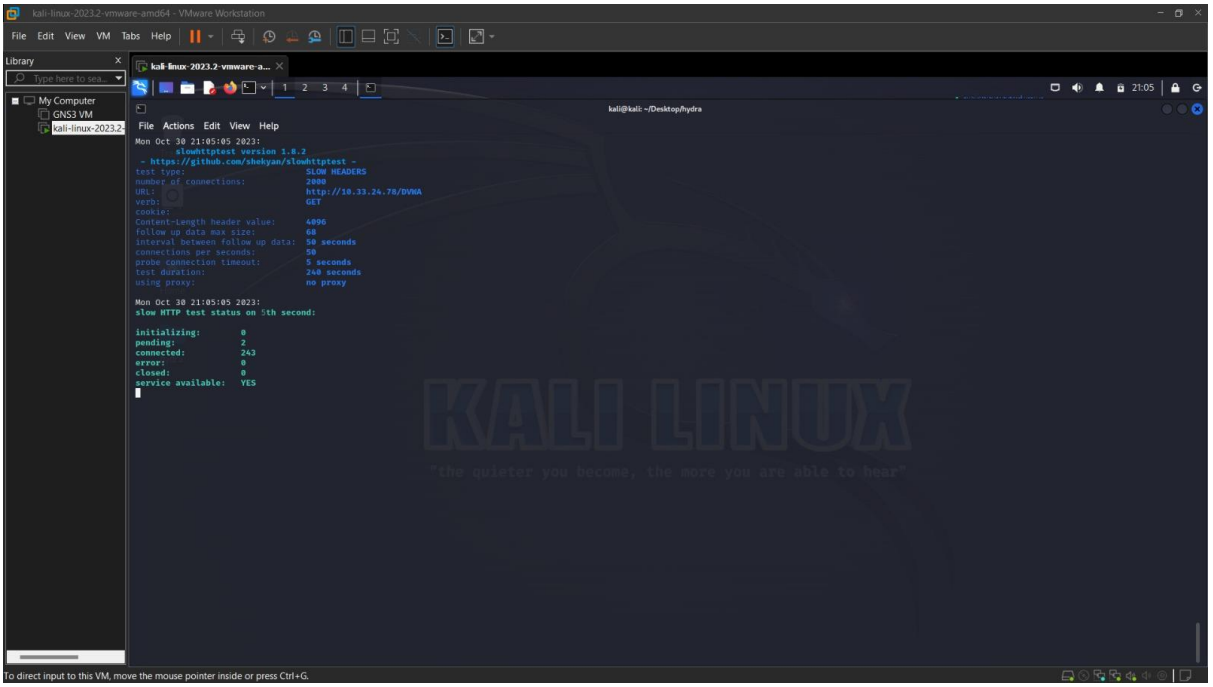
Grupo: 7° M

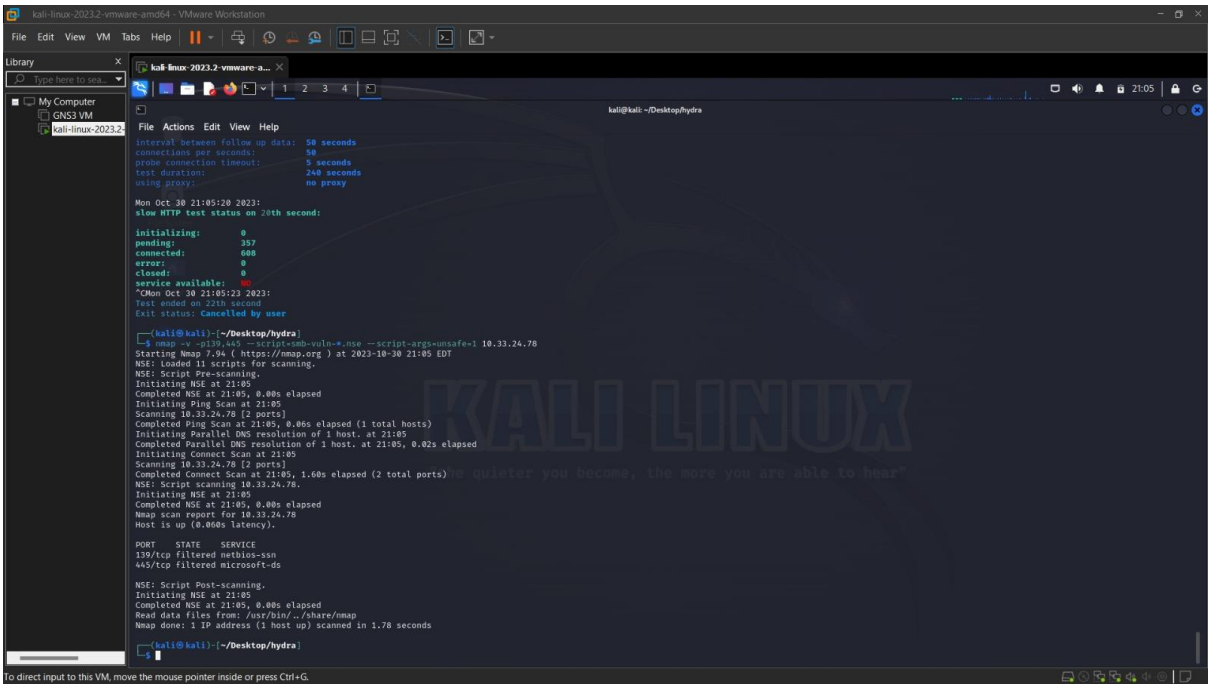
31 de Octubre del 2023.

Ataque a Cristian Gutierrez Hernandez :

