

Securitatea rețelei de acces și wireless

Ultima lucrare face ceva ce se evită de obicei: execută trei atacuri reale pe rețeaua proprie - un switch transformat în hub, un server DHCP fals și un dispozitiv care se dă drept gateway - apoi le închide, pe rând, ușile. La final, adăugați o rețea wireless și îi comparați securitatea cu cea a cablului.

OBIECTIVELE CAPITOLULUI

- Construiți topologia și verificați funcționarea normală, înainte de orice atac
- Demonstrați efectul unei table CAM golite și configurați port security pe toate porturile de acces
- Executați atacul cu server DHCP fals și demonstrați că DHCP snooping îl oprește
- Explicați în scris mecanismul ARP poisoning și configurați Dynamic ARP Inspection, inclusiv ARP ACL pentru stația statică
- Aplicați toate măsurile împotriva VLAN hopping și a atacurilor STP; demonstrați BPDU Guard în acțiune
- Configurați accesul de administrare prin SSH, cu restricție de sursă
- Construiți rețeaua wireless cu WPA2-PSK, apoi migrați-o pe autentificare RADIUS
- Redactați lista finală de verificare pentru securizarea unui switch de acces, cu justificarea fiecărei linii

7.1 Regula de aur a acestei lucrări

Citiți înainte de a începe. Toate atacurile din această lucrare se execută *exclusiv* pe topologia proprie, în laborator sau în bancul de lucru din pagină. Aceleași tehnici aplicate pe o rețea reală - a facultății, a unei firme, a unui vecin - constituie infracțiune, indiferent de intenție și indiferent dacă „nu s-a stricat nimic”.

Scopul lucrării nu este să învățați să atacați, ci să înțelegeți *de ce* funcționează atacurile, pentru că numai așa configurațiile defensive încetează să fie o listă memorată și devin decizii înțelese.

Cele trei atacuri au același numitor comun: protocoalele rețelei locale au fost proiectate într-o epocă în care oricine avea acces fizic la cablu era, prin definiție, de încredere. Niciunul dintre ele nu are autentificare. Toate contramăsurile de mai jos adaugă, într-o formă sau alta, exact ce lipsește: o sursă de adevăr despre cine are voie să spună ce.

Tabelul 7.1 Regula de aur a acestei lucrări.

Atacul	De ce funcționează	Contramăsura
CAM overflow	tabela de comutare e finită; plină, switch-ul inundă tot	port-security
Rogue DHCP	DHCP nu are autentificare; clientul crede primul răspuns	ip dhcp snooping
ARP poisoning	ARP acceptă răspunsuri nesolicitate, fără verificare	ip arp inspection

7.2 Echipamente necesare

Tabelul 7.2 Echipamente necesare.

Buc.	Echipament	Model	Categoria din Packet Tracer	La ce folosește aici
1	Ruter	4331	Network Devices → Routers	gateway și server DHCP legitim
1	Switch de acces	2960	Network Devices → Switches	SW-ACCES, echipamentul pe care îl securizați
1	Switch suplimentar	2960	Network Devices → Switches	„switch-ul adus de cineva”, pentru BPDU Guard
2	Calculator	PC-PT	End Devices	PC-1 și PC-2, clienți DHCP
1	Server	Server-PT	End Devices	SERVER, cu adresă statică
1	Server (atacator)	Server-PT	End Devices	ATACATOR, cu serviciul DHCP pornit
1	Punct de acces	Access Point-PT	Network Devices → Wireless Devices	rețeaua wireless
1	Laptop	Laptop-PT	End Devices	clientul wireless - necesită modul WPC300N
1	Server AAA	Server-PT	End Devices	opțional, pentru partea cu RADIUS

Laptopul nu are placă wireless din fabrică. În Packet Tracer, deschideți laptopul → fila *Physical* → opriți-l din butonul de alimentare → trageți afară modulul Ethernet existent → puneți în loc WPC300N → porniți-l la loc. Este pasul pe care îl ratează toată lumea la prima încercare.

