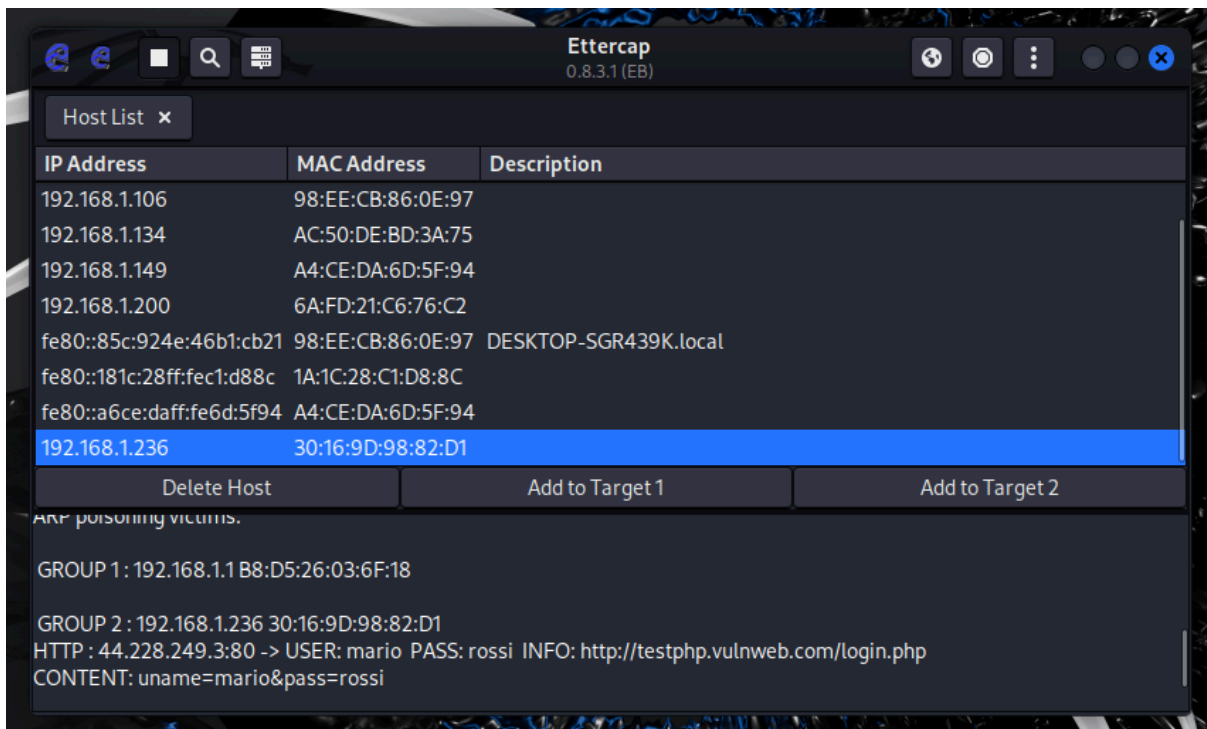
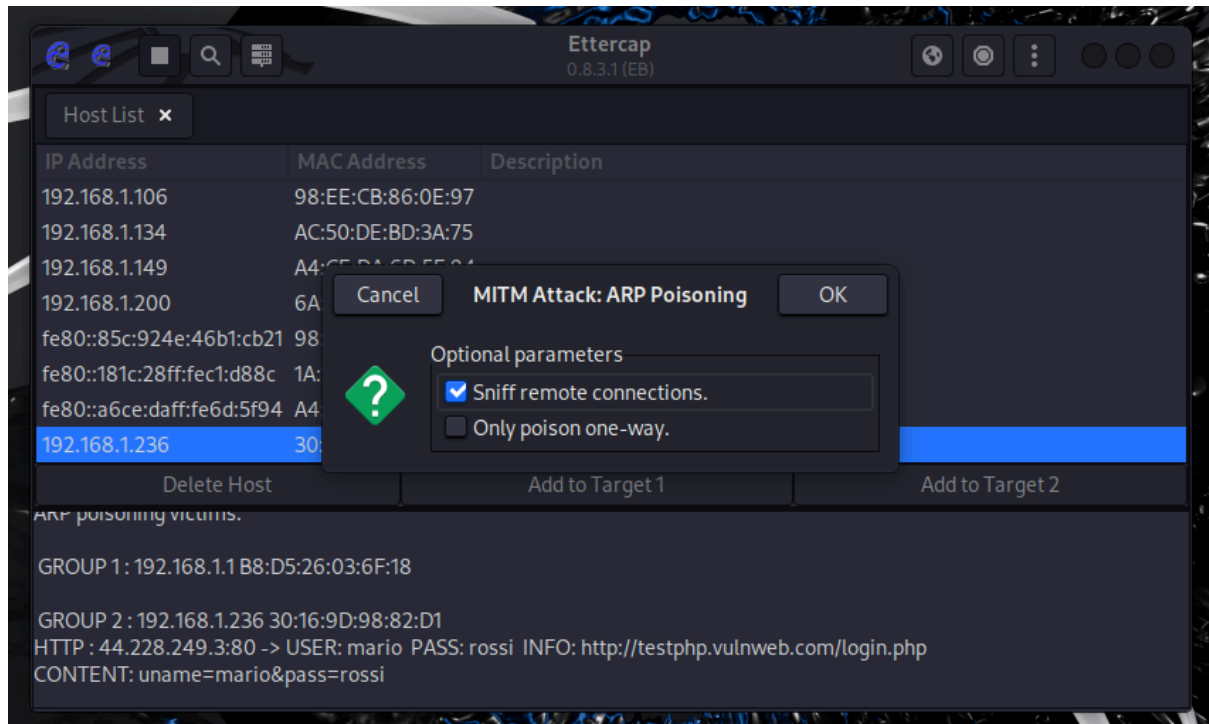


