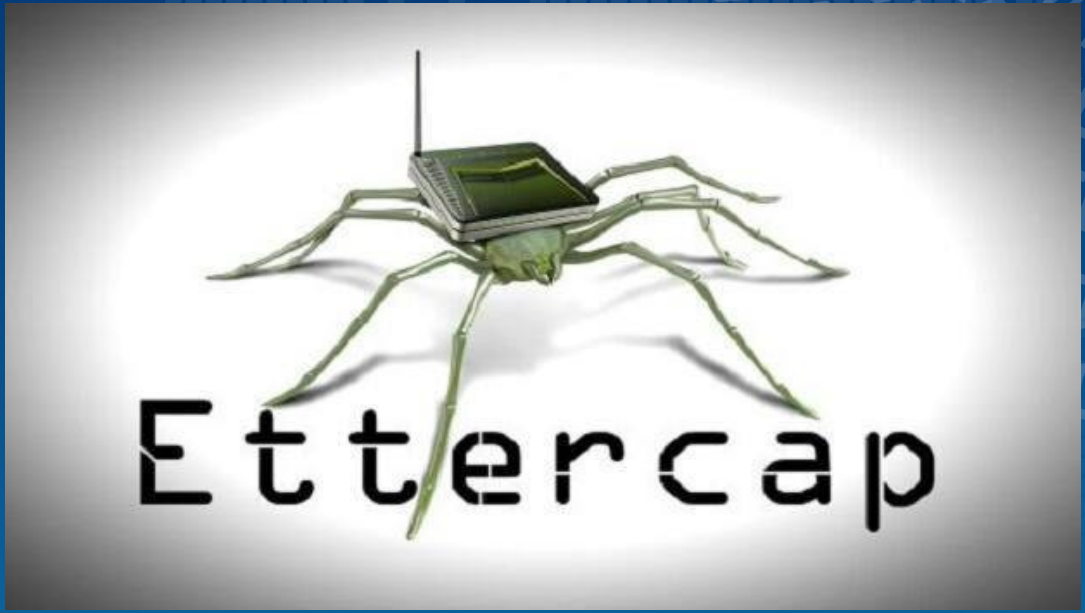
OWASP
Open Web Application Security Project



DNS Spoofing Demonstration

OWASP
Open Web Application Security Project

The demonstration is carried on a LAN network composed of the following three elements:

- Default Gateway (IP address 192.168.224.2)

- Attacker computer (IP address 192.168.224.13)

- Target computer (IP address 192.168.224.211)

The application used to carry out the DNS Spoofing is *Ettercap*: a free and open source network security tool for man-in-the-middle attacks.

OWASP
Open Web Application Security Project

Prepare for the attack by configuring the attack parameters:

- Step 1: Make a fake OWASP HTML web-page (phishing web-page). Set it up on an Apache Web Server hosted on the Attacker computer (the fake web-site will be accessed by typing the IP address of the Attacker computer onto a browser).

- Step 2: Go to the Ettercap directory and open the “etter.dns” using a text editor. At the bottom of the file, add the name to the website that we want to want to attack (in this case, “www.owasp.org”) and also add the IP that we want the Target

computer to be redirected to (in this case, the IP address of the Attacker computer, hosting the fake web-page). See the following screenshot for illustration.

