

Progetto Internet Security



VLAN HOPPING

LEONARDO CARACCI
X81001070

INDICE

CAPITOLO 1: VLAN HOPPING	3
1.1 Cos'è	3
1.2 Cos'è una VLAN	3
CAPITOLO 2: VLAN DOUBLE TAGGING	4
2.1 In cosa consiste l'attacco	4
2.2 Come difendersi	4
CAPITOLO 3: SWITCH SPOOFING	5
3.1 DTP (Dynamic Trunking Protocol)	5
3.2 In cosa consiste l'attacco	5
3.3 Come difendersi	6
CAPITOLO 4: DIMOSTRAZIONE ATTACCO	6
4.1 Requisiti	6
4.2 Scenario	7
4.3 L'attacco	9
CAPITOLO 5: CONCLUSIONI	14
CAPITOLO 6: BIBLIOGRAFIA	15

1 VLAN HOPPING

1.1 cos'è

Il VLAN Hopping è un attacco contro le reti VLAN. Per mezzo di questo attacco il “malintenzionato” è in grado di catturare dati che passano su diverse VLAN e di “saltare” da una VLAN all'altra. Ci sono due metodi per realizzare l'attacco:

- **Double Tags:** L'attaccante deve essere connesso a un'interfaccia appartenente alla VLAN nativa, modificherà il frame originale per aggiungere due TAG VLAN, un TAG esterno (della sua VLAN) e un TAG nascosto della VLAN della vittima.
- **Switch spoofing:** L'attaccante configurerà un sistema per falsificare se stesso come switch.

Prima di poter parlare dell'attacco in sé, ai fini della comprensione, diamo una spiegazione molto generale di cos'è una VLAN:

1.2 cos'è una VLAN

Quando creiamo una rete ci saranno numerosi host che comunicheranno tra loro, può essere utile separare la connessione a determinati utenti, ad esempio ad un gestore di un'attività gli tornerebbe utile creare una rete separata tra clienti e dipendenti per motivi di sicurezza, per mezzo delle VLAN (Virtual Local Area Network) è possibile allestire più reti locali che non comunicano tra loro ma ne condividono la stessa infrastruttura. Per poter creare delle Vlan abbiamo bisogno di un dispositivo chiamato Switch che ci permette di organizzare il traffico della rete suddividendolo in varie porte. Esistono due tipologie di VLAN:

- **Trunked:** basate su porte, in questo caso ogni porta sarà associata a ogni sottorete.
- **Basate su tag:** Viene utilizzato un protocollo di comunicazione che aggiunge un TAG con le informazioni delle VLAN.

2 VLAN DOUBLE TAGGING

L'attacco **double tags** consiste nel inserire in modo nascosto dei tag (802.1Q) all'interno di trame VLAN già in possesso di un loro tag. Ovviamente l'attacco potrà concretizzarsi solamente se l'attaccante si trova nella stessa Vlan nativa delle porte Trunk.

2.1 In cosa consiste l'attacco

Per compiere l'attacco si deve costruire una trama con doppio tag 802.1Q dove l'header esterno ha il tag della VLAN da cui parte l'attacco, mentre quello interno ha il tag della VLAN da attaccare nascosto. Appena la trama arriva nella porta di accesso dello switch verranno verificati i primi 4 byte del tag 802.1Q, verrà cancellato il tag e verrà inoltrata la trama nelle porte della VLAN nativa. A questo punto la nostra trama sarà senza il primo tag 802.1Q, ma avrà ancora il secondo tag nascosto, invece il secondo Switch utilizzerà il tag occultato per decidere su quale VLAN inoltrare la trama.

