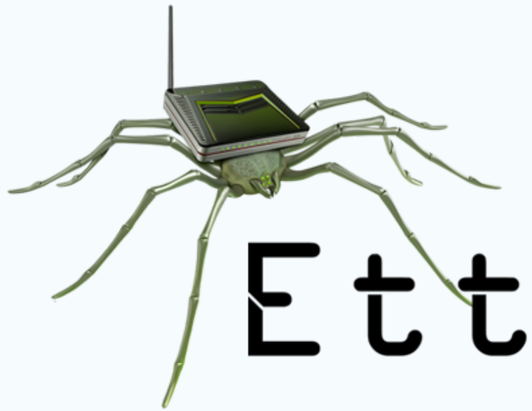
ETTERCAP
COMPITO S6-L1



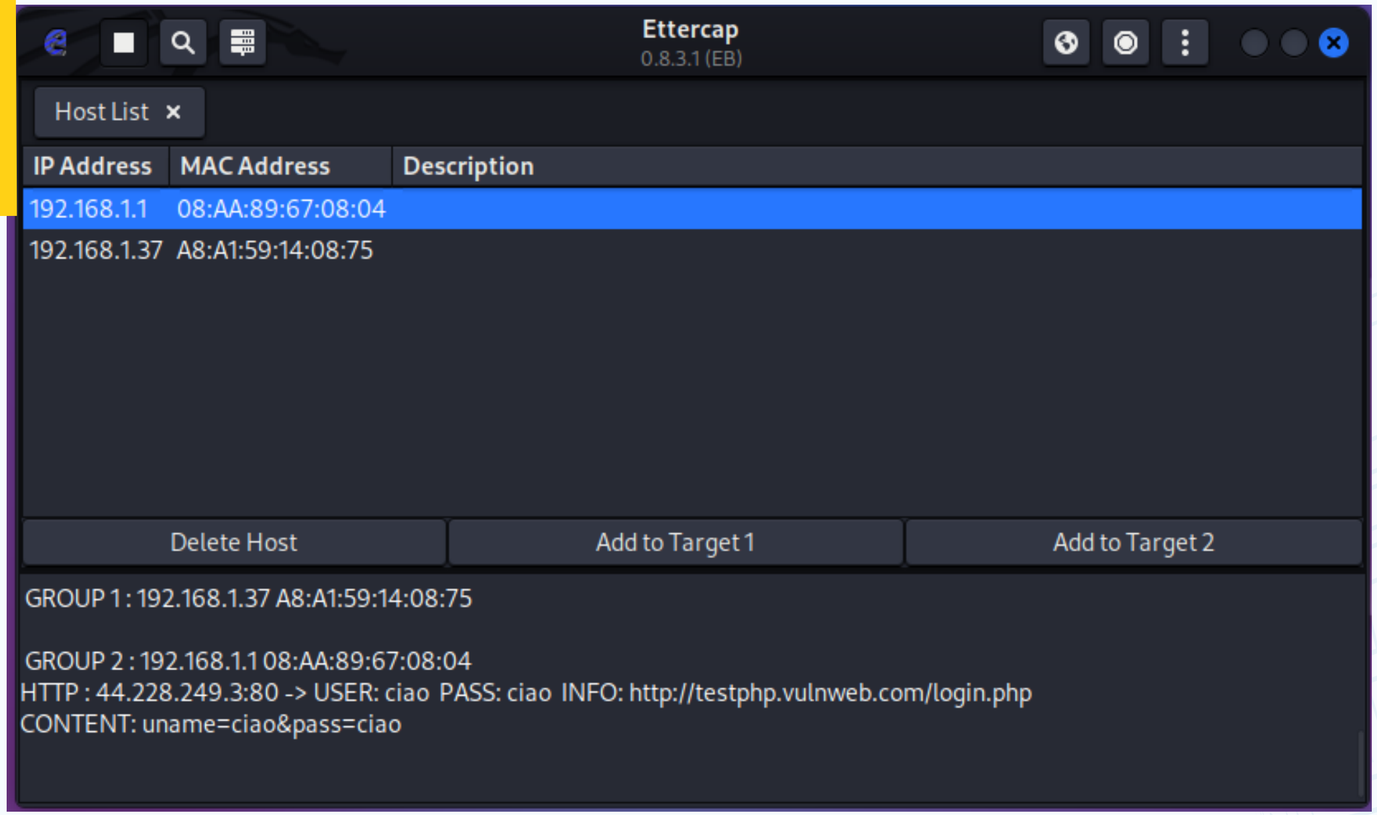
ETTERCAP

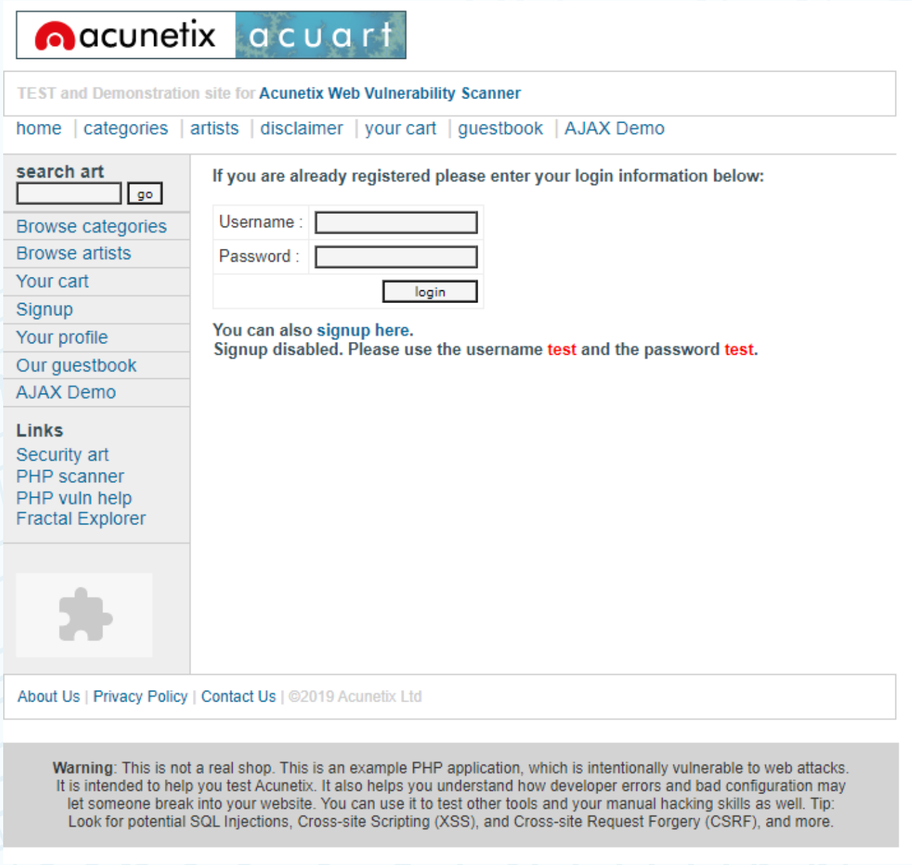
Cos'è Ettercap?

Ettercap è uno strumento open-source ampiamente utilizzato per la sicurezza e il monitoraggio delle reti. È progettato per eseguire attacchi di tipo man-in-the-middle nelle reti locali (LAN).

Può intercettare, registrare ed analizzare il traffico di rete in tempo reale. È importante notare che l'uso di tali strumenti per scopi non autorizzati o su reti senza permesso è illegale e contro le norme etiche.

PROJECT


Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.1.1 08:AA:89:67:08:04
192.168.1.37 A8:A1:59:14:08:75
Delete Host
Add to Target 1
Add to Target 2
GROUP 1 : 192.168.1.37 A8:A1:59:14:08:75
GROUP 2 : 192.168.1.1 08:AA:89:67:08:04
HTTP : 44.228.249.3:80 -> USER: ciao PASS: ciao INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=ciao&pass=ciao


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 :
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.

REPORT

01 Il protocollo ARP (Address Resolution Protocol) è un protocollo di rete utilizzato per associare un indirizzo IP a un indirizzo MAC (Media Access Control) all'interno di una rete locale. Quando un dispositivo deve comunicare con un altro sulla stessa rete, utilizza ARP per ottenere l'indirizzo MAC associato all'indirizzo IP di destinazione.