scansione hosts 192.168.1.1 gateway e 192.168.1.236 pc host (attuale)



## ARP POISONING



PRIMA

```
Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.5854]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Stefano>arp -a

Interfaccia: 192.168.1.236 --- 0x4
Indirizzo Internet    Indirizzo fisico      Tipo
192.168.1.1           b8-d5-26-03-6f-18    dinamico
192.168.1.134         ac-50-de-bd-3a-75    dinamico
192.168.1.149         a4-ce-da-6d-5f-94    dinamico
192.168.1.190         08-00-27-6e-13-6e    dinamico
192.168.1.255         ff-ff-ff-ff-ff-ff    statico
224.0.0.5             01-00-5e-00-00-05    statico
224.0.0.22            01-00-5e-00-00-16    statico
224.0.0.251          01-00-5e-00-00-fb    statico
224.0.0.252          01-00-5e-00-00-fc    statico
239.255.102.18        01-00-5e-7f-66-12    statico
239.255.255.250       01-00-5e-7f-ff-fa    statico
255.255.255.255       ff-ff-ff-ff-ff-ff    statico

Interfaccia: 192.168.56.1 --- 0x13
Indirizzo Internet    Indirizzo fisico      Tipo
192.168.56.255        ff-ff-ff-ff-ff-ff    statico
224.0.0.5             01-00-5e-00-00-05    statico
224.0.0.22            01-00-5e-00-00-16    statico
224.0.0.251          01-00-5e-00-00-fb    statico
224.0.0.252          01-00-5e-00-00-fc    statico
239.255.255.250       01-00-5e-7f-ff-fa    statico

C:\Users\Stefano>arp -a
```

DOPO

```
Prompt dei comandi

239.255.255.250       01-00-5e-7f-ff-fa    statico

C:\Users\Stefano>arp -a

Interfaccia: 192.168.1.236 --- 0x4
Indirizzo Internet    Indirizzo fisico      Tipo
192.168.1.1           08-00-27-6e-13-6e    dinamico
192.168.1.134         ac-50-de-bd-3a-75    dinamico
192.168.1.149         a4-ce-da-6d-5f-94    dinamico
192.168.1.190         08-00-27-6e-13-6e    dinamico
192.168.1.255         ff-ff-ff-ff-ff-ff    statico
224.0.0.5             01-00-5e-00-00-05    statico
224.0.0.22            01-00-5e-00-00-16    statico
224.0.0.251          01-00-5e-00-00-fb    statico
224.0.0.252          01-00-5e-00-00-fc    statico
239.255.102.18        01-00-5e-7f-66-12    statico
239.255.255.250       01-00-5e-7f-ff-fa    statico
255.255.255.255       ff-ff-ff-ff-ff-ff    statico

Interfaccia: 192.168.56.1 --- 0x13
Indirizzo Internet    Indirizzo fisico      Tipo
192.168.56.255        ff-ff-ff-ff-ff-ff    statico
224.0.0.5             01-00-5e-00-00-05    statico
224.0.0.22            01-00-5e-00-00-16    statico
224.0.0.251          01-00-5e-00-00-fb    statico
224.0.0.252          01-00-5e-00-00-fc    statico
239.255.255.250       01-00-5e-7f-ff-fa    statico

C:\Users\Stefano>arp -a
```