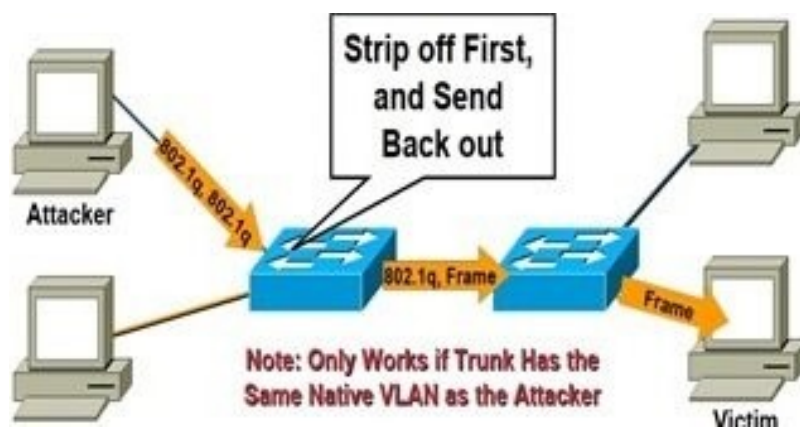


Immagine 1 Schema che mostra il funzionamento di un attacco Vlan double tags

2.2 Come difendersi

Con le giuste precauzioni è possibile difendersi da questo tipo di attacco, innanzitutto non bisogna mai utilizzare la VLAN nativa per nessuna rete, per default la VLAN nativa è la VLAN-1. Durante la creazione delle VLAN occorre configurare l'interfaccia degli endpoint in modo chiaro e specificare sempre gli ID VLAN consentiti per il trunk. È importante non consentire mai a tutto il traffico VLAN di passare attraverso qualsiasi porta trunk.

3 SWITCH SPOOFING

Prima di parlare dell'attacco switch spoofing occorre chiarire cos'è il DTP (Dynamic Trunking Protocol)

3.1 DTP (Dynamic Trunking Protocol)

Il DTP (Dynamic Trunking Protocol) è un protocollo proprietario di trunking sviluppato da Cisco, viene usato per gestire in modo automatico le porte di trunk degli switch. In base alla sua configurazione può essere utilizzato per la negoziazione dinamica dei collegamenti in trunk tra due o più switch.

DTP può operare in differenti modi di trunking come mostrato in questo schema:

DYNAMIC TRUNKING PROTOCOL (DTP)					
	SWITCHPORT MODE DYNAMIC AUTO	SWITCHPORT MODE DYNAMIC DESIRABLE	SWITCHPORT MODE TRUNK	SWITCHPORT MODE NEGOTIATE	SWITCHPORT MODE ACCESS
SWITCHPORT MODE DYNAMIC AUTO	Access	Trunk	Trunk	Limited Connectivity	Access
SWITCHPORT MODE DYNAMIC DESIRABLE	Trunk	Trunk	Trunk	Limited Connectivity	Access
SWITCHPORT MODE TRUNK	Trunk	Trunk	Trunk	Trunk	Limited Connectivity
SWITCHPORT MODE NEGOTIATE	Limited Connectivity	Limited Connectivity	Trunk	Trunk	Limited Connectivity
SWITCHPORT MODE ACCESS	Access	Access	Limited Connectivity	Limited Connectivity	Access

