**Amenințări de securitate de nivel 2**

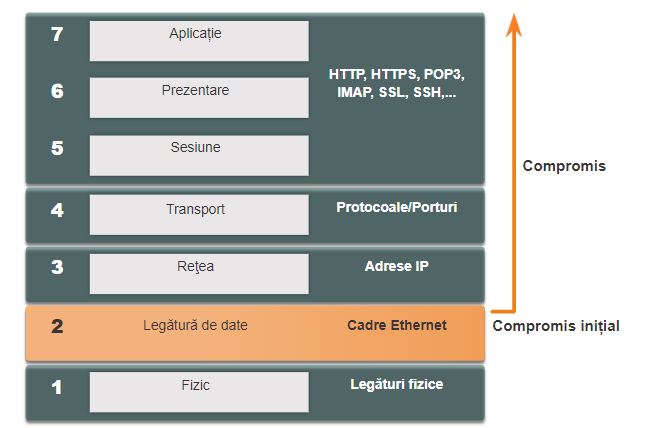
**Vulnerabilități de nivel 2**

Cele două subiecte anterioare au discutat despre securizarea punctelor finale. În acest subiect, veți continua să aflați despre modalități de securizare a rețelei LAN concentrându-vă asupra cadrelor găsite în stratul de legătură de date (Layer 2) și comutator.

Reamintim că modelul de referință OSI este împărțit în șapte straturi care funcționează independent unul de celălalt. Figura prezintă funcția fiecărui strat și elementele de bază care pot fi exploatate.

Administratorii de rețea implementează în mod obișnuit soluții de securitate pentru a proteja elementele din Layer 3 până la Layer 7. Ei folosesc VPN-uri, firewall-uri și dispozitive IPS pentru a proteja aceste elemente. Cu toate acestea, dacă Stratul 2 este compromis, atunci toate straturile de deasupra acestuia sunt și ele afectate. De exemplu, dacă un actor de amenințare cu acces la rețeaua internă a capturat cadre de Layer 2, atunci toată securitatea implementată pe straturile de mai sus ar fi inutilă. Actorul amenințării ar putea provoca multe daune asupra infrastructurii de rețea LAN de nivel 2.

Diagrama arată numărul, numele și alte informații legate de straturile OSI de sus în jos: 7 - aplicație, 6 - prezentare, 5 - sesiune, 4 - transport, 3 - Rețea, 2 - legătură de date și 1 - fizică . Acesta arată un compromis inițial al cadrelor Ethernet la nivelul 2, cu o săgeată care indică că toate straturile de mai sus au fost de asemenea compromise.



**Comutați categoriile de atac**

Securitatea este la fel de puternică ca și cea mai slabă verigă din sistem, iar stratul 2 este considerat a fi acea verigă slabă. Acest lucru se datorează faptului că LAN-urile erau în mod tradițional sub controlul administrativ al unei singure organizații. Am avut încredere în mod inerent în toate persoanele și dispozitivele conectate la LAN-ul nostru. Astăzi, cu BYOD și atacuri mai sofisticate, rețelele LAN au devenit mai vulnerabile la penetrare. Prin urmare, pe lângă protejarea de la Layer 3 la Layer 7, profesioniștii în securitatea rețelei trebuie, de asemenea, să atenueze atacurile asupra infrastructurii LAN de Layer 2.

Primul pas în atenuarea atacurilor asupra infrastructurii Layer 2 este înțelegerea funcționării de bază a Layer 2 și a amenințărilor reprezentate de Layer 2.

Atacurile împotriva infrastructurii LAN de nivel 2 sunt descrise în tabel și sunt discutate mai detaliat mai târziu în acest modul.

**Atacurile de strat 2**

|  |  |
| --- | --- |
| **Categorie** | **Exemple** |
| **Atacurile MAC Table** | Include atacuri de inundare a adresei MAC. |
| **Atacurile VLAN** | Include atacuri de salt VLAN și atacuri cu etichetare dublă VLAN. De asemenea, include atacuri între dispozitive pe un VLAN comun. |
| **Atacurile DHCP** | Include înfometarea DHCP și atacurile de falsificare DHCP. |
| **Atacurile ARP** | Include spoofing ARP și atacuri de otrăvire ARP. |
| **Abordați atacurile de falsificare** | Include atacuri de falsificare a adresei MAC și a adresei IP. |
| **Atacurile STP** | Include atacuri de manipulare Spanning Tree Protocol. |

**Schimbarea tehnicilor de atenuare a atacurilor**

Tabelul oferă o prezentare generală a soluțiilor Cisco pentru a ajuta la atenuarea atacurilor de nivel 2.

Nivelul 2 de atenuare a atacurilor

|  |  |
| --- | --- |
| Legenda tabelului | |
| **Soluţie** | **Descriere** |
| **Securitatea Portului** | Previne multe tipuri de atacuri, inclusiv atacurile de inundare a adresei MAC și atacurile de foame DHCP. |
| **Snooping DHCP** | Previne înfometarea DHCP și atacurile de falsificare DHCP. |
| **Inspecție dinamică ARP (DAI)** | Previne falsificarea ARP și atacurile de otrăvire ARP. |
| **IP Source Guard (IPSG)** | Previne atacurile de falsificare a adreselor MAC și IP. |

Aceste soluții de nivel 2 nu vor fi eficiente dacă protocoalele de management nu sunt securizate. De exemplu, protocoalele de management Syslog, Simple Network Management Protocol (SNMP), Trivial File Transfer Protocol (TFTP), telnet, File Transfer Protocol (FTP) și majoritatea altor protocoale comune sunt nesigure; prin urmare, se recomandă următoarele strategii:

* Utilizați întotdeauna variante securizate ale acestor protocoale, cum ar fi SSH, Secure Copy Protocol (SCP), Secure FTP (SFTP) și Secure Socket Layer/Transport Layer Security (SSL/TLS).
* Luați în considerare utilizarea rețelei de gestionare în afara benzii pentru a gestiona dispozitivele.
* Utilizați un VLAN de management dedicat în care nu există decât traficul de management.
* Utilizați ACL-uri pentru a filtra accesul nedorit.