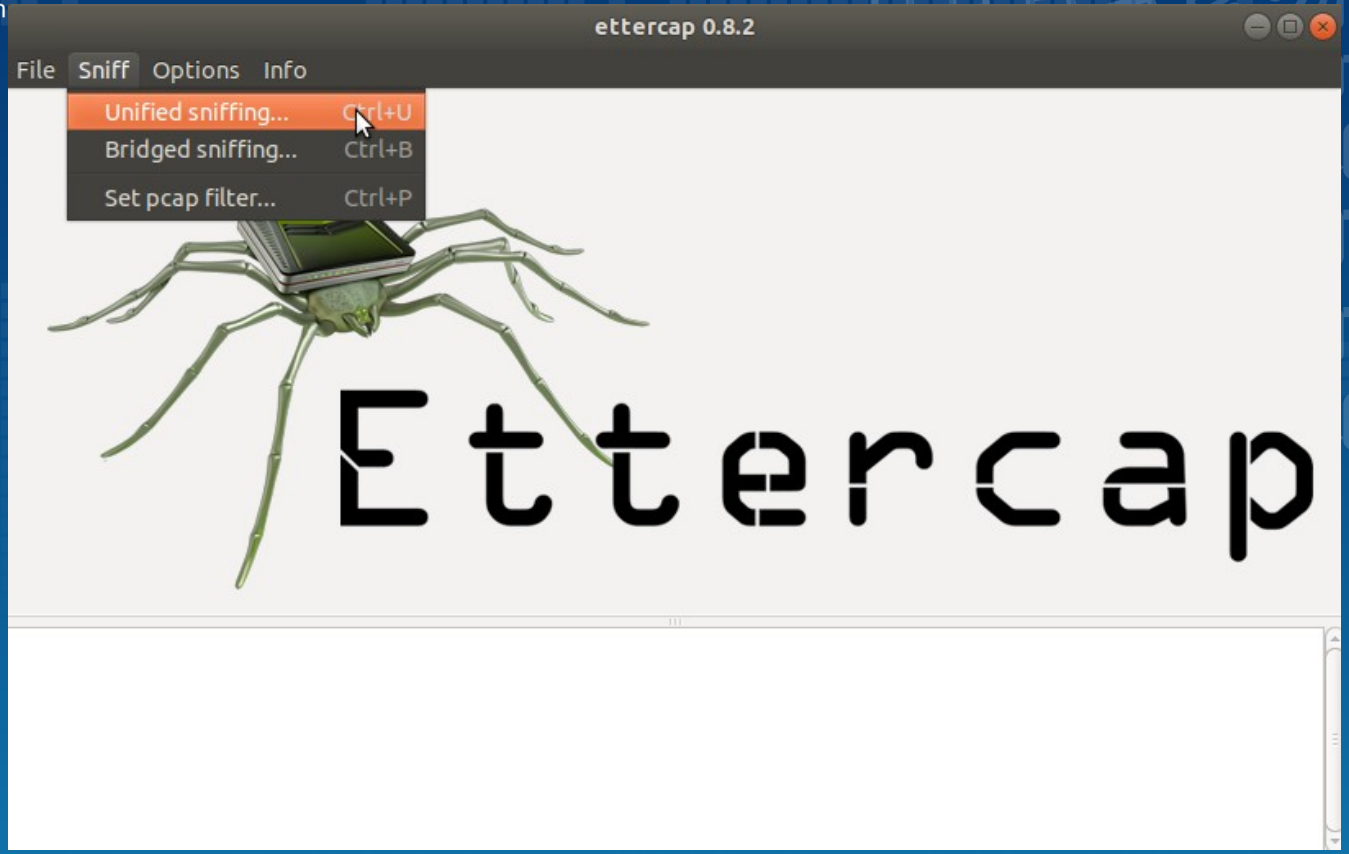
OWASP
Open Web Application Security Project

The attack parameters that were added manually are marked with the red square:

```
Activities   Terminal
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                                  /etc/ettercap/etter.dns

# resolutions. I.e. Windows/Samba file sharing.
#

LAB-PC*  WINS  127.0.0.1

##################################################
# Demonstration for OWASP Security Event

owasp.org        A        192.168.224.13
*.owasp.org      A        192.168.224.13
www.owasp.org    A        192.168.224.13

# vim:ts=8:noexpandtab
```

