Kali Lunix Penetration Testing
http://testhtml5.vulnweb.com/#/popular

The following pages show the output from the Kali Lunix penetration testing in relation to the test web-application http://testhtml5.vulnweb.com/#/popular which has been designed with deliberate vulnerability flaws.

whois vulnweb.com

```
Registrars.
Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Acunetix Acunetix
Registrant Organization: Acunetix Ltd
Registrant Street: 3rd Floor,, J&C Building,, Road Town
Registrant City: Tortola
Registrant State/Province:
Registrant Postal Code: VG1110
Registrant Country: VG
Registrant Phone: +1.23456789
Registrant Fax:
Registrant Email: administrator@acunetix.com
Registry Admin ID:
Admin Name: Acunetix Acunetix
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@acunetix.com
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
```

DNS Enumerate vulnweb.com

```
; <<>> DiG 9.20.2-1-Debian <<>> vulnweb.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4248
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;vulnweb.com.                   IN      NS

;; ANSWER SECTION:
vulnweb.com.            939     IN      NS      ns4.eurodns.com.
vulnweb.com.            939     IN      NS      ns1.eurodns.com.
vulnweb.com.            939     IN      NS      ns3.eurodns.com.
vulnweb.com.            939     IN      NS      ns2.eurodns.com.

;; Query time: 20 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Fri Mar 07 18:37:58 GMT 2025
;; MSG SIZE  rcvd: 120
```

Reverse DNS sweeping

```
┌──(user㉿vbox)-[~]
└─$ nmap -sL 44.228.249.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-07 18:42 GMT
Nmap scan report for ec2-44-228-249-0.us-west-2.compute.amazonaws.com (44.228.249.0)
Nmap scan report for ec2-44-228-249-1.us-west-2.compute.amazonaws.com (44.228.249.1)
Nmap scan report for ec2-44-228-249-2.us-west-2.compute.amazonaws.com (44.228.249.2)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Nmap scan report for ec2-44-228-249-4.us-west-2.compute.amazonaws.com (44.228.249.4)
Nmap scan report for ec2-44-228-249-5.us-west-2.compute.amazonaws.com (44.228.249.5)
Nmap scan report for ec2-44-228-249-6.us-west-2.compute.amazonaws.com (44.228.249.6)
Nmap scan report for ec2-44-228-249-7.us-west-2.compute.amazonaws.com (44.228.249.7)
Nmap scan report for ec2-44-228-249-8.us-west-2.compute.amazonaws.com (44.228.249.8)
Nmap scan report for ec2-44-228-249-9.us-west-2.compute.amazonaws.com (44.228.249.9)
Nmap scan report for ec2-44-228-249-10.us-west-2.compute.amazonaws.com (44.228.249.10)
Nmap scan report for ec2-44-228-249-11.us-west-2.compute.amazonaws.com (44.228.249.11)
Nmap scan report for ec2-44-228-249-12.us-west-2.compute.amazonaws.com (44.228.249.12)
Nmap scan report for ec2-44-228-249-13.us-west-2.compute.amazonaws.com (44.228.249.13)
Nmap scan report for ec2-44-228-249-14.us-west-2.compute.amazonaws.com (44.228.249.14)
Nmap scan report for ec2-44-228-249-15.us-west-2.compute.amazonaws.com (44.228.249.15)
Nmap scan report for ec2-44-228-249-16.us-west-2.compute.amazonaws.com (44.228.249.16)
Nmap scan report for ec2-44-228-249-17.us-west-2.compute.amazonaws.com (44.228.249.17)
Nmap scan report for ec2-44-228-249-18.us-west-2.compute.amazonaws.com (44.228.249.18)
Nmap scan report for ec2-44-228-249-19.us-west-2.compute.amazonaws.com (44.228.249.19)
Nmap scan report for ec2-44-228-249-20.us-west-2.compute.amazonaws.com (44.228.249.20)
Nmap scan report for ec2-44-228-249-21.us-west-2.compute.amazonaws.com (44.228.249.21)
```

```
Trying Zone Transfers and getting Bind Versions:
_____________________________________________


Trying Zone Transfer for vulnweb.com on ns2.eurodns.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for vulnweb.com on ns4.eurodns.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for vulnweb.com on ns3.eurodns.com ...
AXFR record query failed: REFUSED

Trying Zone Transfer for vulnweb.com on ns1.eurodns.com ...
AXFR record query failed: REFUSED


Brute forcing with /usr/share/dnsenum/dns.txt:
_____________________________________________



vulnweb.com class C netranges:
______________________________

 44.228.249.0/24


Performing reverse lookup on 256 ip addresses:
______________________________________________


0 results out of 256 IP addresses.


vulnweb.com ip blocks:
______________________


done.
```