CAMBIA INDIRIZZO MAC CON QUELLO DI KALI (sul gateway 192.168.1.1)

kali-linux-2024.4-virtualbox-amd64 (la vera VM) [In esecuzione] - Oracle VirtualBox

File Machine Visualizza Impostazioni Dispositivi Aiuto

\*eth0



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
277	9.93113626	PCSSystemtec_6e:13:: ZyxelCommuni_03:6f:: ARP	42 192.168.1.236 is at 08:00:27:6e:13:6e			
287	9.93149881	PCSSystemtec_6e:13:: MercusysTech_98:82:: ARP	42 192.168.1.1 is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.236 detected!)			
140	17.940321289	PCSSystemtec_6e:13:: ZyxelCommuni_03:6f:: ARP	42 192.168.1.236 is at 08:00:27:6e:13:6e			
147	17.940348432	PCSSystemtec_6e:13:: MercusysTech_98:82:: ARP	42 192.168.1.1 is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.236 detected!)			
195	25.69688415	PCSSystemtec_6e:13:: ZyxelCommuni_03:6f:: ARP	42 Who has 192.168.1.1? Tell 192.168.1.198			
196	25.71271725	ZyxelCommuni_03:6f:: PCSSystemtec_6e:13:: ARP	60 192.168.1.1 is at b8:d5:26:03:6f:18			
198	27.959541898	PCSSystemtec_6e:13:: ZyxelCommuni_03:6f:: ARP	42 192.168.1.236 is at 08:00:27:6e:13:6e			
199	27.95971463	PCSSystemtec_6e:13:: MercusysTech_98:82:: ARP	42 192.168.1.1 is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.236 detected!)			
297	37.960772488	PCSSystemtec_6e:13:: ZyxelCommuni_03:6f:: ARP	42 192.168.1.236 is at 08:00:27:6e:13:6e			
298	37.960883963	PCSSystemtec_6e:13:: MercusysTech_98:82:: ARP	42 192.168.1.1 is at 08:00:27:6e:13:6e (duplicate use of 192.168.1.236 detected!)			

wireshark.

Una volta configurato Ettercap, scegliamo un sito in HTTP e testiamo un attacco MITM.

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.

Ettercap  
0.8.3.1 (EB)

Host List x

IP Address	MAC Address	Description
192.168.1.106	98:EE:CB:86:0E:97	
192.168.1.134	AC:50:DE:BD:3A:75	
192.168.1.149	A4:CE:DA:6D:5F:94	
192.168.1.200	6A:FD:21:C6:76:C2	
fe80::85c:924e:46b1:cb21	98:EE:CB:86:0E:97	DESKTOP-SGR439K.local
fe80::181c:28ff:fec1:d88c	1A:1C:28:C1:D8:8C	
fe80::a6ce:daff:fe6d:5f94	A4:CE:DA:6D:5F:94	
192.168.1.236	30:16:9D:98:82:D1	

Delete Host

Add to Target 1

Add to Target 2

GROUP 2 : 192.168.1.236 30:16:9D:98:82:D1

HTTP : 44.228.249.3:80 -> USER: mario PASS: rossi INFO: http://testphp.vulnweb.com/login.php  
CONTENT: uname=mario&pass=rossi

HTTP : 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php  
CONTENT: uname=test&pass=test

usando il sito: <http://testphp.vulnweb.com/login.php> e inserendo delle credenziali, vedremo ciò su Ettercap.

### **NULL Session**

La vulnerabilità Null Session su Windows è una vulnerabilità di sicurezza che consente a un attaccante di accedere a informazioni sensibili sui sistemi Windows, come nomi di account utente, password e informazioni di condivisione delle risorse. Questa vulnerabilità si verifica quando un client Windows si connette a un server Windows utilizzando un'identità vuota, ovvero senza specificare alcuna credenziale di accesso. La vulnerabilità Null Session colpisce i sistemi operativi Windows NT, Windows 2000, Windows XP e Windows Server 2003. Tuttavia, è importante notare che è stata risolta in versioni successive dei sistemi operativi Windows e che molti amministratori di sistema di Windows hanno adottato misure di sicurezza per mitigare questa vulnerabilità.