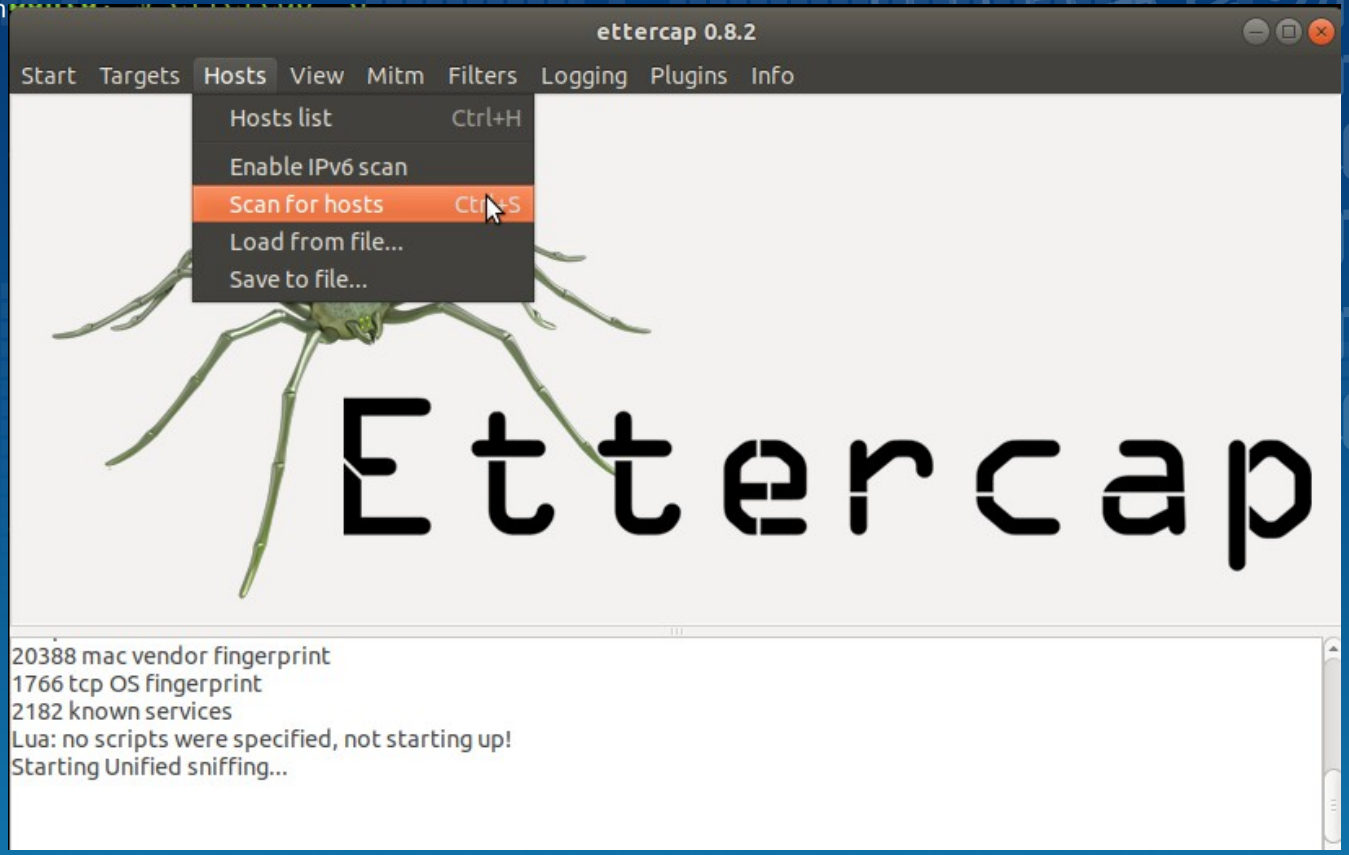
OWASP
Open Web Application Security Project