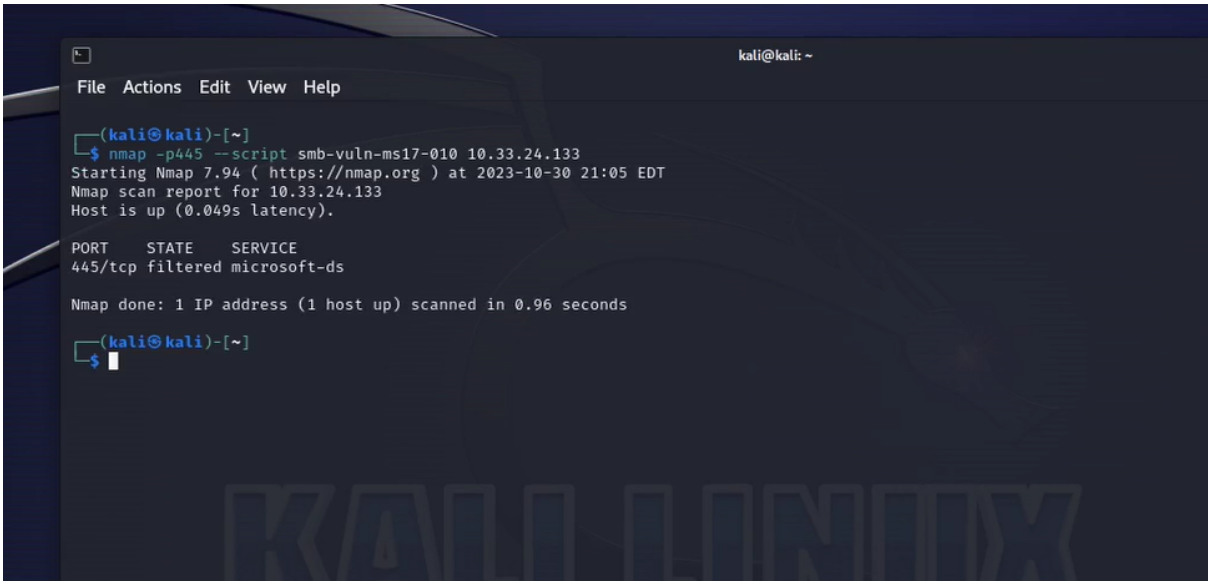


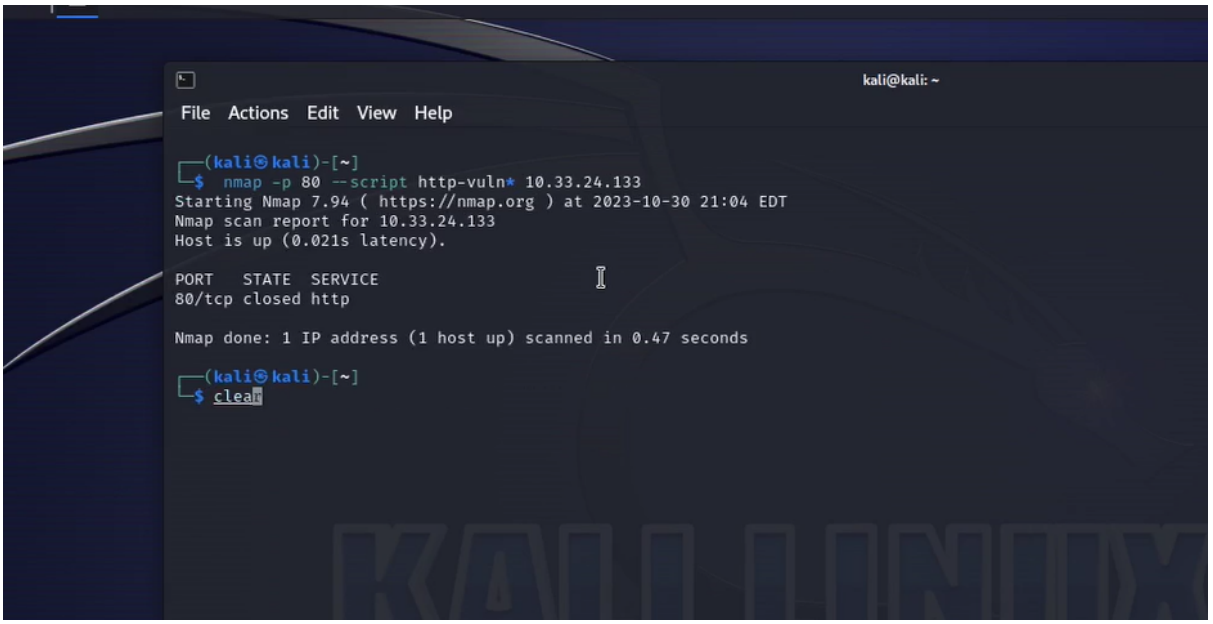


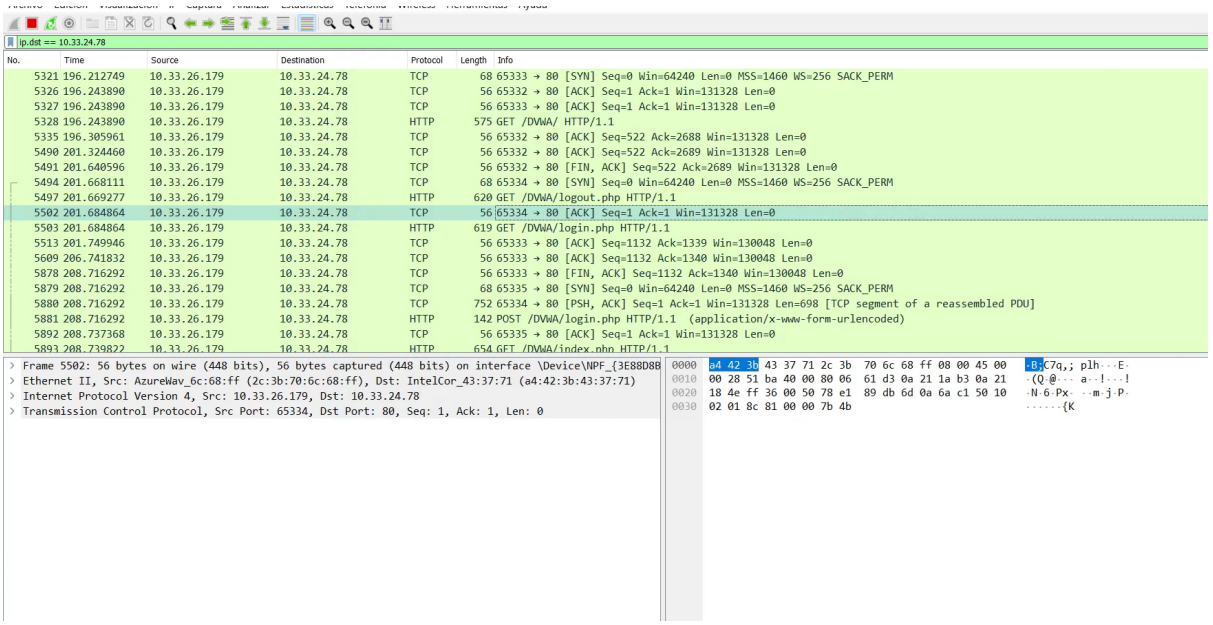

kali-linux-2023.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
GNS3 VM
kali-linux-2023.2-
kali-linux-2023.2-vmware-a...
kali@kali: ~/Desktop/hydra
File Actions Edit View Help
Mon Oct 30 21:05:05 2023:
slowhttptest version 1.8.2
- https://github.com/shekyan/slowhttptest -
test type: SLOW HEADERS
number of connections: 2000
URL: http://10.33.24.78/DVWA
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 50 seconds
connections per seconds: 50
probe connection timeout: 5 seconds
test duration: 240 seconds
using proxy: no proxy
Mon Oct 30 21:05:05 2023:
slow HTTP test status on 5th second:
initializing: 0
pending: 2
connected: 243
error: 0
closed: 0
service available: YES
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

