# Endpoint Security

**1. Care atac criptează datele de pe gazde în încercarea de a extrage o plată bănească de la victimă?**

DDoS

Data breach

Malware

**Ransomware**

**Explicație:** Ransomware-ul criptează datele de pe o gazdă și blochează accesul la acestea până când se plătește o răscumpărare.

**2. Ce dispozitive sunt concepute special pentru securitatea rețelei? (Alege trei)**

**VPN-enabled router**

**NGFW**

Switch

WLC

**NAC**

**Explicație:** Un router compatibil VPN, NGFW și NAC sunt dispozitive de rețea proiectate special pentru securitate. Deși un comutator și un WLC pot fi configurate cu măsuri de securitate, acestea sunt dispozitive de acces pentru punctele finale.

**3. Ce dispozitiv monitorizează traficul SMTP pentru a bloca amenințările și a cripta mesajele trimise pentru a preveni pierderea datelor?**

NGFW

**ESA**

NAC

WSA

**Explicație:** Un ESA este conceput special pentru a monitoriza traficul SMTP.

**4. Ce dispozitiv monitorizează traficul HTTP pentru a bloca accesul la site-uri riscante și pentru a cripta mesajele trimise?**

NGFW

ESA

NAC

**WSA**

**Explicație:** Un WSA este special conceput pentru a monitoriza traficul HTTP.

**Access Control**

**1. Care componentă AAA este responsabilă pentru colectarea și raportarea datelor de utilizare în scopuri de auditare și facturare?**

Authentication

Authorization

**Accounting**

**Explicație:** Contabilitatea colectează și raportează date.

**2. Care componentă AAA este responsabilă pentru controlul cui are permisiunea de a accesa rețeaua?**

**Authentication**

Authorization

Accounting

**Explicație:** Autentificarea controlează cui are permisiunea de a accesa rețeaua.

**3. Ce componentă AAA este responsabilă pentru a determina ce poate accesa utilizatorul?**

Authentication

Authorization

Accounting

**Explicație:** Autorizarea determină ce poate accesa un utilizator.

**4. Într-o implementare 802.1X, ce dispozitiv este responsabil pentru transmiterea răspunsurilor?**

Supplicant

**Authenticator**

Router

Authentication server

Client

**Explicație:** În 802.1X, autentificatorul, care este de obicei un comutator sau un punct de acces fără fir, este responsabil pentru transmiterea mesajelor între solicitant (client) și serverul de autentificare.

**Layer 2 Security Threats**

**1. Care dintre următoarele tehnici de atenuare sunt utilizate pentru a proteja stratul 3 până la stratul 7 al modelului OSI? (Alege trei.)**

DHCP snooping

**VPN**

**Firewalls**

IPSG

**IPS devices**

**Explicație:** VPN-urile, firewall-urile și dispozitivele IP sunt exemple de tehnici de atenuare de la Layer 3 la Layer 7. Snooping DHCP și IPSG sunt folosite pentru a atenua atacurile de nivel 2.

**2. Care dintre următoarele tehnici de atenuare previne multe tipuri de atacuri, inclusiv depășirea tabelului de adrese MAC și atacurile de foame DHCP?**

IPSG

DHCP snooping

DAI

**Port security**

**Explicație:** Securitatea porturilor previne multe tipuri de atacuri, inclusiv depășirea tabelului de adrese MAC și atacurile de foame DHCP.

**3. Care dintre următoarele tehnici de atenuare previne falsificarea adreselor MAC și IP?**

**IPSG**

DHCP snooping

DAI

Port security

**Explicație:** IPSG previne falsificarea adreselor MAC și IP.

**4. Care dintre următoarele tehnici de atenuare previne falsificarea ARP și atacurile de otrăvire ARP?**

IPSG

DHCP snooping

**DAI**

Port security

**Explicație:** DAI previne falsificarea ARP și atacurile de otrăvire ARP.

**5. Care dintre următoarele tehnici de atenuare previne înfometarea DHCP și atacurile de falsificare DHCP?**

IPSG

**DHCP snooping**

DAI

Port security

**Explicație:** Snoopingul DHCP previne înfometarea DHCP și atacurile de falsificare DHCP.

**MAC Address Table Attacks**

**1.Care este comportamentul unui comutator ca urmare a unui atac reușit la tabelul de adrese MAC?**

Comutatorul se va închide.