7.3 Topologia

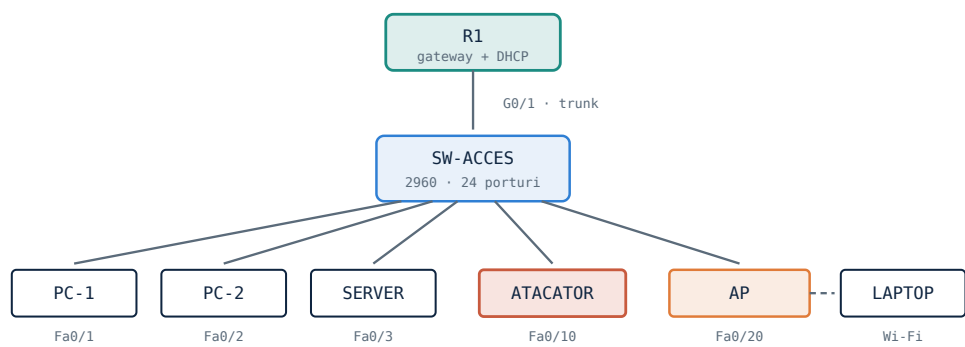


Figura 7.1 Topologia lucrării. Stația ATACATOR este un calculator obișnuit, conectat la un port obișnuit - exact cum ar arăta un laptop adus de cineva în sala de ședințe.

Tabelul 7.3 Topologia.

Dispozitiv	Adresă	Port	VLAN
R1 (gateway și server DHCP)	192.168.100.1/24, pe G0/0/0.10	G0/0/0 (trunk)	10
PC-1, PC-2	prin DHCP	Fa0/1, Fa0/2	10
SERVER	192.168.100.10, static	Fa0/3	10
ATACATOR	192.168.100.66, static, cu DHCP pornit	Fa0/10	10
AP wireless	-	Fa0/20	10
VLAN nativ al trunk-ului	-	-	99, gol

7.4 Bancul de lucru

Rețeaua este deja cablată și adresată, iar **ATACATOR are deja un server DHCP fals pornit** - este punctul de plecare ostil. Switch-ul suplimentar stă deoparte, neconectat; îl veți lega voi, la secțiunea cu BPDU Guard, din panoul *Cablurile*.

7.5 Pasul 0: rețeaua care merge

```
Router(config)# hostname R1
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# no ip address
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitEthernet 0/0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.100.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface gigabitEthernet 0/0/0.99
R1(config-subif)# encapsulation dot1Q 99 native
R1(config-subif)# exit

R1(config)# ip dhcp excluded-address 192.168.100.1 192.168.100.19
R1(config)# ip dhcp pool LAN
R1(dhcp-config)# network 192.168.100.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.100.1
R1(dhcp-config)# dns-server 192.168.100.10
R1(dhcp-config)# end
```

Listingul 7.1 pe R1 copiază

```
Switch(config)# hostname SW-ACCES
SW-ACCES(config)# vlan 10
SW-ACCES(config-vlan)# name UTILIZATORI
SW-ACCES(config-vlan)# vlan 99
SW-ACCES(config-vlan)# name NATIV-GOL
SW-ACCES(config-vlan)# exit

SW-ACCES(config)# interface range fastEthernet 0/1 - 21
SW-ACCES(config-if-range)# switchport mode access
SW-ACCES(config-if-range)# switchport access vlan 10
SW-ACCES(config-if-range)# exit

SW-ACCES(config)# interface gigabitEthernet 0/1
SW-ACCES(config-if)# switchport mode trunk
SW-ACCES(config-if)# switchport trunk native vlan 99
SW-ACCES(config-if)# switchport trunk allowed vlan 10,99
SW-ACCES(config-if)# end
```

Listingul 7.2 pe SW-ACCES copiază

interface range vă scutește de 21 de repetări. Tot ce scrieți în modul *config-if-range* se aplică pe toate porturile din interval deodată. Promptul vă amintește unde sunteți. Este comanda pe care o veți folosi cel mai des într-o zi de configurare reală.

Verificați că rețeaua funcționează: de pe PC-2, `ipconfig /renew` apoi `ping 192.168.100.10`.