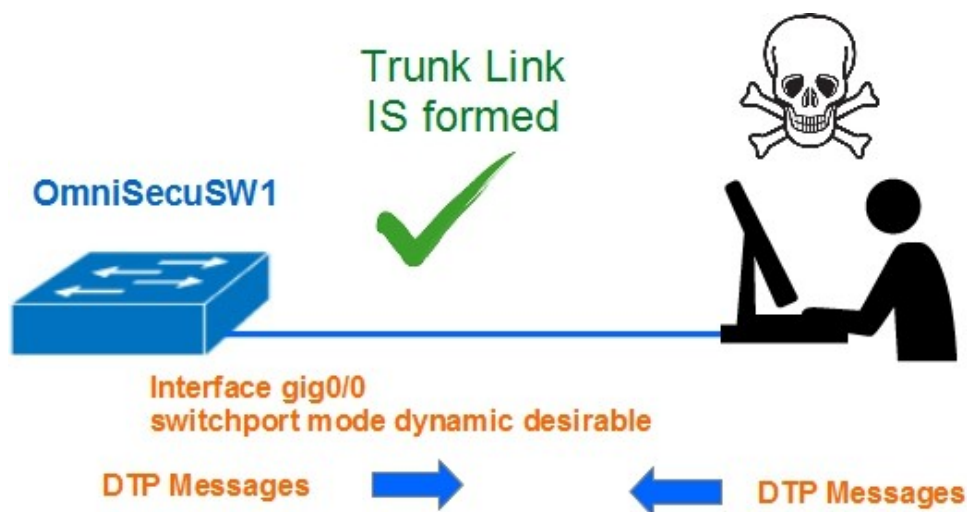
<https://ipwithease.com>

Immagine 2 Tabella che mostra le modalità di configurazione del protocollo DTP

3.2 In cosa consiste l'attacco

Lo switch spoofing è un attacco alle reti VLAN che sfrutta la configurazione non corretta delle porte di trunk, di default le porte di trunk hanno accesso a tutte le VLAN. L'attaccante sfrutta il fatto che la configurazione di default delle porte degli switch è impostata come dynamic auto, "il malintenzionato" configurerà un sistema per fingere se stesso come uno switch, per fare ciò è

necessario che l'attaccante sia in grado di emulare i messaggi 802.1Q e DTP, in questo modo può ottenere l'accesso a tutte le VLAN consentite sulla porta trunk.



3.3 Come difendersi

Il miglior modo per proteggersi da questo tipo di attacco è spegnere il trunking a tutte le porte, tranne quella che necessita il trunking. Sulle porte trunking richieste disabilitare il DTP e abilitare manualmente il trunking.

4 DIMOSTRAZIONE ATTACCO

Qui di seguito verrà presentata una dimostrazione pratica dell'attacco.