Interfețele comutatorului vor trece la starea dezactivată de eroare.

**Comutatorul va redirecționa toate cadrele primite către toate celelalte porturi din VLAN.**

Comutatorul va elimina toate cadrele primite.

**2.Care ar fi motivul principal pentru care un actor de amenințare ar lansa un atac de depășire a adresei MAC?**

**Pentru ca actorul amenințării să poată vedea cadrele care sunt destinate altor dispozitive.**

Pentru ca actorul amenințării să poată executa cod arbitrar pe comutator.

Pentru ca comutatorul să oprească redirecționarea traficului.

Astfel încât gazdele legitime nu pot obține o adresă MAC.

**3.Ce tehnică de atenuare trebuie implementată pentru a preveni atacurile de depășire a adresei MAC?**

IPSG

DAI

Port security

DHCP snooping

**LAN Attacks**

**1. Un actor de amenințare schimbă adresa MAC a dispozitivului actorului de amenințare cu adresa MAC a gateway-ului implicit. Ce tip de atac este acesta?**

Address spoofing

ARP spoofing

CDP reconnaissance

DHCP starvation

STP attack

VLAN hopping

**Explicație:** Atacurile de falsificare de adrese au loc atunci când actorul amenințării schimbă adresa MAC și/sau IP a dispozitivului actorului amenințării pentru a prezenta ca un alt dispozitiv legitim, cum ar fi gateway-ul implicit.

**2. Un actor de amenințare trimite un mesaj BPDU cu prioritate 0. Ce tip de atac este acesta?**

Address spoofing

ARP spoofing

CDP reconnaissance

DHCP starvation

**STP attack**

VLAN hopping

**Explicație:** Un actor de amenințare care trimite mesaje BPDU cu o prioritate de 0 încearcă să devină puntea rădăcină în topologia STP.

**3. Un actor de amenințare închiriază toate adresele IP disponibile pe o subrețea. Ce tip de atac este acesta?**

Address spoofing

ARP spoofing

CDP reconnaissance

**DHCP starvation**

STP attack

VLAN hopping

**Explicație:** Atacurile de foame DHCP apar atunci când un actor de amenințare solicită și primește toată adresa IP disponibilă pentru o subrețea.

**4. Un actor de amenințare trimite un mesaj care face ca toate celelalte dispozitive să creadă că adresa MAC a dispozitivului actorului amenințării este gateway-ul implicit. Ce tip de atac este acesta?**

Address spoofing

**ARP spoofing**

CDP reconnaissance

DHCP starvation

STP attack

VLAN hopping

**Explicație**: Un actor de amenințare poate trimite un răspuns ARP gratuit, determinând toate dispozitivele să creadă că dispozitivul actorului amenințării este un dispozitiv legitim, cum ar fi gateway-ul implicit.

**5. Un actor de amenințare configurează o gazdă cu protocolul 802.1Q și formează un trunchi cu comutatorul conectat. Ce tip de atac este acesta?**

Address spoofing

ARP spoofing

CDP reconnaissance

DHCP starvation

STP attack

**VLAN hopping**

**Explicație:** Un actor de amenințare poate sări efectiv la VLAN-uri dacă dispozitivul actorului de amenințare aparține VLAN-ului nativ și trunchiuri cu comutatorul.

**6. Un actor de amenințare descoperă versiunea IOS și adresele IP ale comutatorului local. Ce tip de atac este acesta?**

Address spoofing

ARP spoofing

**CDP reconnaissance**

DHCP starvation

STP attack

VLAN hopping

**Explicație:** Un actor de amenințare poate folosi un software de detectare a pachetelor, cum ar fi Wireshark, pentru a vizualiza conținutul mesajelor CDP, care sunt trimise necriptate și includ o varietate de informații despre dispozitiv, inclusiv versiunea IOS și adresele IP.

**LAN Security Concepts Answers**

**1. Ce două protocoale sunt acceptate pe dispozitivele Cisco pentru comunicațiile AAA? (Alege doua.)**

**RADIUS**

LLDP

HSRP

VTP

**TACACS+**

**Explicație:** Două protocoale AAA sunt acceptate pe dispozitivele Cisco, TACACS+ și RADIUS. Hot Standby Router Protocol (HSRP) este utilizat pe routerele Cisco pentru a permite redundanța gateway-ului. Link Layer Discovery Protocol (LLDP) este un protocol pentru descoperirea vecinilor. Protocolul de trunking VLAN (VTP) este utilizat pe comutatoarele Cisco pentru a gestiona VLAN-urile pe un comutator de server compatibil VTP.