Step 3:
Open Ettercap in sudo mode and select Sniff>Unified Sniffing



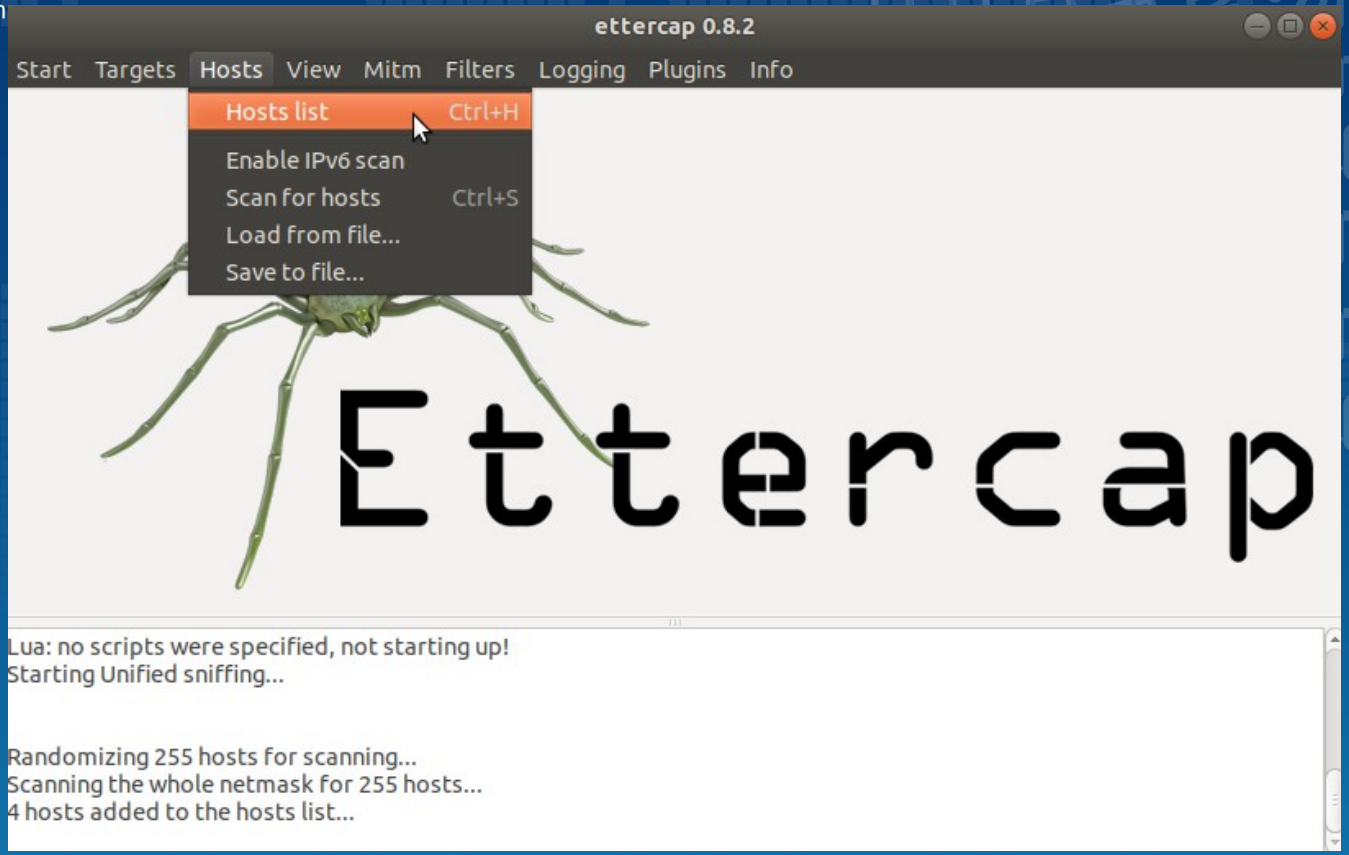
OWASP
Open Web Application Security Project