7.6 Atacul 1: switch-ul care devine hub

Tabela de comutare a unui switch este finită. Dacă se umple, switch-ul nu mai poate învăța adrese noi și începe să inunde traficul necunoscut pe toate porturile - adică se comportă ca un hub, iar atacatorul vede tot.

1. Situația inițială

pe SW-ACCES

```
SW-ACCES# show mac address-table
SW-ACCES# show mac address-table count
```

Notați câte intrări există și care este capacitatea. Generați trafic între PC-1 și SERVER și observați că traficul nu ajunge la ATACATOR.

2. Demonstrația efectului

Nici Packet Tracer, nici bancul din pagină nu au un generator de cadre cu adrese MAC false, așa că demonstrăm efectul, nu atacul: goliți tabela și priviți ce se întâmplă cu primul cadru.

pe SW-ACCES

```
SW-ACCES# clear mac address-table dynamic
```

Trimiteți imediat un cadru de la PC-1 spre SERVER. Cu tabela goală, destinația este necunoscută, deci cadrul pleacă pe **toate** porturile, inclusiv pe Fa0/10. *Aceasta este exact starea în care un atac CAM overflow menține switch-ul, permanent.*

3. Contramăsura: port security

pe toate porturile de acces

```
SW-ACCES(config)# interface range fastEthernet 0/1 - 21
SW-ACCES(config-if-range)# switchport mode access
SW-ACCES(config-if-range)# switchport port-security
SW-ACCES(config-if-range)# switchport port-security maximum 2
SW-ACCES(config-if-range)# switchport port-security mac-address sticky
SW-ACCES(config-if-range)# switchport port-security violation restrict
SW-ACCES(config-if-range)# end
```

```
SW-ACCES# show port-security
SW-ACCES# show port-security address
```

De ce maximum 2 și nu 1 Un singur MAC pare mai sigur, dar rupe două situații complet normale: un telefon IP cu un calculator conectat în spatele lui, și o mașină virtuală cu adresă proprie. Valoarea 2 sau 3 este compromisul uzual în rețelele de birou.

4. Comparați cele trei acțiuni la violare

Acțiune	Cadrele în exces	Contor	Notificare	Portul
protect	aruncate	nu	nu	rămâne activ
restrict	aruncate	da	SNMP + syslog	rămâne activ
shutdown	-	da	SNMP + syslog	err-disabled

Testați ambele comportamente: cu `restrict`, verificați că se schimbă doar contorul din `show port-security interface fastEthernet 0/1`; cu `shutdown`, portul trece în `err-disabled` și trebuie reactivat manual:

reactivarea unui port `err-disabled`

```
SW-ACCES(config)# interface fastEthernet 0/1
SW-ACCES(config-if)# shutdown
SW-ACCES(config-if)# no shutdown
```

Alegeți cu cap acțiunea `shutdown` pare cea mai sigură, dar înseamnă că orice utilizator care își schimbă laptopul rămâne fără rețea până când vine cineva să reactiveze portul. În majoritatea rețelelor de birou, `restrict` este compromisul corect: blochează traficul suspect, dar anunță în loc să pedepsească.

7.7 Atacul 2: serverul DHCP fals

Un atacator pornește pe calculatorul lui un server DHCP și răspunde mai repede decât cel legitim. Toate stațiile care se conectează după aceea primesc de la el adresă, mască - și, mai ales, un gateway care este chiar el.

1. Executați atacul

În bancul din pagină, ATACATOR are deja serviciul pornit. În Packet Tracer, înlocuiți stația cu un *Server-PT*, dați-i adresa 192.168.100.66 și activați DHCP din fila *Services* → *DHCP*, cu aceste valori:

Parametru	Valoare la atacator	Valoare legitimă
Default Gateway	192.168.100.66 - el însuși	192.168.100.1
DNS Server	192.168.100.66	192.168.100.10
Start IP	192.168.100.150	192.168.100.20

Pe PC-1, cereți o adresă nouă:

pe PC-1

```
ipconfig /release
ipconfig /renew
ipconfig
```

Priviți câmpul *Default Gateway*. Dacă arată 192.168.100.66, atacul a reușit: tot traficul lui spre exterior trece acum prin atacator, care îl poate citi și transmite mai departe.