Per mitigare questa vulnerabilità, è possibile adottare i seguenti metodi:

1. Disabilitare la condivisione file e stampanti su Windows: eliminare completamente la condivisione su tutti i computer e server della rete. Estirpo il problema alla radice, ma le aziende usano la condivisione dei file e non è un'ottima soluzione.
2. Disabilitare il supporto per NetBIOS su TCP/IP: questo riduce il numero di porte aperte sul sistema e rimuove il supporto per il protocollo NetBIOS che è vulnerabile alla null session.
3. Utilizzare il filtro del traffico di rete: i firewall bloccano i tentativi di connessione remota non autorizzati e filtrano le connessioni in ingresso sulla base delle porte che tentano di utilizzare. Il monitoraggio di rete è una delle pratiche di sicurezza sempre raccomandate.
4. Disattivare l'account Guest: l'account guest consente l'accesso alle risorse della rete senza richiedere alcuna credenziale. Disabilitare l'account Guest può limitare l'accesso di utenti non autorizzati. Certamente un'ottima soluzione, da applicare in ogni caso.
5. Aggiornare il sistema operativo: Microsoft rilascia regolarmente gli aggiornamenti di sicurezza per il sistema operativo Windows. Assicurarsi di aver installato l'ultimo aggiornamento di sicurezza per mitigare i rischi di vulnerabilità. Con una patch l'effort per l'azienda è basso. Passare ad un sistema operativo più moderno è oneroso a livello di configurazione e richieste hardware.
6. Configurare le autorizzazioni di condivisione file: limita l'accesso alle risorse ai soli utenti specifici che ne hanno bisogno, utilizzando i permessi appropriati. Questo evita il potenziale accesso non autorizzato. Certamente un ottimo sistema e una best practice in ogni caso, non sempre applicato nelle aziende medio/piccole.
7. Utilizzare un software di sicurezza: implementare un software di sicurezza per i sistemi Windows che possa monitorare e prevenire l'accesso non autorizzato. Fa parte delle soluzioni base da applicare sempre. Possono esserci anche altre azioni di mitigazione, ad esempio intervenire sul registro di Windows.

## **ARP Poisoning**

L'attacco ARP Poisoning è una tecnica malevola utilizzata per intercettare, analizzare o manipolare il traffico di rete all'interno di una LAN (rete locale). Questo attacco sfrutta il protocollo ARP Address Resolution Protocol per inviare informazioni ARP false sulla rete, promuovendo il proprio indirizzo MAC come il legittimo indirizzo MAC del router o di un'altra macchina. Ciò consente all'attaccante di intercettare il traffico di rete tra le macchine e il router o di dirottare questo traffico ogni volta che una macchina invia un pacchetto al gateway o al router. L'attacco ARP Poisoning colpisce esclusivamente i sistemi all'interno di una LAN, in particolare tutte le macchine che utilizzano lo stesso gateway e lo stesso indirizzo IP di rete. In altre parole, gli utenti all'interno della stessa rete locale saranno vulnerabili all'attacco ARP Poisoning.

Esistono diverse tecniche per mitigare questo tipo di attacco:

1. Utilizzo di protocolli di sicurezza: i protocolli come HTTPS, SSL, TLS o VPN crittografano i dati in transito e impediscono agli attaccanti di leggerli o manipolarli.
2. Utilizzare Switch livello 3: in questo modo si divide la rete in sottoreti, ma gli switch layer 3 hanno un costo maggiore e richiedono configurazione.
3. Monitoraggio costante: controllare regolarmente la rete per individuare eventuali intrusioni, come accessi non autorizzati o attacchi di ARP poisoning.
4. Utilizzo di software per la sicurezza: alcuni software antivirus e anti-malware possono individuare e prevenire attacchi ARP poisoning.
5. Educazione del personale: informare gli utenti sulla sicurezza informatica e sui rischi di attacchi come l'ARP poisoning può aiutare a prevenire incidenti. Informare gli utenti che non tutto il traffico può essere lecito.

## **Monitoraggio di rete**

Diversi produttori di software offrono anche dei programmi di monitoring con i quali si possono controllare le reti e rilevare i procedimenti ARP insoliti.

Ad esempio: Arpwatch XArp

Altrimenti possiamo usare l'IDS Snort per effettuare il monitoraggio