**2. Ce serviciu este activat implicit pe un router Cisco, care poate dezvălui informații semnificative despre router și, potențial, îl face mai vulnerabil la atac?**

HTTP

LLDP

**CDP**

FTP

**Explicație:** CDP este un protocol proprietar Cisco care adună informații de la alte dispozitive Cisco conectate și este activat implicit pe dispozitivele Cisco. LLDP este un protocol standard deschis care oferă același serviciu. Poate fi activat pe un router Cisco. HTTP și FTP sunt protocoale de nivel de aplicație care nu colectează informații despre dispozitivele din rețea.

**3. Când securitatea este o problemă, care strat OSI este considerat a fi cea mai slabă verigă dintr-un sistem de rețea?​**

Layer 4

Layer 7

**Layer 2**

Layer 3

**Explicație:** Securitatea este la fel de puternică ca cea mai slabă verigă din sistem, iar Stratul 2 este considerat a fi cea mai slabă verigă. Pe lângă protecția de la Layer 3 la Layer 7, profesioniștii în securitatea rețelei trebuie, de asemenea, să atenueze atacurile asupra infrastructurii LAN de Layer 2.

**4. Care atac Layer 2 va avea ca rezultat un comutator care va inunda cadrele primite către toate porturile?**

**MAC address overflow**

Spanning Tree Protocol manipulation

IP address spoofing

ARP poisoning

**Explicație:** Când un atacator trimite rapid cadre cu adrese MAC falsificate către un comutator, tabelul de adrese MAC al comutatorului devine plin. Odată ce tabelul de adrese MAC al comutatorului este plin, comutatorul va inunda toate cadrele noi primite în toate porturile.

**5. De ce este preferată autentificarea cu AAA în detrimentul unei baze de date locale?**

Specifică o parolă diferită pentru fiecare linie sau port.

Necesită o combinație de autentificare și parolă pe consolă, linii vty și porturi auxiliare.

**Oferă o metodă de autentificare alternativă dacă administratorul uită numele de utilizator sau parola.**

Utilizează mai puțină lățime de bandă a rețelei.

**Explicație:** Metoda de autentificare a bazei de date locală nu oferă o metodă de autentificare alternativă dacă un administrator uită numele de utilizator sau parola. Recuperarea parolei va fi singura opțiune. Când se utilizează autentificarea cu AAA, o metodă alternativă poate fi configurată pentru a permite unui administrator să utilizeze una dintre multele metode de autentificare de rezervă posibile.

**6. Într-o implementare AAA bazată pe server, ce protocol va permite routerului să comunice cu succes cu serverul AAA?**

SSH

802.1x

**RADIUS**

TACACS

**Explicație:** Cu o metodă bazată pe server, routerul accesează un server central AAA utilizând fie protocolul RADIUS (Remote Authentication Dial-In User) fie sistemul de control al accesului pentru controlerul de acces la terminal (TACACS+). SSH este un protocol folosit pentru autentificarea de la distanță. 802.1x este un protocol utilizat în autentificarea bazată pe porturi. TACACS este un protocol moștenit și nu mai este utilizat.

**7. Ce soluție Cisco ajută la prevenirea atacurilor de falsificare a adreselor MAC și IP?**

Dynamic ARP Inspection

**IP Source Guard**

Port Security

DHCP Snooping

**Explicație:** Cisco oferă soluții pentru a ajuta la atenuarea atacurilor de nivel 2, inclusiv:

IP Source Guard (IPSG) – previne atacurile de falsificare a adreselor MAC și IP

Inspecție dinamică ARP (DAI) – previne falsificarea ARP și atacurile de otrăvire ARP

DHCP Snooping – previne înfometarea DHCP și atacurile de falsificare SHCP

Port Security – previne multe tipuri de atacuri, inclusiv atacurile de depășire a tabelului MAC și atacurile de foame DHCP

**8. Care este scopul contabilității AAA?**

pentru a determina ce resurse poate accesa utilizatorul

**pentru a colecta și raporta utilizarea aplicației**

pentru a demonstra că utilizatorii sunt cine spun că sunt

pentru a determina ce operațiuni poate efectua utilizatorul

**Explicație:** Contabilitatea AAA colectează și raportează datele de utilizare a aplicației. Aceste date pot fi utilizate în scopuri precum auditul sau facturarea. Autentificarea AAA este procesul de verificare a utilizatorilor care spun că sunt. Autorizarea AAA este ceea ce utilizatorii pot și nu pot face în rețea după ce sunt autentificați.

