Il protocollo ARP

L’ARP (Address Resolution Protocol) è un protocollo o una procedura che collega un indirizzo IP (Internet Protocol) in continua evoluzione a un indirizzo fisso del computer fisico, noto anche come indirizzo MAC (Media Access Control), in una rete locale (LAN) Quando un nuovo computer si collega a una LAN, gli viene assegnato un indirizzo IP univoco, da utilizzare per l'identificazione e la comunicazione.
I pacchetti di dati arrivano a un gateway, destinato a un particolare dispositivo host. Il gateway, o l'hardware di una rete che consente ai dati di essere trasmessi da una rete a un'altra, chiede al programma ARP di trovare un indirizzo MAC corrispondente all'indirizzo IP. La cache ARP tiene traccia di ogni indirizzo IP e dell'indirizzo MAC corrispondente.

Gli attacchi MITM

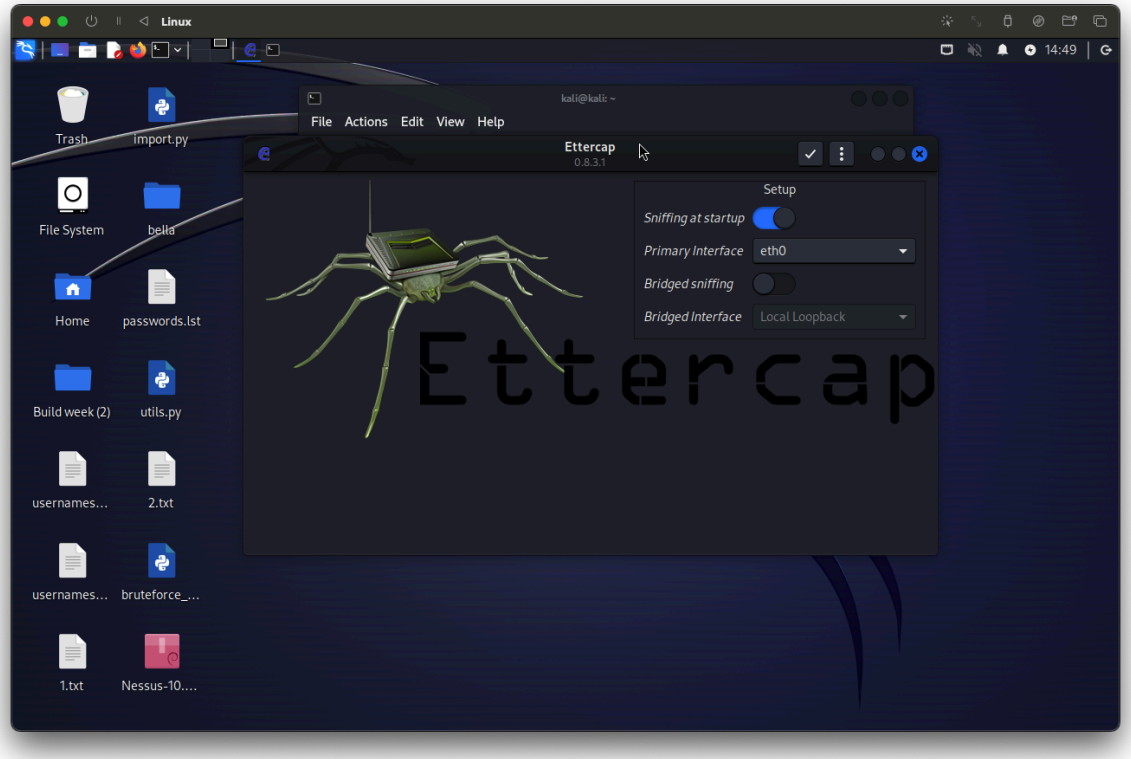
Un attacco Man-in-the-Middle (MITM) è una tipologia di attacco informatico in cui un aggressore si inserisce in una comunicazione tra due parti legittime e la intercetta o controlla attivamente la comunicazione. In sostanza, l'attaccante si posiziona "nel mezzo" della comunicazione, consentendogli di intercettare, inviare e ricevere dati destinati all'entità legittima senza che le parti coinvolte ne siano consapevoli