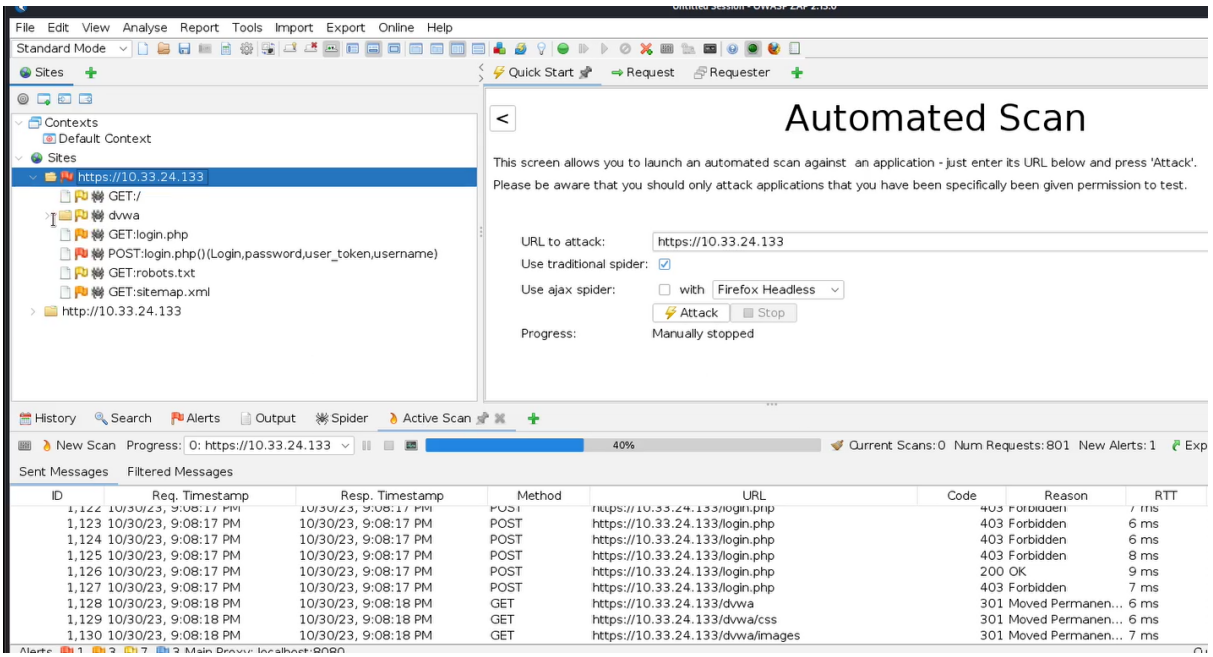

kali-linux-2023.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
GNS3 VM
kali-linux-2023.2-
kali-linux-2023.2-vmware-a...
kali@kali: ~/Desktop/hydra
File Actions Edit View Help
interval between follow up data: 50 seconds
connections per seconds: 50
probe connection timeout: 5 seconds
test duration: 240 seconds
using proxy: no proxy
Mon Oct 30 21:05:20 2023:
slow HTTP test status on 20th second:
initializing: 0
pending: 357
connected: 608
error: 0
closed: 0
service available: NO
^CMon Oct 30 21:05:23 2023:
Test ended on 23th second
Exit status: Cancelled by user
┌──(kali㉿kali)-[~/Desktop/hydra]
└─$ nmap -v -p139,445 --script-smb-vuln-*.nse --script-args=unsafe=1 10.33.24.78
Starting Nmap 7.94 (https://nmap.org) at 2023-10-30 21:05 EDT
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Initiating Ping Scan at 21:05
Scanning 10.33.24.78 [2 ports]
Completed Ping Scan at 21:05, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:05
Completed Parallel DNS resolution of 1 host. at 21:05, 0.02s elapsed
Initiating Connect Scan at 21:05
Scanning 10.33.24.78 [2 ports]
Completed Connect Scan at 21:05, 1.60s elapsed (2 total ports)
NSE: Script scanning 10.33.24.78.
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Nmap scan report for 10.33.24.78
Host is up (0.060s latency).
PORT STATE SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
NSE: Script Post-scanning.
Initiating NSE at 21:05
Completed NSE at 21:05, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
┌──(kali㉿kali)-[~/Desktop/hydra]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Ataque a Cedrick Marcial Quintero :






ip.dst == 10.33.24.78
No. Time Source Destination Protocol Length Info
5321 196.212749 10.33.26.179 10.33.24.78 TCP 68 65333 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5326 196.243890 10.33.26.179 10.33.24.78 TCP 56 65332 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5327 196.243890 10.33.26.179 10.33.24.78 TCP 56 65333 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5328 196.243890 10.33.26.179 10.33.24.78 HTTP 575 GET /DVWA/ HTTP/1.1