**9. Care atac de nivel 2 va duce la ca utilizatorii legitimi să nu obțină adrese IP valide?**

ARP spoofing

**DHCP starvation**

IP address spoofing

MAC address flooding

**Explicație:** Atacul de înfometare DHCP provoacă epuizarea pool-ului de adrese IP al unui server DHCP înainte ca utilizatorii legitimi să poată obține adrese IP valide.

**10. Care trei produse Cisco se concentrează pe soluții de securitate pentru punctele terminale? (Alege trei.)**

**NAC Appliance**

Adaptive Security Appliance

SSL/IPsec VPN Appliance

IPS Sensor Appliance

**Web Security Appliance**

**Email Security Appliance**

**Explicație:** Componentele principale ale soluțiilor de securitate pentru punctele terminale sunt dispozitivele Cisco Email și Web Security și dispozitivul Cisco NAC. Dispozitivele ASA, SSL/IPsec VPN și senzori IPS oferă toate soluții de securitate care se concentrează pe rețeaua întreprinderii, nu pe dispozitivele terminale.

**11. Adevărat sau fals?**

În standardul 802.1X, clientul care încearcă să acceseze rețeaua este denumit solicitant.

Fals

**Adevărat**

**Explicație:** În terminologia 802.1X, stația de lucru client este cunoscută sub numele de solicitant.

**12. Ce este implicat într-un atac de falsificare a adresei IP?**

Mesajele DHCPDISCOVER false sunt trimise pentru a consuma toate adresele disponibile pe un server DHCP.

Un server DHCP nepoliticos oferă parametri de configurare IP falși clienților DHCP legitimi.

Un nod necinstit răspunde la o solicitare ARP cu propria sa adresă MAC indicată pentru adresa IP țintă.

**O adresă IP legitimă a rețelei este deturnată de un nod necinstit.**

**Explicație:** Într-un atac de falsificare a adresei IP, adresa IP a unei gazde legitime de rețea este deturnată și utilizată de un nod necinstit. Acest lucru permite nodului necinstiți să se prezinte ca un nod valid în rețea.

**13. Ce trei servicii sunt furnizate de cadrul AAA? (Alege trei.)**

**authentication**

**authorization**

**accounting**

autoconfiguration

automation

autobalancing

**Explicație:** Cadrul de autentificare, autorizare și contabilitate (AAA) oferă servicii pentru a ajuta la securizarea accesului la dispozitivele din rețea.

**14. Din cauza controalelor de securitate implementate, un utilizator poate accesa doar un server cu FTP. Ce componentă AAA realizează acest lucru?**

**authentication**

authorization

accounting

autoconfiguration

automation

autobalancing

**Explicație:** Una dintre componentele din AAA este autorizarea. După ce un utilizator este autentificat prin AAA, serviciile de autorizare determină ce resurse poate accesa utilizatorul și ce operațiuni îi este permis să efectueze.

**15. Ce plan de atenuare este cel mai bun pentru a contracara un atac DoS care creează o depășire a tabelului de adrese MAC?**

**Enable port security.**

Disable DTP.

Disable STP.

Place unused ports in an unused VLAN(Plasați porturile neutilizate într-un VLAN neutilizat)

**Explicație:** Un atac de depășire a tabelului de adrese MAC (CAM), depășirea bufferului și falsificarea adresei MAC pot fi toate atenuate prin configurarea securității porturilor. De obicei, un administrator de rețea nu ar dori să dezactiveze STP, deoarece previne buclele de nivel 2. DTP este dezactivat pentru a preveni saltul VLAN. Plasarea porturilor neutilizate într-un VLAN neutilizat previne conexiunea prin cablu neautorizată.