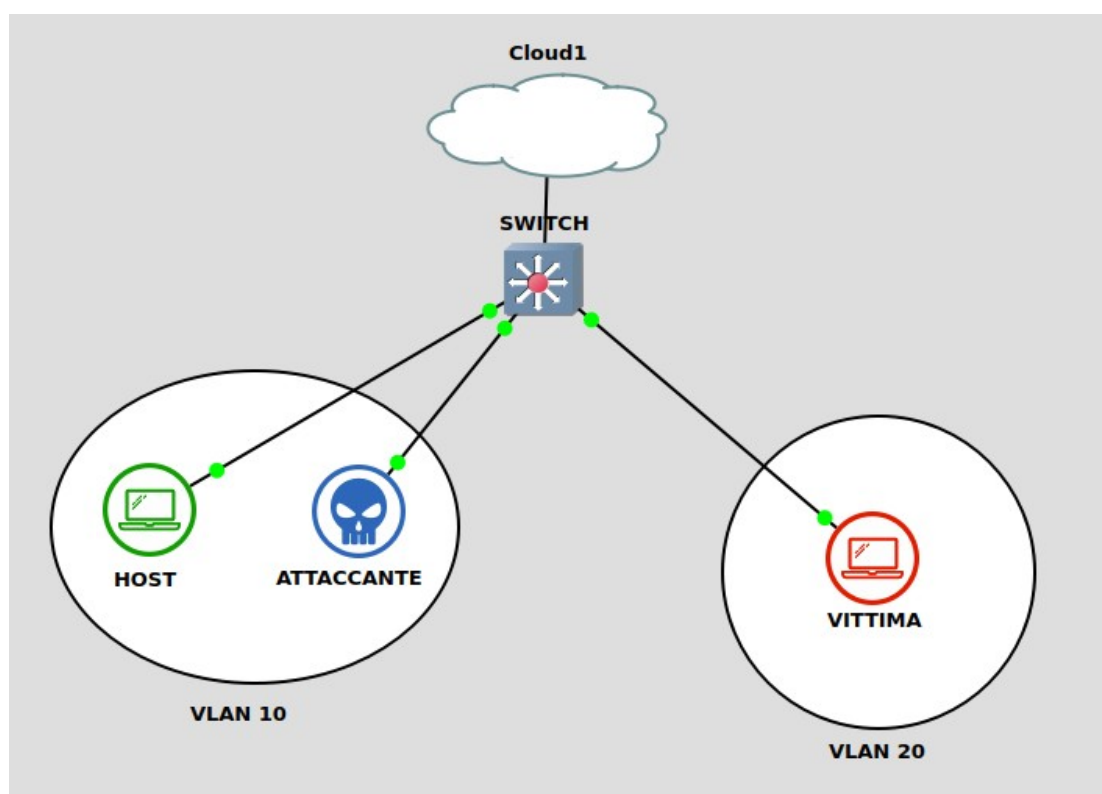
4.1 Requisiti

- **GNS3:** GNS3 è un emulatore di rete, il software consente di combinare dispositivi virtuali e reali, verrà utilizzata per simulare lo scenario.
- **Macchina Attaccante:** Macchina da cui partirà l'attacco, come sistema operativo verrà utilizzato Kali Linux, distribuzione di Linux pensata per la sicurezza e il penetration test.
- **Host:** Una comune macchina che sarà collegata nella stessa rete VLAN dell'attaccante.

- **Vittima:** Una comune macchina connessa in una VLAN differente dall'attaccante che subirà l'attacco
- **Switch:** Switch dove saranno connessi tutti gli host, lo switch utilizzato per questa dimostrazione è il cisco-iosvl2

4.2 Scenario

Lo scenario che ci troveremo davanti sarà il seguente: una piccola rete dove sono collegati tre dispositivi a uno switch. I dispositivi sono HOST e ATTACCANTE che sono collegati all'interno della VLAN 10 mentre la vittima è collegata all'interno della VLAN 20, in questo modo:



Nella seguente tabella vengono mostrati le informazioni dei vari dispositivi:

NOME	INDIRIZZO IP	VLAN ID
HOST	192.168.1.2	10
ATTACCANTE	192.168.1.38	10
VITTIMA	192.168.1.3	20

quindi possiamo dall'host pingare l'attaccante e viceversa:

```
HOST
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

HOST> ping 192.168.1.38

84 bytes from 192.168.1.38 icmp_seq=1 ttl=64 time=3.953 ms
84 bytes from 192.168.1.38 icmp_seq=2 ttl=64 time=5.204 ms
84 bytes from 192.168.1.38 icmp_seq=3 ttl=64 time=5.327 ms
84 bytes from 192.168.1.38 icmp_seq=4 ttl=64 time=4.166 ms
84 bytes from 192.168.1.38 icmp_seq=5 ttl=64 time=3.759 ms

HOST> 
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=2.91 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=1.57 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=4.79 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=4.64 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=4.83 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=4.58 ms

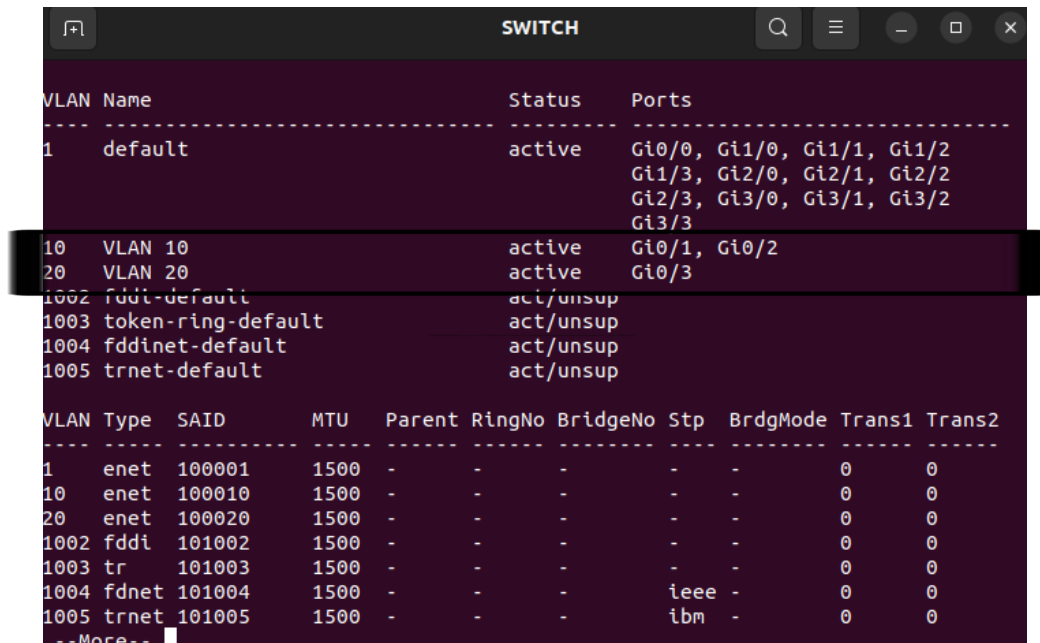
```