5335 196.305961 10.33.26.179 10.33.24.78 TCP 56 65332 → 80 [ACK] Seq=522 Ack=2688 Win=131328 Len=0
5490 201.324460 10.33.26.179 10.33.24.78 TCP 56 65332 → 80 [ACK] Seq=522 Ack=2689 Win=131328 Len=0
5491 201.640596 10.33.26.179 10.33.24.78 TCP 56 65332 → 80 [FIN, ACK] Seq=522 Ack=2689 Win=131328 Len=0
5494 201.668111 10.33.26.179 10.33.24.78 TCP 68 65334 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5497 201.669277 10.33.26.179 10.33.24.78 HTTP 620 GET /DVWA/logout.php HTTP/1.1
5502 201.684864 10.33.26.179 10.33.24.78 TCP 56 65334 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5503 201.684864 10.33.26.179 10.33.24.78 HTTP 619 GET /DVWA/login.php HTTP/1.1
5513 201.749946 10.33.26.179 10.33.24.78 TCP 56 65333 → 80 [ACK] Seq=1132 Ack=1339 Win=130048 Len=0
5609 206.741832 10.33.26.179 10.33.24.78 TCP 56 65333 → 80 [ACK] Seq=1132 Ack=1340 Win=130048 Len=0
5878 208.716292 10.33.26.179 10.33.24.78 TCP 56 65333 → 80 [FIN, ACK] Seq=1132 Ack=1340 Win=130048 Len=0
5879 208.716292 10.33.26.179 10.33.24.78 TCP 68 65335 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
5880 208.716292 10.33.26.179 10.33.24.78 TCP 752 65334 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=698 [TCP segment of a reassembled PDU]
5881 208.716292 10.33.26.179 10.33.24.78 HTTP 142 POST /DVWA/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5892 208.737368 10.33.26.179 10.33.24.78 TCP 56 65335 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
5893 208.739822 10.33.26.179 10.33.24.78 HTTP 654 GET /DVWA/index.php HTTP/1.1
Frame 5502: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{3E88D88
Ethernet II, Src: AzureWav_6c:68:ff (2c:3b:70:6c:68:ff), Dst: IntelCor_43:37:71 (a4:42:3b:43:37:71)
Internet Protocol Version 4, Src: 10.33.26.179, Dst: 10.33.24.78
Transmission Control Protocol, Src Port: 65334, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 a4 42 3b 43 37 71 2c 3b 70 6c 68 ff 08 00 45 00
0010 00 28 51 ba 40 00 80 06 61 d3 0a 21 1a b3 0a 21
0020 18 4e ff 36 00 50 78 e1 89 db 6d 0a 6a c1 50 10
0030 02 01 8c 81 00 00 7b 4b