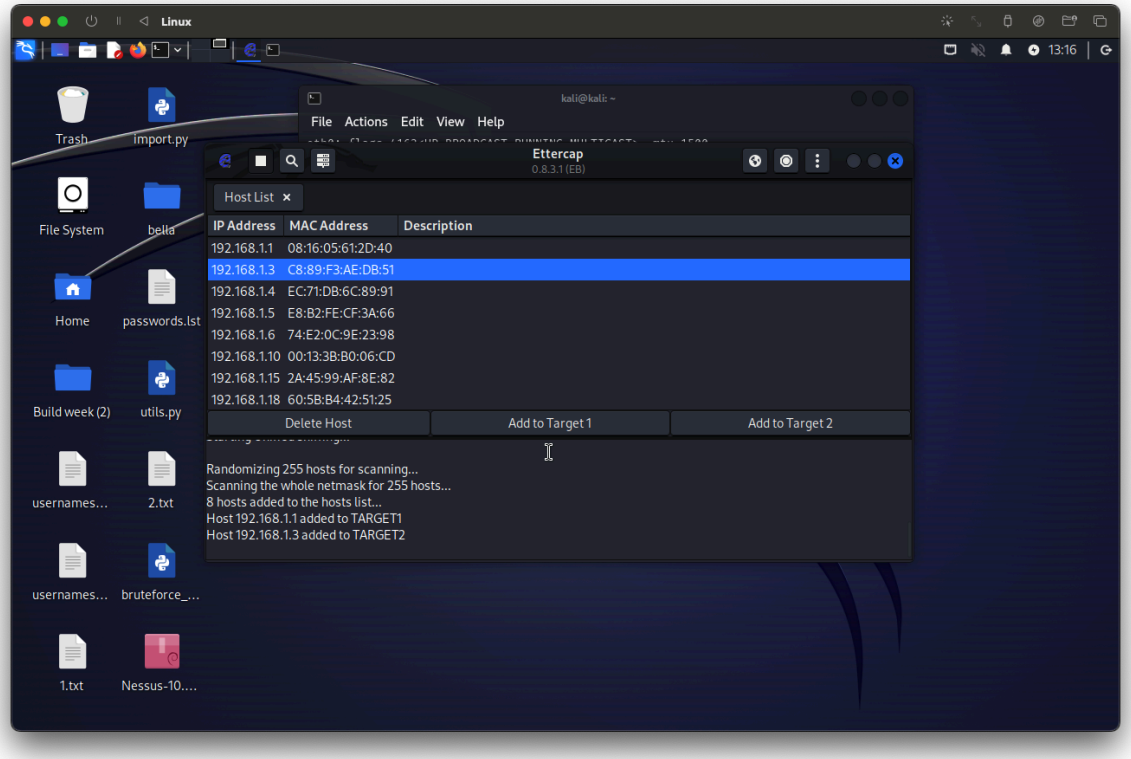
ARP poisoning

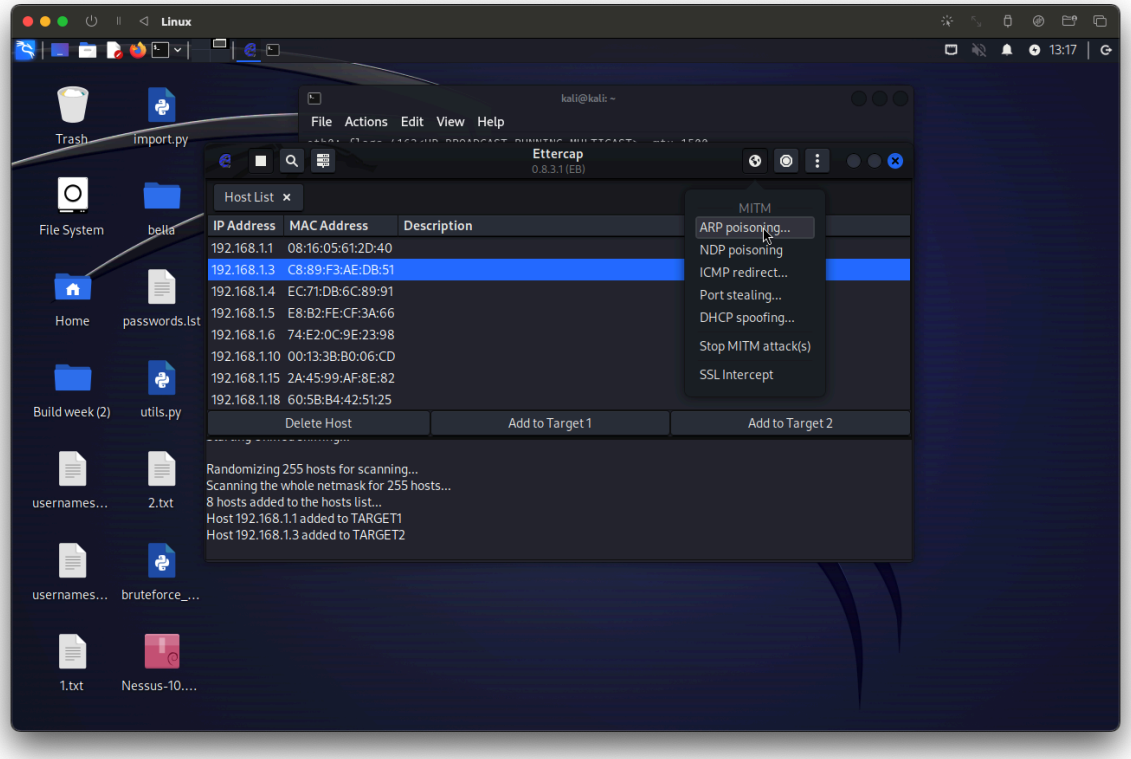
ARP Poisoning (Address Resolution Protocol Poisoning): Questo tipo di attacco coinvolge la manipolazione della tabella di traduzione degli indirizzi IP nei pacchetti di rete. In un attacco ARP Poisoning, l'attaccante invia pacchetti ARP falsificati nella rete locale, in modo che il traffico destinato a un determinato indirizzo MAC venga deviato verso l'attaccante anziché verso il destinatario previsto. Ciò consente all'attaccante di intercettare e modificare il traffico di rete tra due host.