Step 4:
Go to Hosts>Scan for Hosts to find devices connected to the LAN



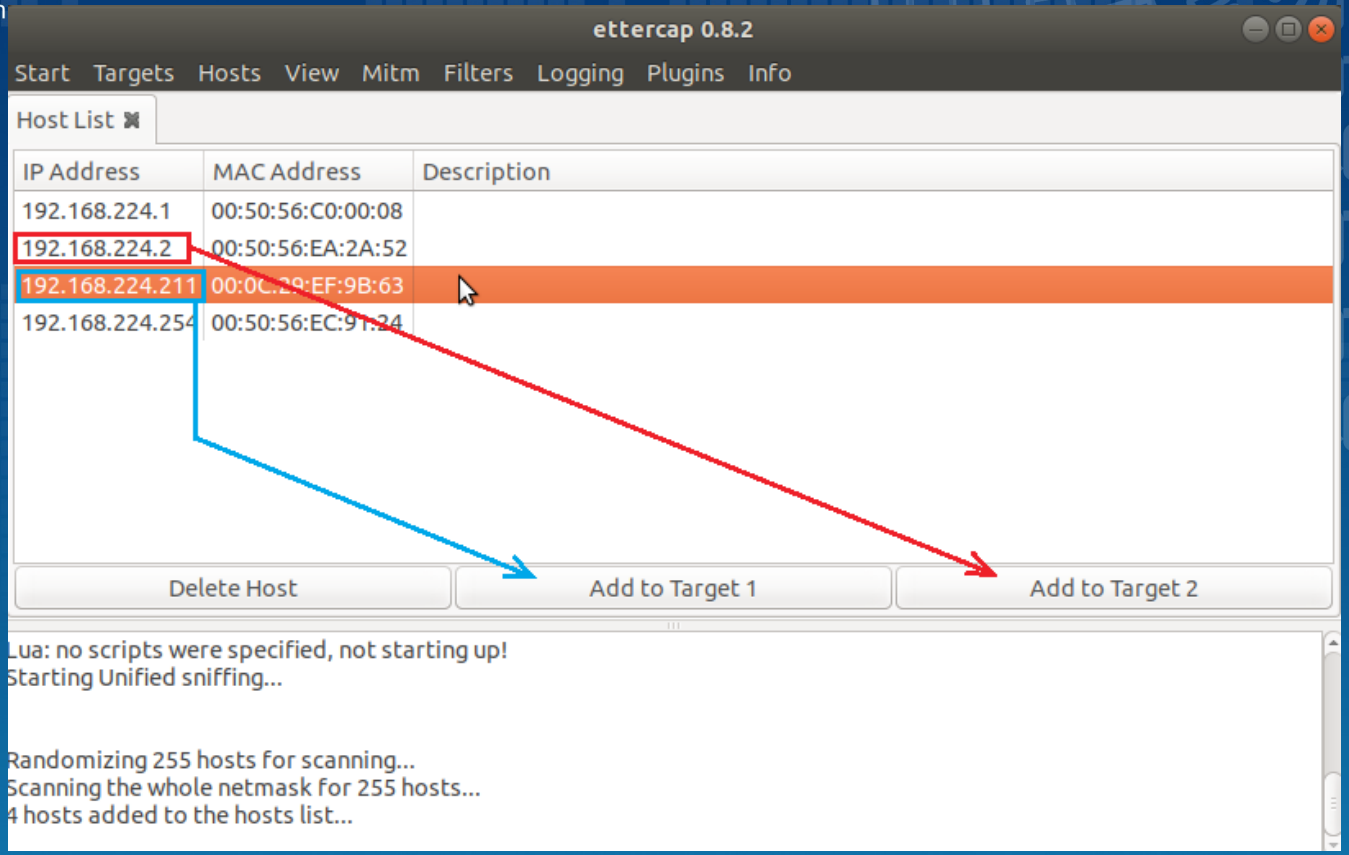
OWASP
Open Web Application Security Project