02 Gli attacchi MITM (Man-in-the-Middle) sono una categoria di attacchi in cui un attaccante si colloca tra due parti che stanno cercando di comunicare, intercettando e potenzialmente modificando il traffico tra di loro senza che le parti coinvolte se ne accorgano.

03 L'attacco ARP-Poisoning, noto anche come attacco ARP Spoofing o ARP Cache Poisoning, è un tipo di attacco MITM che sfrutta le debolezze nel protocollo ARP. In questo attacco, l'attaccante invia pacchetti ARP falsificati (spoofati) alla rete, inducendo i dispositivi a associare un indirizzo IP legittimo a un indirizzo MAC controllato dall'attaccante. Questo consente all'attaccante di intercettare o manipolare il traffico tra i dispositivi.

LE FASI DELL'ATTACCO.

- Raccolta di informazioni: L'attaccante esegue la scansione della rete per identificare gli indirizzi IP e MAC degli altri dispositivi sulla stessa rete.
- Inondazione ARP falsificata: L'attaccante invia pacchetti ARP contenenti informazioni falsificate sulla corrispondenza tra indirizzi IP e MAC. Questo può essere fatto in modo continuo per mantenere aggiornata la cache ARP dei dispositivi target.
- Ascolto del traffico: Una volta che la cache ARP è stata avvelenata, l'attaccante può intercettare il traffico tra le vittime senza che esse se ne accorgano.
- Possibili azioni: L'attaccante può ora eseguire varie azioni, come il monitoraggio del traffico per raccogliere informazioni sensibili o l'iniezione di pacchetti malevoli nella comunicazione tra le vittime.