**LAN Security Concepts**

Dispozitivele finale sunt susceptibile la atacuri legate de malware care provin prin e-mail sau navigare pe web, cum ar fi DDOS, încălcări ale datei și programe malware. Punctele finale au folosesc caracteristici tradiționale de securitate bazate pe gazdă, cum ar fi antivirus/antimalware, firewall-uri bazate pe gazdă și sisteme de prevenire a intruziunilor (HIPS) bazate pe gazdă. Punctele finale sunt protejate printr-o combinație de NAC, software AMP bazat pe gazdă, un dispozitiv de securitate pentru e-mail (ESA) și un dispozitiv de securitate web (WSA). Cisco WSA poate efectua lista neagră de adrese URL, filtrare URL, scanare malware, categorizare URL, filtrare a aplicațiilor web și criptare și decriptare a traficului web.

**AAA** controlează cui are permisiunea de a accesa o rețea (autentificare), ce pot face în timp ce sunt acolo (autorizare) și să auditeze ce acțiuni au efectuat în timp ce accesează rețeaua (contabilitate). Autorizarea folosește un set de atribute care descriu accesul utilizatorului la rețea. Contabilitatea este combinată cu autentificarea AAA. Serverul AAA păstrează un jurnal detaliat cu exact ceea ce face utilizatorul autentificat pe dispozitiv. Standardul IEEE 802.1X este un protocol de autentificare și control al accesului bazat pe porturi care restricționează stațiile de lucru neautorizate să se conecteze la o rețea LAN prin porturi de comutare accesibile public.

Dacă Stratul 2 este compromis, atunci toate straturile de deasupra acestuia sunt și ele afectate. Primul pas în atenuarea atacurilor asupra infrastructurii Layer 2 este înțelegerea funcționării de bază a Layer 2 și a soluțiilor Layer 2: Port Security, DHCP Snooping, DAI și IPSG. Acestea nu vor funcționa decât dacă protocoalele de management sunt securizate.

Atacurile de inundare a adreselor MAC bombardează comutatorul cu adrese MAC sursă false până când tabelul de adrese MAC al comutatorului este plin. În acest moment, 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. Actorul amenințării poate captura acum toate cadrele trimise de la o gazdă la alta pe LAN local sau VLAN local. Actorul amenințării folosește **macof** pentru a genera rapid multe surse aleatorii și destinații MAC și IP. Pentru a atenua atacurile de depășire a tabelelor MAC, administratorii de rețea trebuie să implementeze securitatea porturilor.

Un atac de salt VLAN permite traficul de la un VLAN să fie văzut de un alt VLAN fără ajutorul unui router. Actorul amenințării configurează o gazdă să acționeze ca un comutator pentru a profita de funcția de port trunking automat activată în mod implicit pe majoritatea porturilor de comutare.

Un atac cu etichetare dublă VLAN este unidirecțional și funcționează numai atunci când actorul amenințării este conectat la un port care locuiește în același VLAN ca și VLAN-ul nativ al portului trunk. Etichetarea dublă permite actorului amenințării să trimită date către gazde sau servere pe un VLAN care altfel ar fi blocat de un anumit tip de configurație de control al accesului. Traficul de întoarcere va fi, de asemenea, permis, permițând actorului amenințării să comunice cu dispozitivele de pe VLAN-ul blocat în mod normal.

Atacurile de salt VLAN și de dubla etichetare VLAN pot fi prevenite prin implementarea următoarelor reguli de securitate a trunchiului: -Dezactivați trunchiul pe toate porturile de acces.

-Dezactivați trunchiul automat pe legăturile trunchiului, astfel încât trunchiurile trebuie activate manual.

-Asigurați-vă că VLAN-ul nativ este utilizat numai pentru legăturile trunchiului.

Atacul DHCP: serverele DHCP oferă în mod dinamic clienților informații despre configurația IP, inclusiv adresa IP, masca de subrețea, gateway implicit, servere DNS și multe altele. Două tipuri de atacuri DHCP sunt DHCP starvation și DHCP spoofing. Ambele atacuri sunt atenuate prin implementarea DHCP Snooping.

**Atacul ARP:** un actor de amenințare trimite un mesaj ARP gratuit care conține o adresă MAC falsificată către un comutator, iar comutatorul își actualizează tabelul MAC în consecință. Acum, actorul amenințării trimite solicitări ARP nesolicitate către alte gazde de pe subrețea cu adresa MAC a actorului amenințării și adresa IP a gateway-ului implicit. Falsificarea ARP și otrăvirea ARP sunt atenuate prin implementarea DAI.

Atacul de falsificare a adresei: falsificarea adresei IP este atunci când un actor de amenințare deturnează o adresă IP validă a altui dispozitiv din subrețea sau folosește o adresă IP aleatorie. Atacurile de falsificare a adresei MAC apar atunci când actorii amenințărilor modifică adresa MAC a gazdei lor pentru a se potrivi cu o altă adresă MAC cunoscută a unei gazde țintă. Falsificarea adreselor IP și MAC poate fi atenuată prin implementarea IPSG.