File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Requester
Contexts
Default Context
Sites
https://10.33.24.133
GET:/
dvwa
GET:login.php
POST:login.php() (Login,password,user_token,username)
GET:robots.txt
GET:sitemap.xml
http://10.33.24.133
Automated Scan
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: https://10.33.24.133
Use traditional spider:
Use ajax spider: with Firefox Headless
Attack
Stop
Progress: Manually stopped
History
Search
Alerts
Output
Spider
Active Scan
New Scan
Progress: 0: https://10.33.24.133
40%
Current Scans: 0 Num Requests: 801 New Alerts: 1
Sent Messages
Filtered Messages
ID Req. Timestamp Resp. Timestamp Method URL Code Reason RTT
1,123 10/30/23, 9:08:17 PM 10/30/23, 9:08:17 PM POST https://10.33.24.133/login.php 403 Forbidden 6 ms
1,124 10/30/23, 9:08:17 PM 10/30/23, 9:08:17 PM POST https://10.33.24.133/login.php 403 Forbidden 6 ms
1,125 10/30/23, 9:08:17 PM 10/30/23, 9:08:17 PM POST https://10.33.24.133/login.php 403 Forbidden 8 ms
1,126 10/30/23, 9:08:17 PM 10/30/23, 9:08:17 PM POST https://10.33.24.133/login.php 200 OK 9 ms
1,127 10/30/23, 9:08:17 PM 10/30/23, 9:08:17 PM POST https://10.33.24.133/login.php 403 Forbidden 7 ms
1,128 10/30/23, 9:08:18 PM 10/30/23, 9:08:18 PM GET https://10.33.24.133/dvwa 301 Moved Permanen... 6 ms
1,129 10/30/23, 9:08:18 PM 10/30/23, 9:08:18 PM GET https://10.33.24.133/dvwa/css 301 Moved Permanen... 6 ms
1,130 10/30/23, 9:08:18 PM 10/30/23, 9:08:18 PM GET https://10.33.24.133/dvwa/images 301 Moved Permanen... 7 ms


kali@kali: ~
File Actions Edit View Help
Mon Oct 30 21:02:26 2023:
slowhttptest version 1.8.2
- https://github.com/shekyan/slowhttptest -
test type: SLOW HEADERS
number of connections: 2000
URL: https://10.33.24.133/
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 50 seconds
connections per seconds: 50
probe connection timeout: 5 seconds
test duration: 240 seconds
using proxy: no proxy
Mon Oct 30 21:02:26 2023:
slow HTTP test status on 10th second:
initializing: 0
pending: 246
connected: 150
error: 0
closed: 0
service available: NO
KALI LINUX
"the quieter you become, the more you are able to hear"