NMAP sSc

```
┌──(user㉿vbox)-[~]
└─$ nmap -sSC 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 12:56 GMT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.84 seconds
```

UDP MAP

Starting Nmap 7.94SVN (https://nmap.org) at 2025-03-08 17:55 GMT

Initiating UDP Scan at 17:55

Scanning 22.228.249.3 [100 ports]

Completed UDP Scan at 17:55, 21.10s elapsed (100 total ports)

Nmap scan report for 22.228.249.3

Host is up, received user-set.

Scanned at 2025-03-08 17:55:27 GMT for 21s

PORT	STATE	SERVICE	REASON
7/udp	open|filtered	echo	no-response
9/udp	open|filtered	discard	no-response
17/udp	open|filtered	qotd	no-response
19/udp	open|filtered	chargen	no-response
49/udp	open|filtered	tacacs	no-response
53/udp	open|filtered	domain	no-response
67/udp	open|filtered	dhcps	no-response
68/udp	open|filtered	dhcpc	no-response
69/udp	open|filtered	tftp	no-response
80/udp	open|filtered	http	no-response
88/udp	open|filtered	kerberos-sec	no-response
111/udp	open|filtered	rpcbind	no-response
120/udp	open|filtered	cfdptkt	no-response
123/udp	open|filtered	ntp	no-response
135/udp	open|filtered	msrpc	no-response
136/udp	open|filtered	profile	no-response
137/udp	open|filtered	netbios-ns	no-response
138/udp	open|filtered	netbios-dgm	no-response
139/udp	open|filtered	netbios-ssn	no-response
158/udp	open|filtered	pcmail-srv	no-response