ovviamente nè l'attaccante nè l'host potranno pingare la vittima:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
From 192.168.1.38 icmp_seq=1 Destination Host Unreachable
From 192.168.1.38 icmp_seq=2 Destination Host Unreachable
From 192.168.1.38 icmp_seq=3 Destination Host Unreachable
From 192.168.1.38 icmp_seq=4 Destination Host Unreachable
From 192.168.1.38 icmp_seq=5 Destination Host Unreachable
From 192.168.1.38 icmp_seq=6 Destination Host Unreachable
From 192.168.1.38 icmp_seq=7 Destination Host Unreachable
From 192.168.1.38 icmp_seq=8 Destination Host Unreachable
From 192.168.1.38 icmp_seq=9 Destination Host Unreachable

```


In questo momento quindi lo stato delle VLAN sarà quello mostrato in questa foto:



The screenshot shows a network switch configuration window titled "SWITCH". It displays two tables. The first table shows the status of various VLANs, and the second table provides detailed configuration for each VLAN.

VLAN	Name	Status	Ports
1	default	active	Gi0/0, Gi1/0, Gi1/1, Gi1/2, Gi1/3, Gi2/0, Gi2/1, Gi2/2, Gi2/3, Gi3/0, Gi3/1, Gi3/2, Gi3/3
10	VLAN 10	active	Gi0/1, Gi0/2
20	VLAN 20	active	Gi0/3
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

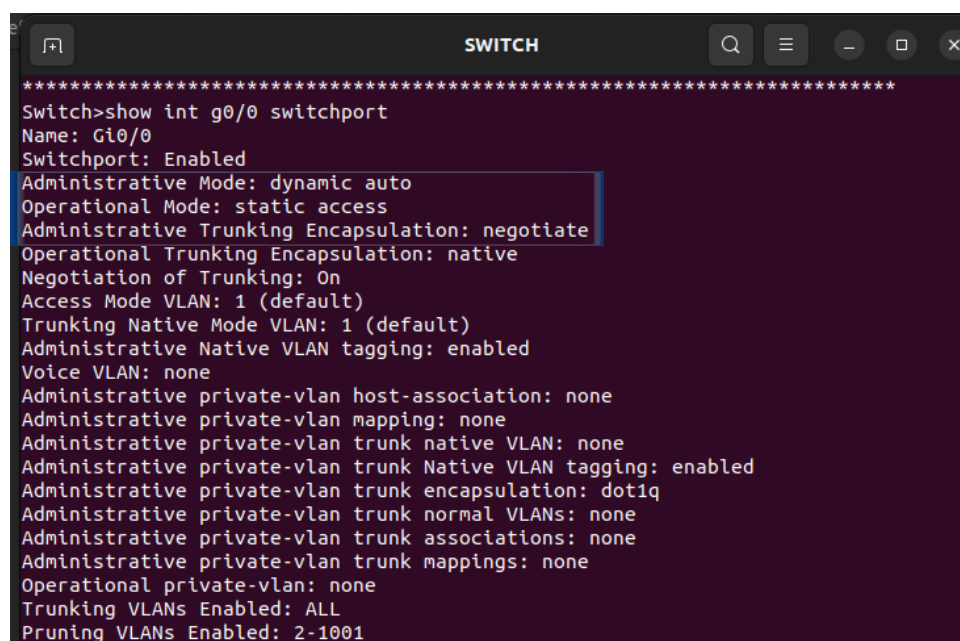
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

--More--

Come si può vedere le interfacce G0/1 e G0/2 che sono Host e l'Attaccante sono assegnate alla VLAN 10, mentre l'interfaccia G0/3 (la vittima) è assegnata alla vlan 20.

4.3 L'attacco

In questa dimostrazione d'attacco eseguiremo passo passo la tecnica di "switch spoofing". Come abbiamo detto in precedenza, per far sì che l'attacco abbia successo dobbiamo assicurarci che lo switch sia configurato come "dynamic auto" in modo tale che le VLAN potranno essere negoziate insieme.



The screenshot shows a network switch configuration window titled "SWITCH". It displays the configuration for interface Gi0/0, which is set to "dynamic auto" mode.

