**Modul de practică și test**

**Ce am învățat în acest modul?**

Punctele finale sunt deosebit de 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. Aceste puncte finale au folosit de obicei 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 cel mai bine 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.