Step 5:
Go to Hosts>Hosts List to display the list of devices



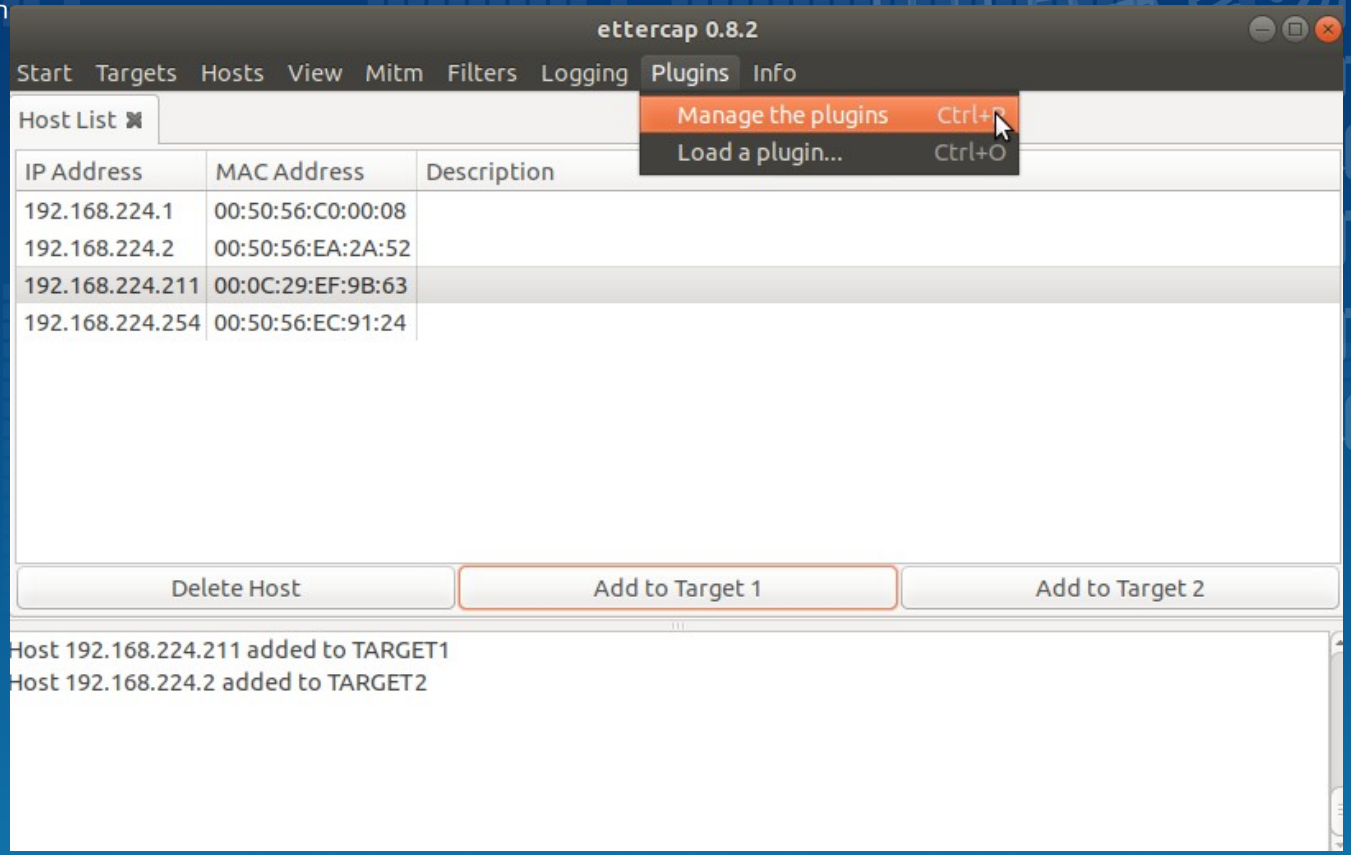
OWASP
Open Web Application Security Project