```
Switch>show int g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

Lo stato delle VLAN per il momento quindi sarà il seguente

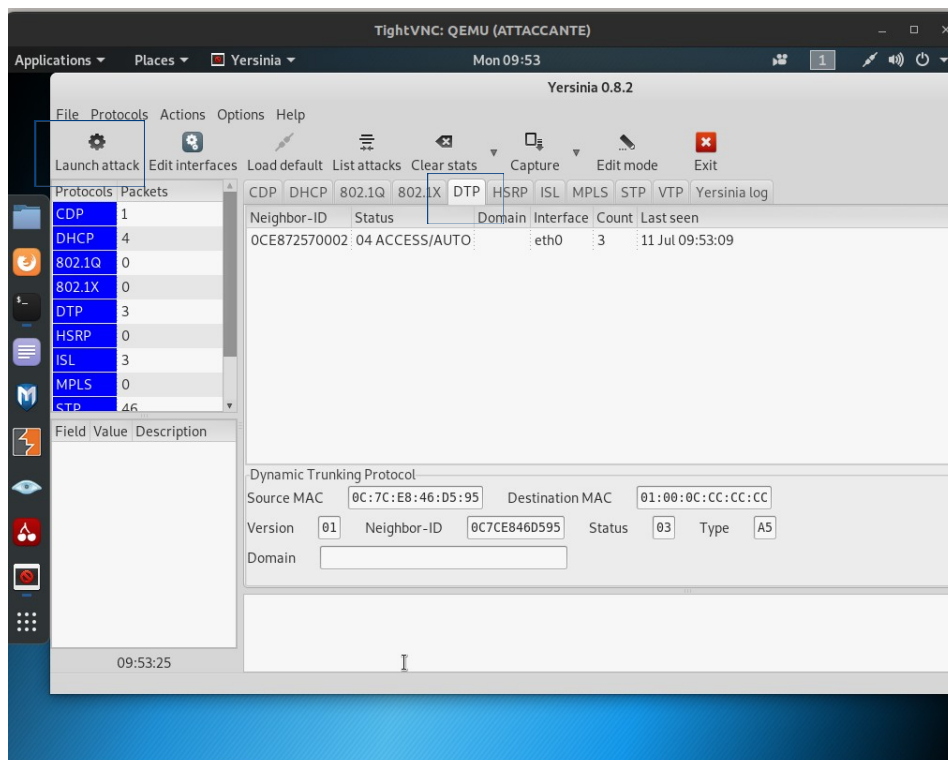
```
Switch>show int status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gi0/0		connected	1	a-full	auto	RJ45
Gi0/1		connected	10	a-full	auto	RJ45
Gi0/2		connected	10	a-full	auto	RJ45
Gi0/3		connected	20	a-full	auto	RJ45
Gi1/0		notconnect	1	a-full	auto	RJ45
Gi1/1		notconnect	1	a-full	auto	RJ45
Gi1/2		notconnect	1	a-full	auto	RJ45
Gi1/3		notconnect	1	a-full	auto	RJ45
Gi2/0		notconnect	1	a-full	auto	RJ45
Gi2/1		notconnect	1	a-full	auto	RJ45
Gi2/2		notconnect	1	a-full	auto	RJ45
Gi2/3		notconnect	1	a-full	auto	RJ45
Gi3/0		notconnect	1	a-full	auto	RJ45
Gi3/1		notconnect	1	a-full	auto	RJ45
Gi3/2		notconnect	1	a-full	auto	RJ45
Gi3/3		notconnect	1	a-full	auto	RJ45