161/udp open|filtered snmp no-response

162/udp open|filtered snmptrap no-response

177/udp open|filtered xdmcp no-response

427/udp open|filtered svrloc no-response

443/udp open|filtered https no-response

445/udp open|filtered microsoft-ds no-response

497/udp open|filtered retrospect no-response

500/udp open|filtered isakmp no-response

514/udp open|filtered syslog no-response

515/udp open|filtered printer no-response

518/udp open|filtered ntalk no-response

520/udp open|filtered route no-response

593/udp open|filtered http-rpc-epmap no-response

623/udp open|filtered asf-rmcp no-response

626/udp open|filtered serialnumberd no-response

631/udp open|filtered ipp no-response

996/udp open|filtered vsinet no-response

997/udp open|filtered maitrd no-response

998/udp open|filtered puparp no-response

999/udp open|filtered applix no-response

1022/udp open|filtered exp2 no-response

1023/udp open|filtered unknown no-response

1025/udp open|filtered blackjack no-response

1026/udp open|filtered win-rpc no-response

1027/udp open|filtered unknown no-response

1028/udp open|filtered ms-lsa no-response

1029/udp open|filtered solid-mux no-response

1030/udp open|filtered iad1 no-response

1433/udp open|filtered ms-sql-s no-response

1434/udp open|filtered ms-sql-m no-response

1645/udp open|filtered radius no-response

1646/udp open|filtered radacct no-response

1701/udp open|filtered L2TP no-response

1718/udp open|filtered h225gatedisc   no-response
1719/udp open|filtered h323gatestat   no-response
1812/udp open|filtered radius   no-response
1813/udp open|filtered radacct   no-response
1900/udp open|filtered upnp   no-response
2000/udp open|filtered cisco-sccp   no-response
2048/udp open|filtered dls-monitor   no-response
2049/udp open|filtered nfs   no-response
2222/udp open|filtered msantipiracy   no-response
2223/udp open|filtered rockwell-csp2   no-response
3283/udp open|filtered netassistant   no-response
3456/udp open|filtered IISrpc-or-vat   no-response
3703/udp open|filtered adobeserver-3   no-response
4444/udp open|filtered krb524   no-response
4500/udp open|filtered nat-t-ike   no-response
5000/udp open|filtered upnp   no-response
5060/udp open|filtered sip   no-response
5353/udp open|filtered zeroconf   no-response
5632/udp open|filtered pcanywherestat no-response
9200/udp open|filtered wap-wsp   no-response
10000/udp open|filtered ndmp   no-response
17185/udp open|filtered wdbrpc   no-response
20031/udp open|filtered bakbonenetvault no-response
30718/udp open|filtered unknown   no-response
31337/udp open|filtered BackOrifice   no-response
32768/udp open|filtered omad   no-response
32769/udp open|filtered filenet-rpc   no-response
32771/udp open|filtered sometimes-rpc6 no-response
32815/udp open|filtered unknown   no-response
33281/udp open|filtered unknown   no-response
49152/udp open|filtered unknown   no-response
49153/udp open|filtered unknown   no-response
49154/udp open|filtered unknown   no-response

49156/udp open|filtered unknown no-response

49181/udp open|filtered unknown no-response

49182/udp open|filtered unknown no-response

49185/udp open|filtered unknown no-response

49186/udp open|filtered unknown no-response

49188/udp open|filtered unknown no-response

49190/udp open|filtered unknown no-response

49191/udp open|filtered unknown no-response

49192/udp open|filtered unknown no-response

49193/udp open|filtered unknown no-response

49194/udp open|filtered unknown no-response

49200/udp open|filtered unknown no-response

49201/udp open|filtered unknown no-response

65024/udp open|filtered unknown no-response

Read data files from: /usr/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 21.14 seconds

Raw packets sent: 256 (15.724KB) | Rcvd: 0 (0B)

TCP Scan

Starting Nmap 7.94SVN (https://nmap.org) at 2025-03-08 18:03 GMT

Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

Host is up (0.015s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 12.31 seconds

FTP anonymous logins

```
└─$ nmap -sV -sC vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 13:12 GMT
Nmap scan report for vulnweb.com (44.228.249.3)
Host is up (0.016s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0
|_http-title: Acunetix Web Vulnerability Scanner - Test websites

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.85 seconds
```

Web Crawl with Metasploit

```
[*] Crawling http://testhtml5.vulnweb.com:80/...
[*] [00001/00500]    200 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/
[*]                      FORM: POST /login
[-] [00002/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/%23/latest
[-] [00003/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/%23/popular
[-] [00004/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/%23/archive
[-] [00005/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/%23/carousel
[-] [00006/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/%23/contact
[-] [00007/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/%23/about
[-] [00008/00500]    405 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/login
[*] [00009/00500]    200 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/static/css/style.css
[-] [00010/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/test/
[-] [00011/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/tmp/
[-] [00012/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/awstats/
[-] [00013/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/stuff/
[-] [00014/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/awstats/awstats/
[-] [00015/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/basilic/
[-] [00016/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/cacti/
[-] [00017/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/docs/text/manual.txt
[-] [00018/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/docs/html/php_script_server.html
[-] [00019/00500]    404 - testhtml5.vulnweb.com - http://testhtml5.vulnweb.com/docs/CHANGELOG
[*] Crawl of http://testhtml5.vulnweb.com:80/ complete
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/crawler) >
```

Hyrda: Password Grinding

```
┌──(user㉿vbox)-[~]
└─$ hydra -L login.txt -P passwords.txt ftp://44.228.249.3

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-09 19:12:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 75 login tries (l:5/p:15), ~5 tries per task
[DATA] attacking ftp://44.228.249.3:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-09 19:13:18
```

Nginx_vulnerablity

```
[-] http://44.228.249.3/admin.php - nginx - Cannot exploit: the remote server is not vulnerable - Version nginx/1.19.0
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/nginx_source_disclosure) >
```