De ce funcționează DHCP nu are nicio autentificare. Clientul acceptă prima ofertă primită și nu are cum să distingă un server legitim de unul fals. Este exact aceeași categorie de problemă ca la ARP: un protocol proiectat într-o epocă în care rețeaua locală era considerată un spațiu de încredere.

2. Contramăsura: DHCP snooping

pe SW-ACCES

```
SW-ACCES(config)# ip dhcp snooping
SW-ACCES(config)# ip dhcp snooping vlan 10
SW-ACCES(config)# no ip dhcp snooping information option
```

```
SW-ACCES(config)# interface gigabitEthernet 0/1
SW-ACCES(config-if)# ip dhcp snooping trust
SW-ACCES(config-if)# exit
```

```
SW-ACCES(config)# interface range fastEthernet 0/1 - 21
SW-ACCES(config-if-range)# ip dhcp snooping limit rate 10
SW-ACCES(config-if-range)# end
```

```
SW-ACCES# show ip dhcp snooping
```

Ideea, într-o propoziție: **numai porturile declarate de încredere au voie să trimită răspunsuri DHCP**. Uplink-ul spre ruter este de încredere; toate porturile de utilizator nu sunt, iar mesajele Offer venite de acolo sunt aruncate de switch.

Repetăți atacul, de pe PC-2:

pe PC-2

```
ipconfig /release
ipconfig /renew
ipconfig
```

De data aceasta gateway-ul trebuie să fie 192.168.100.1. Verificați și pe ruter, cu `show ip dhcp binding`, că alocarea a venit de la el.

Priviți și `show ip dhcp snooping binding`: switch-ul a construit o evidență cu perechile (MAC, IP, VLAN, port) observate în tranzacțiile legitime. Această tabelă este fundația pasului următor.

7.8 Atacul 3: ARP poisoning

Atacatorul trimite mesaje ARP nesolicitate, în care pretinde că adresa IP a gateway-ului îi aparține. Stațiile își actualizează cache-ul și încep să îi trimită lui tot traficul destinat exteriorului.

1. Situația normală

pe PC-1

```
ping 192.168.100.1
```

```
arp -a
```

Notați adresa MAC asociată gateway-ului. Comparați-o cu adresa MAC reală a interfeței lui R1, din `show arp` pe ruter sau din panoul de configurare al stației.

2. Efectul atacului

Nici Packet Tracer, nici bancul din pagină nu au un generator de ARP fals, așa că demonstrația se face conceptual: dacă atacatorul ar trimite un ARP reply cu `192.168.100.1 → MAC-ul lui`, cache-ul lui PC-1 ar arăta acea adresă MAC în dreptul gateway-ului. De atunci înainte, fiecare cadru destinat exteriorului ar pleca spre atacator, care l-ar putea citi și apoi transmite mai departe - astfel încât nimic să nu pară stricat.

Verificați-vă înțelegerea

După atac, ce s-ar schimba în ieșirea comenzii `arp -a` de pe PC-1? Ce ar rămâne **neschimbat** și de ce?

► Vezi răspunsul

3. Contramăsura: Dynamic ARP Inspection

pe SW-ACCES - necesită DHCP snooping activ

```
SW-ACCES(config)# ip arp inspection vlan 10
```

```
SW-ACCES(config)# interface gigabitEthernet 0/1
```

```
SW-ACCES(config-if)# ip arp inspection trust
```

```
SW-ACCES(config-if)# exit
```

```
SW-ACCES(config)# arp access-list SERVERE
```

```
SW-ACCES(config-arp-nacl)# permit ip host 192.168.100.10 mac host 000A.0B0C.0D0E
```

```
SW-ACCES(config)# ip arp inspection filter SERVERE vlan 10
```

```
SW-ACCES(config)# end
```

```
SW-ACCES# show ip arp inspection
```

Atenție la stațiile cu adresă statică DAI verifică mesajele ARP față de evidența construită de DHCP snooping. O stație configurată static nu apare acolo, deci mesajele ei ARP legitime ar fi aruncate. Trebuie declarată explicit, printr-un ARP ACL - ca în exemplul de mai sus pentru SERVERE. Este cel mai frecvent motiv pentru care „DAI a stricat rețeaua”.