Step 6:
From the list, select the IP address of the Target computer and add it to Target 1 and also select the IP address of the default gateway and add it to Target 2



OWASP
Open Web Application Security Project

Step 7:
Go to Plugins>Manage the Plugins



OWASP
Open Web Application Security Project

Step 8:
From the list of plugins select "dns_spoof"

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

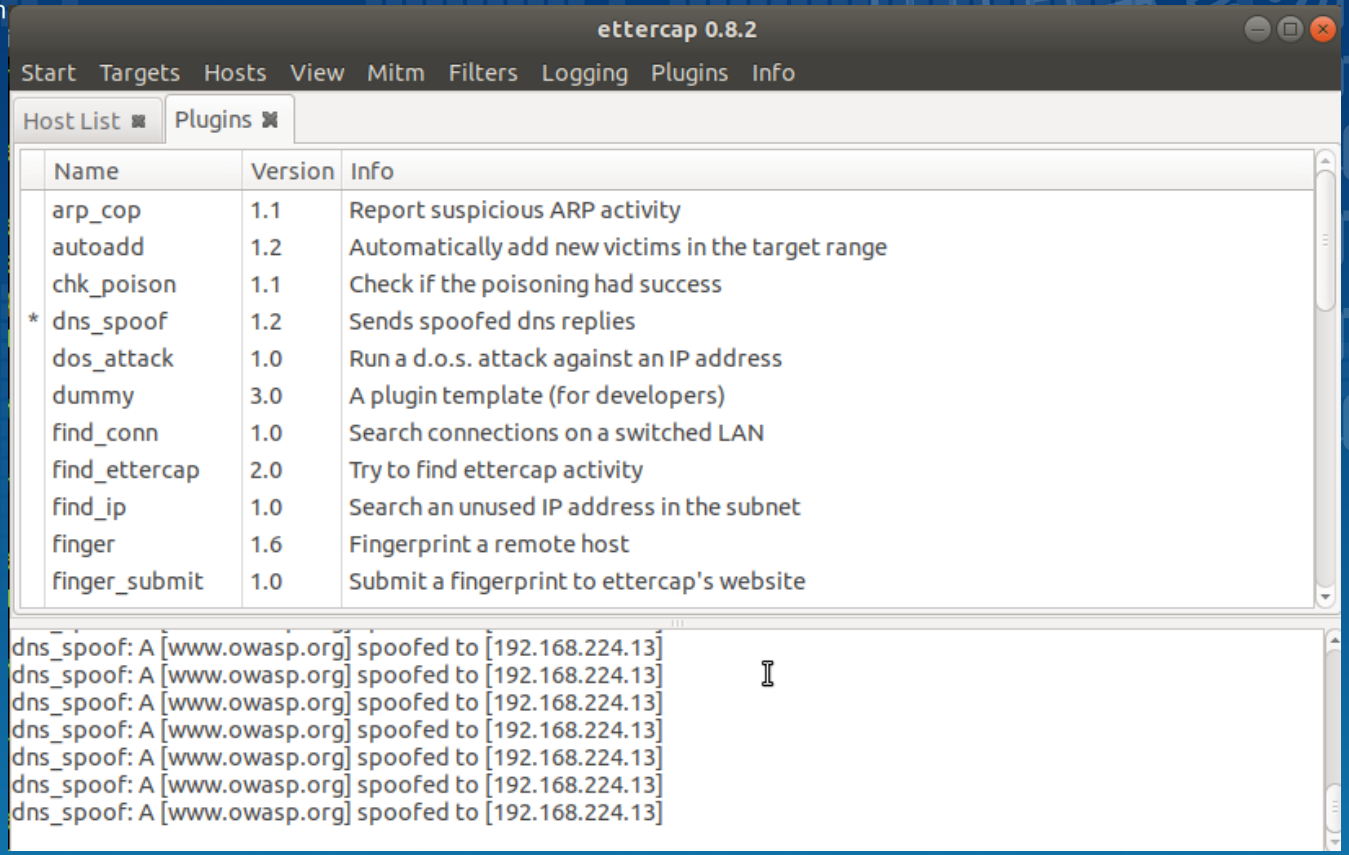
Host List | Plugins

Name	Version	Info
arp_cop	1.1	Report suspicious ARP activity
autoadd	1.2	Automatically add new victims in the target range
chk_poison	1.1	Check if the poisoning had success
dns_spoof	1.2	Sends spoofed dns replies
dos_attack	1.0	Run a d.o.s. attack against an IP address
dummy	3.0	A plugin template (for developers)
find_conn	1.0	Search connections on a switched LAN
find_ettercap	2.0	Try to find ettercap activity
find_ip	1.0	Search an unused IP address in the subnet
finger	1.6	Fingerprint a remote host
finger_submit	1.0	Submit a fingerprint to ettercap's website

Host 192.168.224.211 added to TARGET1
Host 192.168.224.2 added to TARGET2

OWASP
Open Web Application Security Project

Step 9:
The plugin activates the process of bombarding the target machine with fake DNS responses that resolve owasp.org to IP address 192.168.224.13 (where the fake web-page is hosted by web server on the Attacker machine)



OWASP - Mozilla Firefox

OWASP

https://www.owasp.org/index.php/Main_Page

Port in IPTables

Log in Request account

Search

OWASP™ Foundation

the free and open software security community

DONATE
OWASP DONATION PORTAL

Home
About OWASP
Acknowledgements
Advertising
Books
Brand Resources
Careers
Chapters
Donate to OWASP
Downloads
Events
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
Presentations
Press
Projects
Supporting Partners

Member Portal • About • Searching • Editing • New Article • OWASP Categories • Contact Us

Statistics • Recent Changes

Every vibrant technology marketplace needs an unbiased source of information on best practices as well as an active body advocating open standards. In the Application Security space, one of those groups is the Open Web Application Security Project™ (or OWASP for short).

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies, and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. You'll find everything **about OWASP** here on or linked from our wiki and current information on our OWASP Blog. OWASP **does not endorse or recommend commercial products**

Citations

Who Trusts OWASP?

Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice - Click Here

How can OWASP help your org?

Government Bodies
Educational Institutions
Standards Groups
Trade Organizations
Certifying Bodies

(2) Firefox 00:20

As a result, instead of being directed to the real web-page...

OWASP - Mozilla Firefox

OWASP

http://www.owasp.org

133%

Port in IPTables

Welcome to OWASP's Official Web Page

We are sorry to inform you that we are currently undergoing a company-wide rebranding process, which also affects the design of our website. Please send any important information and correspondence to the following e-mail address

Sincerely yours, the OWASP Team

| Copyright ©2019 All rights reserved |

(2) Firefox

00:22

...the Victim is directed to the fake web-page (**notice that the browser displays the same URL!**)

OWASP
Open Web Application Security Project

Please Note:

- We have discussed DNS Cache Poisoning methodology used to compromise DNS Cache records stored on users' computers

- However, these principles also apply for tampering with the cached DNS records on DNS Resolver servers!

The following slide shows a topological illustration of the attack.