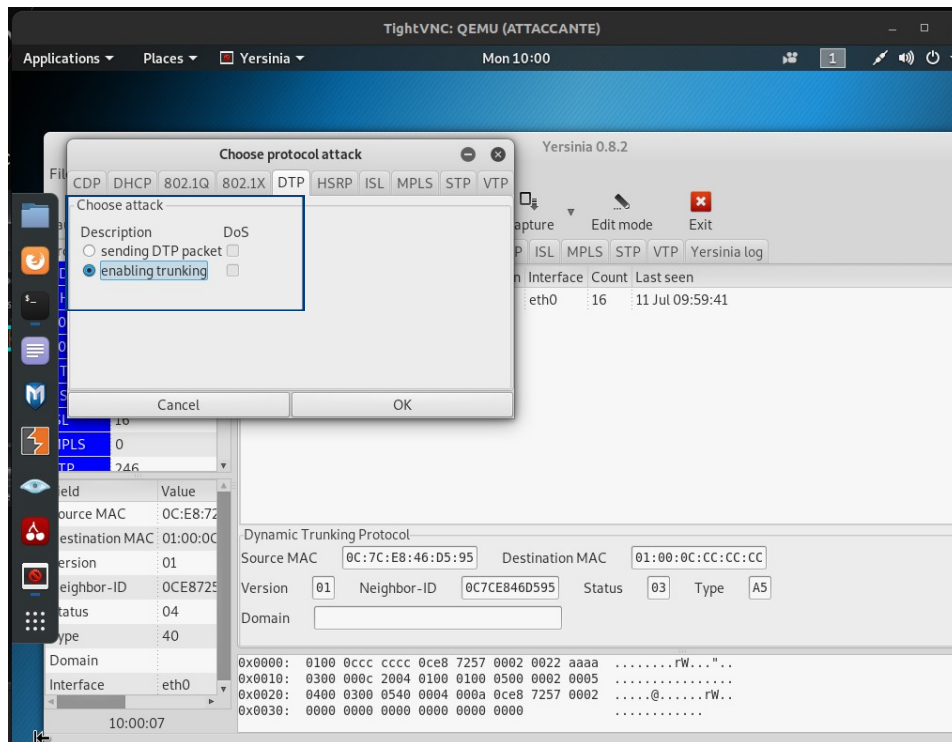
```
Switch>
```

Quindi le VLAN sono configurate correttamente, siamo pronti per effettuare l'attacco. Utilizzeremo **Yersinia**, un tool per sistemi Unix progettato per sfruttare delle falle nei protocolli di rete.

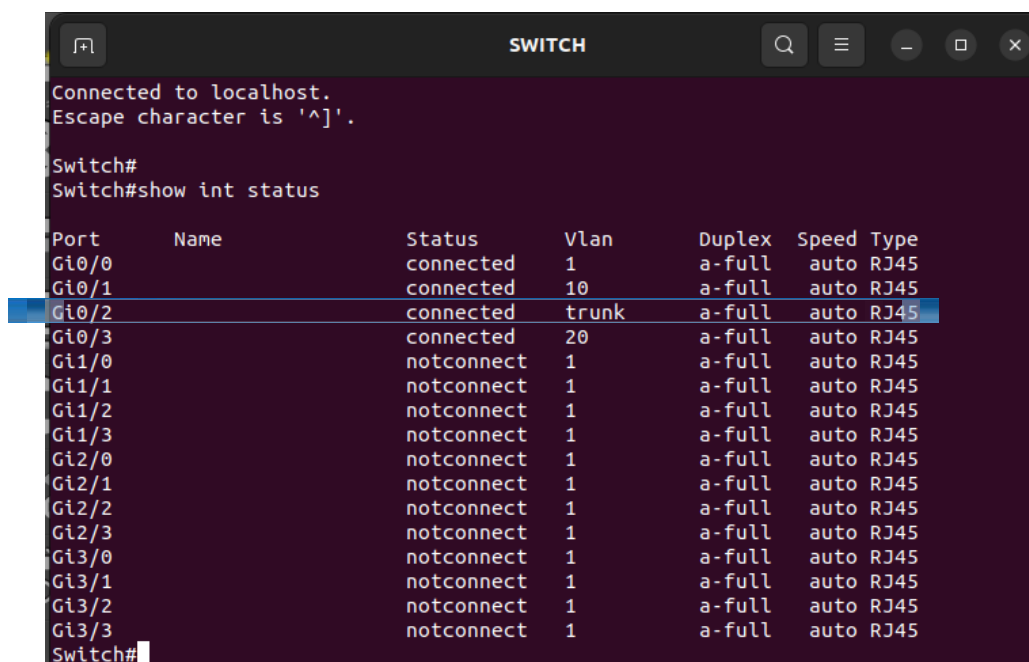
A questo punto con la macchina dell'attaccante possiamo aprire Yersinia e cliccare sulla sezione DTP per lanciare l'attacco



A questo punto possiamo cliccare su Launch Attack e scegliere come protocollo d'attacco enabling trunking



Adesso torniamo nella console dello switch per vedere lo stato delle interfacce VLAN.



Possiamo notare che l'interfaccia G0/2 (l'attaccante) è settato su Trunk, questo significa che possiamo saltare nelle altre VLAN!

Infatti se mostriamo lo stato dell'interfaccia trunk di G0/2 possiamo vedere che tutte le Vlan sono accessibili.