7.9 Închiderea celorlalte uși

VLAN hopping

```
SW-ACCES(config)# interface range fastEthernet 0/1 - 21
SW-ACCES(config-if-range)# switchport mode access
SW-ACCES(config-if-range)# switchport nonegotiate
SW-ACCES(config-if-range)# exit

SW-ACCES(config)# interface gigabitEthernet 0/1
SW-ACCES(config-if)# switchport nonegotiate
SW-ACCES(config-if)# exit

SW-ACCES(config)# vlan 999
SW-ACCES(config-vlan)# name NEFOLOSIT
SW-ACCES(config-vlan)# exit
SW-ACCES(config)# interface fastEthernet 0/21
SW-ACCES(config-if)# switchport access vlan 999
SW-ACCES(config-if)# shutdown
```

Listingul 7.3 pe SW-ACCES copiază

Tabelul 7.4 VLAN hopping.

Măsura	Ce atac închide
switchport nonegotiate pe porturile de acces	switch spoofing; portul nu mai poate fi convins să devină trunk
VLAN nativ 99, gol (configurat la pasul 0)	double tagging; nu mai există stații în VLAN-ul nativ
switchport trunk allowed vlan 10,99	limitează ce poate injecta cineva pe trunk
porturile nefolosite închise, în VLAN mort	accesul fizic la o priză liberă nu mai dă nimic

Atacuri asupra Spanning Tree

```
SW-ACCES(config)# interface range fastEthernet 0/1 - 21
SW-ACCES(config-if-range)# spanning-tree portfast
SW-ACCES(config-if-range)# spanning-tree bpduguard enable
```

Listingul 7.4 pe SW-ACCES copiază

Testați în bancul de lucru: alegeți **SW-STRAIN**, în panoul *Cablurile* apăsați *leagă* pe Fa0/1 și alegeți **SW-ACCES** : Fa0/15. Apoi, pe SW-ACCES:

```
SW-ACCES# show interfaces fastEthernet 0/15 status
```

Listingul 7.5 pe SW-ACCES copiază

Portul apare imediat `err-disabled`: un port de utilizator nu are niciun motiv să primească BPDU-uri, iar dacă primește, acolo s-a conectat un switch - legitim sau nu. Scoateți cablul și reactivați portul cu `shutdown / no shutdown`.

Administrarea switch-ului

```
SW-ACCES(config)# ip domain-name retele.local
SW-ACCES(config)# crypto key generate rsa
SW-ACCES(config)# username admin privilege 15 secret Admin123
SW-ACCES(config)# enable secret Enable123
SW-ACCES(config)# service password-encryption
SW-ACCES(config)# line vty 0 4
SW-ACCES(config-line)# transport input ssh
SW-ACCES(config-line)# login local
SW-ACCES(config-line)# exec-timeout 5 0
SW-ACCES(config-line)# exit
SW-ACCES(config)# banner motd #Acces autorizat numai. Activitatea este inregistrata.#
SW-ACCES(config)# end
SW-ACCES# copy running-config startup-config
```

Listingul 7.6 pe SW-ACCES copiază

7.10 Rețeaua wireless

Un punct de acces este, la nivelul 2, un **hub în aer**: tot ce transmite un client ajunge la toți ceilalți din raza lui. Diferența față de un hub obișnuit este că nu trebuie să intri în clădire ca să te conectezi la el. De aceea criptarea nu este opțională.

În bancul din pagină, laptopul este deja asociat: verificați cu `ping 192.168.100.10` și priviți tabelul *Traseul ultimului pachet* - segmentul prin AP apare la fel ca oricare altul, pentru că din punctul de vedere al rețelei chiar este la fel.