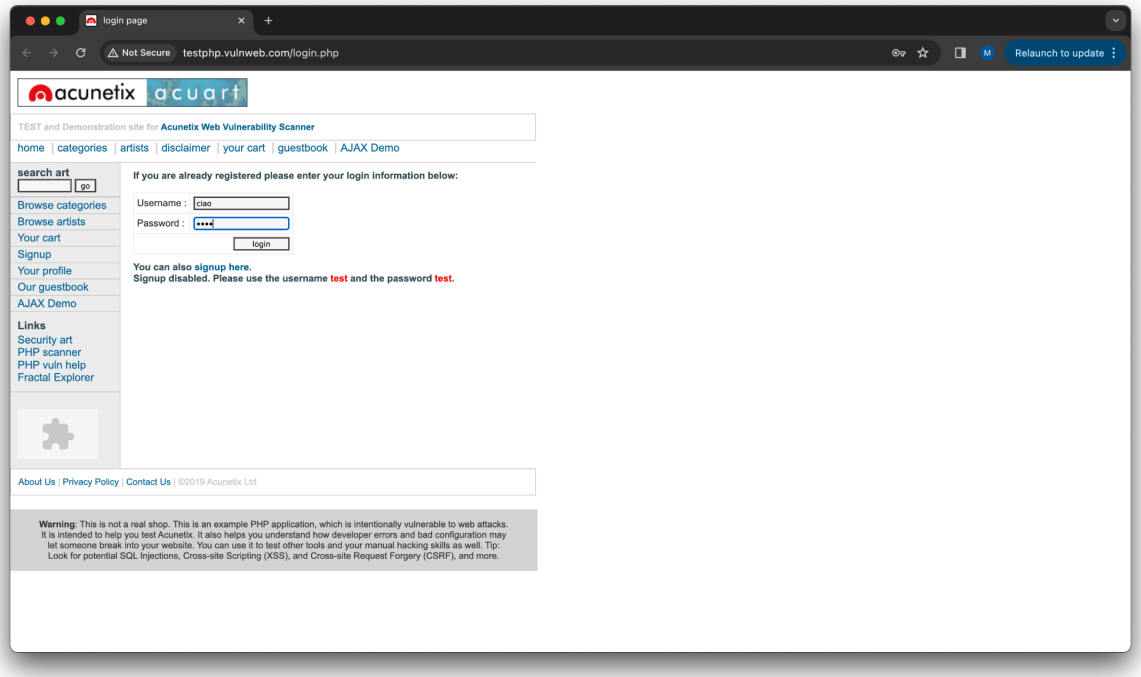
Un esempio di arp poisoning

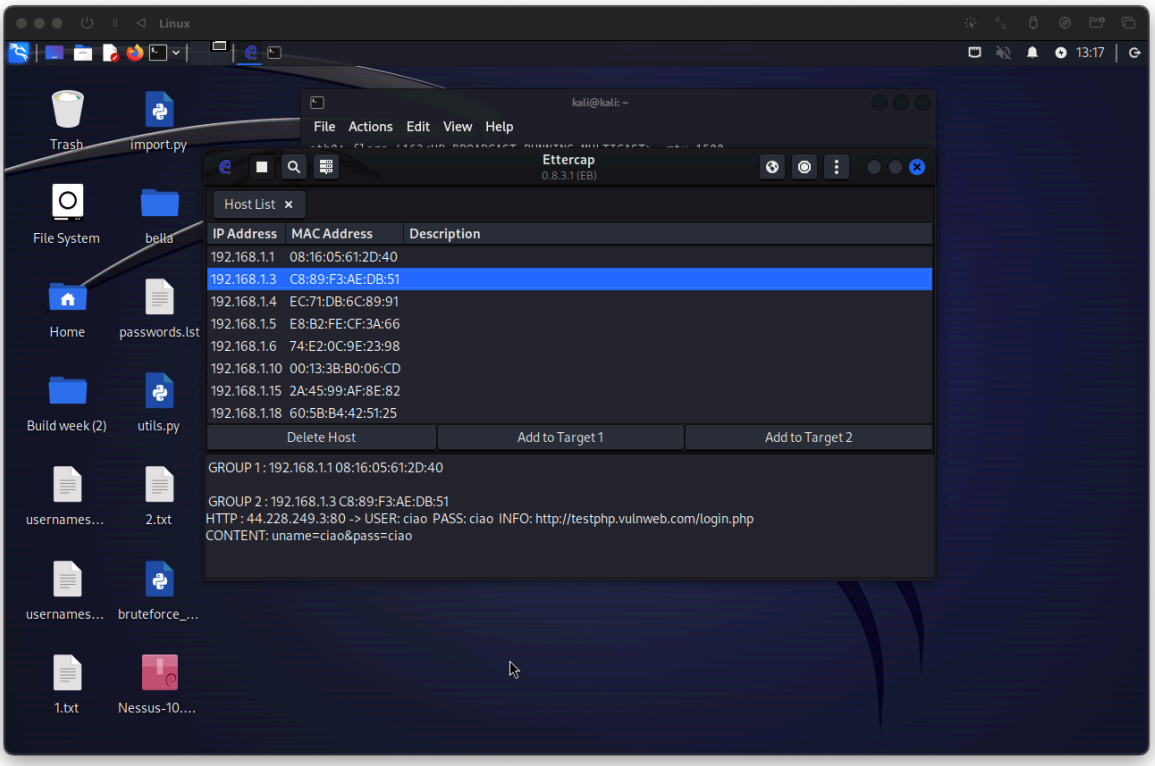
Attraverso Ettercap possiamo effettuare un attacco di arp poisoning, occorre prima di tutto individuare gli host all’interno della rete e successivamente i due target, attraverso il programma mi pongo in mezzo ai due target e “ascolto” quello che viene mandato.


Linux
14:49
kali@kali: ~
File Actions Edit View Help
Ettercap
0.8.3.1
Setup
Sniffing at startup
Primary Interface
eth0
Bridged sniffing
Bridged Interface
Local Loopback
Ettercap
Trash
import.py
File System
bella
Home
passwords.lst
Build week (2)
utils.py
usernames...
2.txt
usernames...
bruteforce_...
1.txt
Nessus-10....


Linux
13:16
kali@kali: ~
File Actions Edit View Help
Ettercap
0.8.3.1 (EB)
Host List
IP Address MAC Address Description
192.168.1.1 08:16:05:61:2D:40
192.168.1.3 C8:89:F3:AE:DB:51
192.168.1.4 EC:71:DB:6C:89:91
192.168.1.5 E8:B2:FE:CF:3A:66
192.168.1.6 74:E2:0C:9E:23:98
192.168.1.10 00:13:3B:B0:06:CD
192.168.1.15 2A:45:99:AF:8E:82
192.168.1.18 60:5B:B4:42:51:25
Delete Host
Add to Target 1
Add to Target 2
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
8 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET1
Host 192.168.1.3 added to TARGET2
Trash
import.py