**Atacul STP:** actorii amenințări manipulează STP pentru a efectua un atac prin falsificarea podului rădăcină și schimbând topologia unei rețele. Actorii amenințărilor își fac gazdele să apară ca punți rădăcină; prin urmare, captarea întregului trafic pentru domeniul comutat imediat. Acest atac STP este atenuat prin implementarea BPDU Guard pe toate porturile de acces

**Recunoaștere CDP:** informațiile CDP sunt trimise în porturile compatibile CDP într-un multicast periodic, necriptat. Informațiile CDP includ adresa IP a dispozitivului, versiunea software-ului IOS, platforma, capabilitățile și VLAN-ul nativ. Dispozitivul care primește mesajul CDP își actualizează baza de date CDP. informațiile furnizate de CDP pot fi folosite și de un actor de amenințare pentru a descoperi vulnerabilitățile infrastructurii de rețea. Pentru a atenua exploatarea CDP, limitați utilizarea CDP pe dispozitive sau porturi.

**Switch Security Configuration**

Toate porturile (interfețele) switch-ului trebuie securizate înainte ca comutatorul să fie implementat pentru utilizare în producție. Cea mai simplă și eficientă metodă de a preveni atacurile de depășire a tabelului de adrese MAC este activarea securității porturilor. În mod implicit, porturile de comutare Layer 2 sunt setate la automat dinamic (trunking activat). Comutatorul poate fi configurat pentru a afla despre adresele MAC pe un port securizat într-unul din trei moduri: configurat manual, învățat dinamic și învățat dinamic - sticky. Îmbătrânirea securității porturilor poate fi utilizată pentru a seta timpul de îmbătrânire pentru adresele securizate statice și dinamice pe un port. Două tipuri de îmbătrânire sunt acceptate pe port: absolută și inactivitate. Dacă adresa MAC a unui dispozitiv atașat la port diferă de lista de adrese securizate, atunci are loc o încălcare a portului. În mod implicit, portul intră în starea dezactivată de eroare. Când un port este oprit și plasat în starea dezactivată de eroare, nu este trimis sau primit niciun trafic pe acel port. Pentru a afișa setările de securitate a porturilor pentru comutator, utilizațiarată comanda port-security .

Pentru a atenua atacurile de salt VLAN:

**Pasul 1.** Dezactivează negocierile DTP pe porturile non-trunking.  
**Pasul 2.** Dezactivează porturile neutilizate.  
**Pasul 3.** Activați manual legătura trunchiului pe un port trunk.  
**Pasul 4.** Dezactivați negocierile DTP pe porturile de trunking.  
**Pasul 5.** Setați VLAN-ul nativ la un alt VLAN decât VLAN 1.

Scopul unui atac de foame DHCP este de a crea un Denial of Service (DoS) pentru conectarea clienților. Atacurile de falsificare DHCP pot fi atenuate prin utilizarea DHCP snooping pe porturile de încredere. Snooping DHCP determină dacă mesajele DHCP provin dintr-o sursă de încredere configurată administrativ sau nede încredere. Apoi filtrează mesajele DHCP și limitează rata traficului DHCP din surse nesigure. Utilizați următorii pași pentru a activa DHCP Snooping:

**Pasul 1.** Activați DHCP Snooping.  
**Pasul 2.** Pe porturile de încredere, utilizați comanda de configurare a interfeței ip dhcp snooping trust .  
**Pasul 3.** Limitați numărul de mesaje de descoperire DHCP care pot fi primite pe secundă pe porturi care nu sunt de încredere.  
**Pasul 4**. Activați DHCP snooping prin VLAN sau printr-o serie de VLAN-uri.

**Inspecția dinamică ARP (DAI)** necesită DHCP snooping și ajută la prevenirea atacurilor ARP prin:

-Nu transmiterea răspunsurilor ARP invalide sau gratuite către alte porturi din același VLAN.

-Interceptarea tuturor solicitărilor și răspunsurilor ARP pe porturi nede încredere.

-Verificarea fiecărui pachet interceptat pentru o legare IP-la-MAC validă.

-Aruncarea și înregistrarea răspunsurilor ARP care provin de la invalid pentru a preveni otrăvirea ARP.

-Eroare la dezactivarea interfeței dacă numărul DAI configurat de pachete ARP este depășit.

Pentru a reduce șansele de falsificare ARP și otrăvire cu ARP, urmați aceste linii directoare de implementare a DAI:

-Activați DHCP Snooping la nivel global.

-Activați DHCP Snooping pe VLAN-urile selectate.

-Activați DAI pe VLAN-urile selectate.

-Configurați interfețe de încredere pentru inspecția DHCP și inspecția ARP.