1. Punct de acces cu WPA2-PSK în Packet Tracer

Adăugați un *Access Point-PT* pe Fa0/20 și un laptop cu placă wireless. Configurați AP-ul din fila *Config* → *Port 1*:

Parametru	Valoare
SSID	RL-LAB
Authentication	WPA2-PSK
Encryption	AES
Pass Phrase	ParolaLung4Lab2026
Channel	1, 6 sau 11

Pe laptop, din *Desktop* → *PC Wireless*, conectați-vă la rețea. Verificați cu `ipconfig` că a primit adresă prin DHCP și dați `ping` către SERVER.

2. Patru experimente de securitate

Experiment	Ce observați	Concluzia
Setați autentificarea pe Disabled	oricine se conectează instantaneu	o rețea deschisă este exact atât: deschisă
Setați WEP cu o cheie de 10 caractere hexa	funcționează, iar Packet Tracer o acceptă fără reținere	WEP dă impresia de securitate; în realitate se sparge în minute
Dezactivați difuzarea SSID-ului	rețeaua nu mai apare în listă, dar conectarea manuală funcționează	ascunderea nu este securitate: SSID-ul apare în cadrele clienților legitimi
Activați filtrarea MAC și adăugați doar laptopul	alte dispozitive sunt respinse	util ca igienă, inutil față de cineva care poate copia o adresă MAC

3. Autentificare individuală, cu RADIUS

Adăugați un server AAA în rețeaua cablată, activați serviciul AAA din fila *Services* și creați doi utilizatori. Înregistrați AP-ul ca client RADIUS, apoi schimbați autentificarea AP-ului pe WPA2 cu server RADIUS.

Conectați laptopul cu numele de utilizator și parola proprii. Ștergeți apoi utilizatorul din server și încercați din nou.

Diferența care contează Cu **WPA2-PSK**, toată lumea folosește aceeași parolă. Când pleacă un angajat, trebuie schimbată pentru toți - deci, în practică, nu se schimbă niciodată.

Cu **WPA2-Enterprise**, fiecare are credențiale proprii. Un utilizator se revocă în zece secunde, individual, iar jurnalele arată cine s-a conectat, când și de pe ce dispozitiv.

7.11 Lista de verificare

Aceasta este, de fapt, livrabilul cel mai util al întregului semestru: ce se configurează pe orice switch de acces, înainte de a-l pune în producție.

Tabelul 7.5 Lista de verificare.

#	Măsura	De ce
1	nume, banner, parole cu <code>enable secret</code>	un echipament fără nume nu a fost configurat conștient niciodată
2	SSH în loc de Telnet, cu <code>login local</code> și <code>exec-timeout</code>	Telnet trimite parolele în clar
3	<code>access-class</code> pe liniile VTY	limitează de unde se poate încerca conectarea
4	porturile de acces: <code>mode access + nonegotiate</code>	închide switch spoofing
5	VLAN nativ gol, listă explicită de VLAN-uri pe trunk	închide double tagging
6	<code>port-security</code> cu <code>restrict</code> și <code>sticky</code>	limitează CAM overflow și MAC spoofing
7	<code>portfast + bpduguard</code> pe porturile de utilizator	închide atacurile STP
8	<code>ip dhcp snooping</code> , cu uplink-ul de încredere	închide rogue DHCP
9	<code>ip arp inspection</code> , plus ARP ACL pentru stațiile statice	închide ARP poisoning
10	porturile nefolosite: închise, în VLAN mort	o priză liberă nu mai este o ușă

7.12 Provocare

Exemplul 7.1. Sunteți chemat să evaluați securitatea rețelei unei firme mici. Găsiți următoarea configurație pe switch-ul de acces:

configurația găsită

```
hostname Switch
!
interface range FastEthernet0/1 - 24
  switchport mode dynamic auto
!
interface GigabitEthernet0/1
  switchport mode trunk
  switchport trunk native vlan 1
!
line vty 0 4
  password cisco
  login
  transport input all
!
enable password cisco
```

Cerințe:

1. Identificați **toate** problemele de securitate din această configurație - sunt cel puțin șapte.
 2. Pentru fiecare, precizați ce atac devine posibil și din ce curs provine.
 3. Scrieți configurația corectată, completă.
 4. Ordonăți problemele după gravitate și argumentați ordinea.
1. `switchport mode dynamic auto` pe toate porturile - DTP activ, deci **switch spoofing** posibil de pe orice port de utilizator (cursul 12).
 2. VLAN nativ 1 pe trunk, adică același cu VLAN-ul stațiilor - **double tagging** posibil (cursul 12).
 3. Fără `switchport trunk allowed vlan` - trunk-ul transportă toate cele 4094 de VLAN-uri.
 4. `transport input all` - Telnet este permis, deci parolele circulă în clar (cursul 8).
 5. `enable password` în loc de `enable secret` - parola este stocată reversibil.
 6. Parola `cisco`, la ambele - spartă instantaneu de orice dicționar (cursul 12).
 7. Fără `access-class` pe liniile VTY - oricine din rețea poate încerca să se conecteze.
 8. Fără port security, fără DHCP snooping, fără DAI - CAM overflow, rogue DHCP și ARP poisoning sunt toate posibile.
 9. Fără `portfast` și `bpduguard` - atac STP posibil de pe orice port.
 10. Porturile nefolosite active și în VLAN 1 - oricine intră în priză are acces imediat la rețea.
 11. Numele implicit `Switch` și lipsa oricărui banner - semne că echipamentul nu a fost niciodată configurat conștient.

Rezolvare. Pentru ordonarea după gravitate, gândiți-vă la trei criterii: cât de ușor este de exploatat, ce obține atacatorul, și cât de repede ar fi observat. Parola slabă combinată cu Telnet permis este, probabil, mai gravă decât lipsa DAI - pentru că duce direct la control total asupra echipamentului, fără ca cineva să afle.

7.13 Ce se predă

Tabelul 7.6 Ce se predă.

Livrabil	Format	Punctaj
Fișier Packet Tracer complet securizat, cu rețeaua wireless funcțională	.pkt	30 %
Documentarea celor trei atacuri: mecanism, efect observat, contramăsură	document	25 %
Lista de verificare pentru securizarea unui switch, cu justificări	document	15 %
Comparația WPA2-PSK / WPA2-Enterprise, cu argumente proprii	document	10 %
Raportul de audit din provocare	document	20 %

Exerciții

- De ce Dynamic ARP Inspection are nevoie de DHCP snooping activ?
 - Pentru ca ambele ruleaza pe acelasi procesor
 - Pentru ca DAI verifica mesajele ARP fata de evidenta de perechi IP-MAC construita de DHCP snooping
 - Pentru ca DHCP snooping cripteaza ARP-ul
 - Nu are nevoie, sunt independente
- O statie configurata static nu mai comunica dupa activarea DAI. De ce?
 - DAI nu suporta adrese statice
 - Statia nu apare in evidenta DHCP snooping, deci mesajele ei ARP sunt aruncate - trebuie declarata printr-un ARP ACL
 - Adresa MAC este gresita
 - Portul trebuie sa fie trust
- Ce face BPDU Guard?
 - Impiedica un port sa devina port radacina
 - Inchide portul daca primeste un BPDU
 - Filtreaza toate BPDU-urile
 - Accelereaza convergenta STP
- De ce port security cu maximum 1 poate crea probleme intr-o retea de birou?
 - Consuma prea multa memorie
 - Rupe scenariile normale cu telefon IP plus calculator, sau cu masini virtuale
 - Nu functioneaza pe porturi de acces
 - Necesita DHCP snooping
- Ce port se declara trusted la DHCP snooping?
 - Toate porturile de utilizator
 - Doar portul spre serverul DHCP legitim, de obicei uplink-ul
 - Niciunul
 - Portul atacatorului, ca sa fie monitorizat
- Care este diferenta practica esentiala dintre WPA2-PSK si WPA2-Enterprise?
 - Viteza de criptare
 - In Enterprise fiecare utilizator are credentiale proprii, deci poate fi revocat individual si apare in jurnale
 - PSK nu foloseste AES
 - Enterprise functioneaza doar pe 5 GHz

Extras din volumul „Rețele Locale - Note de curs și lucrări de laborator”. Varianta online a acestui capitol conține figurile în formă interactivă.