**Atacul tabelului de adrese MAC**

**Revizuirea operațiunii comutatorului**

În acest subiect, accentul este încă pus pe comutatoare, în special pe tabelele lor de adrese MAC și pe modul în care aceste tabele sunt vulnerabile la atacuri.

Amintiți-vă că pentru a lua decizii de redirecționare, un comutator LAN de nivel 2 construiește un tabel bazat pe adresele MAC sursă din cadrele primite. Prezentat în figură, acesta se numește tabel de adrese MAC. Tabelele de adrese MAC sunt stocate în memorie și sunt folosite pentru a transmite mai eficient cadrele.

**S1# show mac address-table dynamic**

**Mac Address Table**

**-------------------------------------------**

**Vlan Mac Address Type Ports**

**---- ----------- -------- -----**

**1 0001.9717.22e0 DYNAMIC Fa0/4**

**1 000a.f38e.74b3 DYNAMIC Fa0/1**

**1 0090.0c23.ceca DYNAMIC Fa0/3**

**1 00d0.ba07.8499 DYNAMIC Fa0/2**

**S1#**

**Inundarea tabelului de adrese MAC**

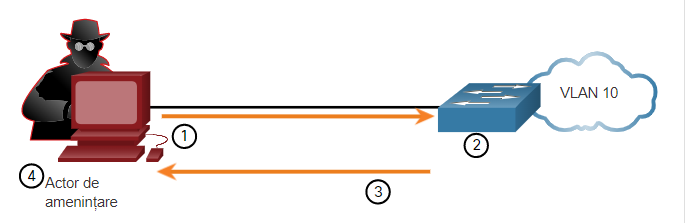
Toate tabelele MAC au o dimensiune fixă ​​și, în consecință, un comutator poate rămâne fără resurse în care să stocheze adrese MAC. Atacurile de inundare a adreselor MAC profită de această limitare bombardând comutatorul cu adrese MAC sursă false până când tabelul de adrese MAC al comutatorului este plin.

Când se întâmplă acest lucru, comutatorul tratează cadrul ca un unicast necunoscut și începe să inunde tot traficul de intrare în toate porturile de pe același VLAN fără a face referire la tabelul MAC. Această condiție permite acum unui actor de amenințare să captureze toate cadrele trimise de la o gazdă la alta pe LAN local sau VLAN local.

**Notă** : Traficul este inundat numai în rețeaua locală LAN sau VLAN. Actorul amenințării poate capta numai traficul în LAN-ul local sau VLAN-ul la care este conectat actorul amenințării.

Figura arată cum un actor de amenințare poate folosi cu ușurință instrumentul de atac de rețea **macof** pentru a depăși un tabel de adrese MAC.

Figura prezintă un actor de amenințare cu un computer conectat la un comutator cu un nor lângă el etichetat V LAN 10.



1. Actorul amenințării este conectat la VLAN 10 și folosește **macof** pentru a genera rapid multe adrese aleatoare sursă și destinație MAC și IP.
2. Într-o perioadă scurtă de timp, tabelul MAC al comutatorului se umple.
3. Când tabelul MAC este plin, comutatorul începe să inunde toate cadrele pe care le primește. Atâta timp cât **macof** continuă să ruleze, tabelul MAC rămâne plin și comutatorul continuă să inunde toate cadrele de intrare în fiecare port asociat cu VLAN 10.
4. Actorul amenințării folosește apoi un software de detectare a pachetelor pentru a captura cadre de pe oricare și toate dispozitivele conectate la VLAN 10.

Dacă actorul amenințării oprește **rularea macof** sau este descoperit și oprit, comutatorul în cele din urmă îndepărtează intrările de adrese MAC mai vechi din tabel și începe să se comporte din nou ca un comutator.

**Atenuarea atacurilor din tabelul de adrese MAC**

Ceea ce face ca instrumente precum **macof** să fie atât de periculoase este că un atacator poate crea un atac de depășire a tabelului MAC foarte rapid. De exemplu, un comutator Catalyst 6500 poate stoca 132.000 de adrese MAC în tabelul său de adrese MAC. Un instrument precum **macof** poate inunda un comutator cu până la 8.000 de cadre false pe secundă; crearea unui atac de depășire a tabelului de adrese MAC în câteva secunde. Exemplul arată un exemplu de ieșire a comenzii **macof** pe o gazdă Linux.

**# macof -i eth1**

**36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512**

**16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512**

**18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512**

**e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512**

**62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512**

**c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512**

**88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512**

**b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512**

**e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512**

Un alt motiv pentru care aceste instrumente de atac sunt periculoase este pentru că nu afectează doar comutatorul local, ci pot afecta și alte comutatoare Layer 2 conectate. Când tabelul de adrese MAC al unui switch este plin, acesta începe să inunde toate porturile, inclusiv cele conectate la alte switch-uri de Layer 2.

Pentru a atenua atacurile de depășire a tabelului de adrese MAC, administratorii de rețea trebuie să implementeze securitatea porturilor. Securitatea portului va permite doar un anumit număr de adrese MAC sursă să fie învățate pe port. Securitatea porturilor este discutată în continuare într-un alt modul.