ARP poisoning

Address Resolution Protocol (ARP) este un protocol de telecomunicatii utilizat pentru translarea adreselor de pe nivelul retea (adrese IP) in adrese de pe nivelul legatura de date (adrese MAC).

Media access control address sau adresa MAC este un identificator unic atribuit interfetei de retea pentru comunicatii pe nivelul fizic. Adresa MAC are 6 bytes si are forma XX:XX:XX:XX:XX:XX (de exemplu 01:23:45:67:89:ab).

Comunicarea intre retele se realizeaza pe baza IP-urilor, in interiorul retelei se realizeaza pe baza MAC-ului. Dar, cand va conectati (chiar in interiorul retelei), nu furnizati adresa MAC a calculatorului destinatie ci adresa IP. ARP va transla adresa IP intr-o adresa MAC , pe baza unei tabele ARP. Fiecare calculator are o tabela (denumita tabela ARP) in care sunt asociate adresele IP cu adresele MAC ale calculatoarelor din aceeasi retea.

Instalati pe cele 3 masini pachetele net-tools, iptables:

sudo apt-get install net-tools
sudo apt-get install iptables

Instalati pe MV C1 pachetele wireshark, ettercap:

sudo apt-get install wireshark
sudo apt-get install ettercap-graphical

Pentru a vizualiza tabela ARP

arp

Ar trebui ca in tabela ARP sa vedeti asocierile dintre adresele IP si adresele MAC a celorlalte 2 masini virtuale (daca nu le vizualizati pe amandoua dati ping catre cea care lipseste)

Wireshark este un tool care realizeaza sniffing de pachete.
Un ghid pentru Wireshark poate fi gasit aici :
https://www.wireshark.org/download/docs/user-guide-a4.pdf

OBS: daca in wireshark (Capture interfaces) nu apare nici o interfata atunci executati urmatoarele comenzi pentru a avea drepturi de acces corespunzatoare, dupa care porniti masina:

sudo addgroup -system wireshark
sudo chown root:wireshark /usr/bin/dumpcap
sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
sudo usermod -a -G wireshark *YOUR_USER_NAME*
sudo poweroff

Ettercap este un tool cu ajutorul caruia se pot realiza diverse atacuri la nivel retea, printre care si cel cerut in exercitiu.

Exercitiu:

1. **Implementarea unui atac MITM ARP poisoning (**modificarea adreselor MAC a 2 victime de catre un intrus) **utilizand Ettercap** si **Wireshark.**
   - Presupunem ca victimele sunt MV C2 si Proxy, intrusul este MV C1 (C1 va intercepta comunicarea intre C2 si Proxy);
2. **Obtineti datele de logare (user, parola) ale unui utilizator** (C2) care acceseaza o pagina web de login (HTTP) sau un server FTP nesecurizat.