File System
bella
Home
passwords.lst
Build week (2)
utils.py
usernames...
2.txt
usernames...
bruteforce_...
1.txt
Nessus-10....


Linux
13:17
Trash
import.py
File System
bella
Home
passwords.lst
Build week (2)
utils.py
usernames...
2.txt
usernames...
bruteforce_...
1.txt
Nessus-10....
kali@kali: ~
File Actions Edit View Help
Ettercap
0.8.3.1 (EB)
Host List
IP Address MAC Address Description
192.168.1.1 08:16:05:61:2D:40
192.168.1.3 C8:89:F3:AE:DB:51
192.168.1.4 EC:71:DB:6C:89:91
192.168.1.5 E8:B2:FE:CF:3A:66
192.168.1.6 74:E2:0C:9E:23:98
192.168.1.10 00:13:3B:B0:06:CD
192.168.1.15 2A:45:99:AF:8E:82
192.168.1.18 60:5B:B4:42:51:25
Delete Host
Add to Target 1
Add to Target 2
MITM
ARP poisoning...
NDP poisoning
ICMP redirect...
Port stealing...
DHCP spoofing...
Stop MITM attack(s)
SSL Intercept
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
8 hosts added to the hosts list...
Host 192.168.1.1 added to TARGET1
Host 192.168.1.3 added to TARGET2


login page
Not Secure
testphp.vulnweb.com/login.php
Relaunch to update
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 : ciao
Password : ••••
login
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.



Come è possibile notare, una volta inseriti i dati di login, appaiono all'interno di ettercap.