Ca un ghid general, configurați toate porturile comutatorului de acces ca neîncrezători și toate porturile de legătură în sus care sunt conectate la alte comutatoare ca fiind de încredere.

DAI poate fi, de asemenea, configurat pentru a verifica ambele adrese MAC și IP de destinație sau sursă:

**-Destination MAC -** Verifică adresa MAC destinație din antetul Ethernet cu adresa MAC țintă din corpul ARP.

**-Sursă MAC** - Verifică adresa MAC sursă din antetul Ethernet cu adresa MAC a expeditorului din corpul ARP.

**-Adresă IP** - Verifică corpul ARP pentru adrese IP nevalide și neașteptate, inclusiv adresele 0.0.0.0, 255.255.255.255 și toate adresele IP multicast.

Pentru a atenua atacurile de manipulare Spanning Tree Protocol (STP), utilizați PortFast și Bridge Protocol Data Unit (BPDU) Guard:

**PortFast**- PortFast aduce imediat o interfață configurată ca port de acces sau trunk în starea de redirecționare dintr-o stare de blocare, ocolind stările de ascultare și de învățare. Aplicați la toate porturile utilizatorului final. PortFast ar trebui configurat numai pe porturile atașate la dispozitivele finale. PortFast ocolește stările de ascultare și învățare STP pentru a minimiza timpul în care porturile de acces trebuie să aștepte ca STP să converge. Dacă PortFast este activat pe un port care se conectează la un alt comutator, există riscul de a crea o buclă spanning-tree.

**BPDU Guard -** eroarea BPDU Guard dezactivează imediat un port care primește un BPDU. La fel ca PortFast, protecția BPDU ar trebui configurată numai pe interfețele atașate la dispozitivele finale. BPDU Guard poate fi activat pe un port utilizând comanda spanning-tree bpduguard enable interface configuration.  **spanning-tree portfast bpduguard** pentru a activa la nivel global protecția BPDU pe toate porturile activate cu PortFast.

Două tipuri de îmbătrânire sunt acceptate pentru fiecare port:

***-Absolut*** - Adresele securizate de pe port sunt șterse după perioada de vechime specificată.

***-Inactivitate*** - Adresele securizate de pe port sunt șterse numai dacă sunt inactive pentru perioada de vechime specificată.

Utilizați comanda **switchport port-security aging** pentru a activa sau dezactiva îmbătrânirea statică pentru portul securizat sau pentru a seta timpul sau tipul de îmbătrânire.

**Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}**

Parametrii pentru comandă sunt descriși în tabel.

|  |  |
| --- | --- |
| **Parametru** | **Descriere** |
| **static** | Activați vechimea pentru adresele securizate configurate static pe acest port. |
| **time time** | Specificați timpul de îmbătrânire pentru acest port. Intervalul este de la 0 la 1440 de minute. Dacă timpul este 0, vechimea este dezactivată pentru acest port. |
| **type absolute** | Setați timpul absolut de îmbătrânire. Toate adresele securizate de pe acest port expiră exact după timpul (în minute) specificat și sunt eliminate din lista de adrese securizate. |
| **type inactivity** | Setați tipul de îmbătrânire inactivitate. Adresele securizate de pe acest port expiră numai dacă nu există trafic de date de la adresa sursă securizată pentru perioada de timp specificată. |

Pentru a seta modul de încălcare a securității porturilor, utilizați următoarea comandă:

**Switch(config-if)# switchport port-security violation { protect | restrict | shutdown }**

Următoarele tabele arată cum reacţionează un comutator pe baza modului de încălcare configurat.

**Descrieri ale modului de încălcare a securității**

|  |  |
| --- | --- |
| **Modul** | **Descriere** |
| **shutdown**  **(default)** | Portul trece imediat la starea dezactivată de eroare, stinge LED-ul portului și trimite un mesaj syslog. Crește contorul de încălcări. Când un port securizat se află în starea dezactivată de eroare, un administrator trebuie să-l reactiveze introducând comenzile de **închidere** și **fără închidere .** |
| **restrict** | Portul elimină pachetele cu adrese sursă necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a scădea sub valoarea maximă sau pentru a crește valoarea maximă. Acest mod face ca contorul de încălcări de securitate să crească și generează un mesaj syslog. |
| **protect** | Acesta este cel mai puțin sigur dintre modurile de încălcare a securității. Portul elimină pachete cu adrese MAC necunoscute până când eliminați un număr suficient de adrese MAC securizate pentru a scădea sub valoarea maximă sau pentru a crește valoarea maximă. Nu este trimis niciun mesaj syslog. |

**Comparația modului de încălcare a securității**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Modul de încălcare** | **Renunță la traficul ofensator** | **Trimite un mesaj Syslog** | **Măriți contorul de încălcări** | **Închide portul** |
| Protect | da | Nu | Nu | Nu |
| R**estrict** | da | da | da | Nu |
| **SHutdown** | da | da | da | da |