```
SWITCH
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Switch>
Switch>show int g0/2 trunk

Port      Mode      Encapsulation  Status      Native vlan
Gi0/2     auto      n-802.1q       trunking    1

Port      Vlan allowed on trunk
Gi0/2     1-4094

Port      Vlan allowed and active in management domain
Gi0/2     1,10,20

Port      Vlan in spanning tree forwarding state and not pruned
Gi0/2     1,10,20
Switch>
```

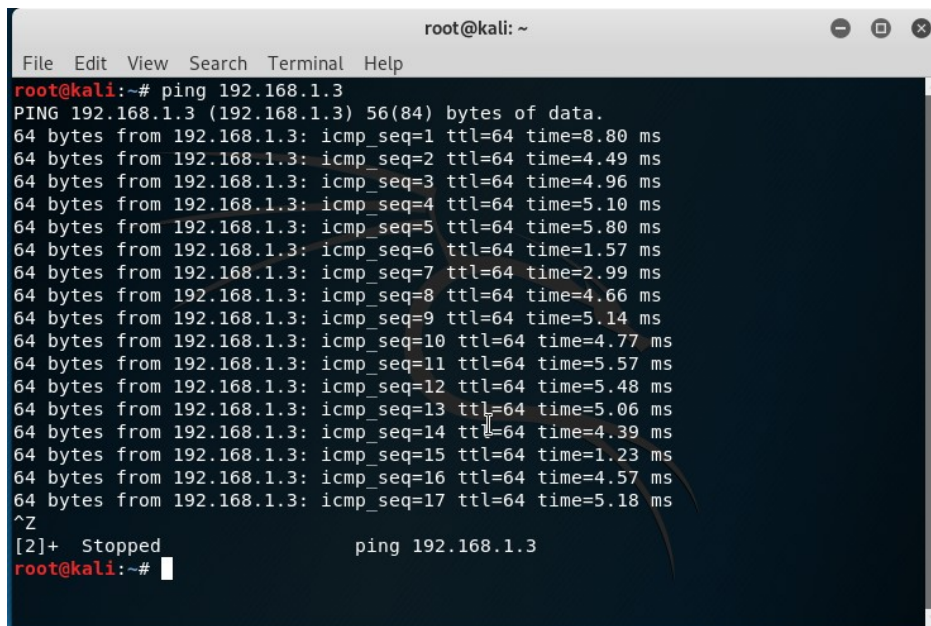
Quindi adesso l'attaccante potrà pingare la vittima, per farlo dal terminale della macchina dell'attaccante lanciamo i seguenti comandi:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# modprobe 8021q
root@kali:~# vconfig add eth0 20

Warning: vconfig is deprecated and might be removed in the future, please migrate to ip(route2) as soon as possible!

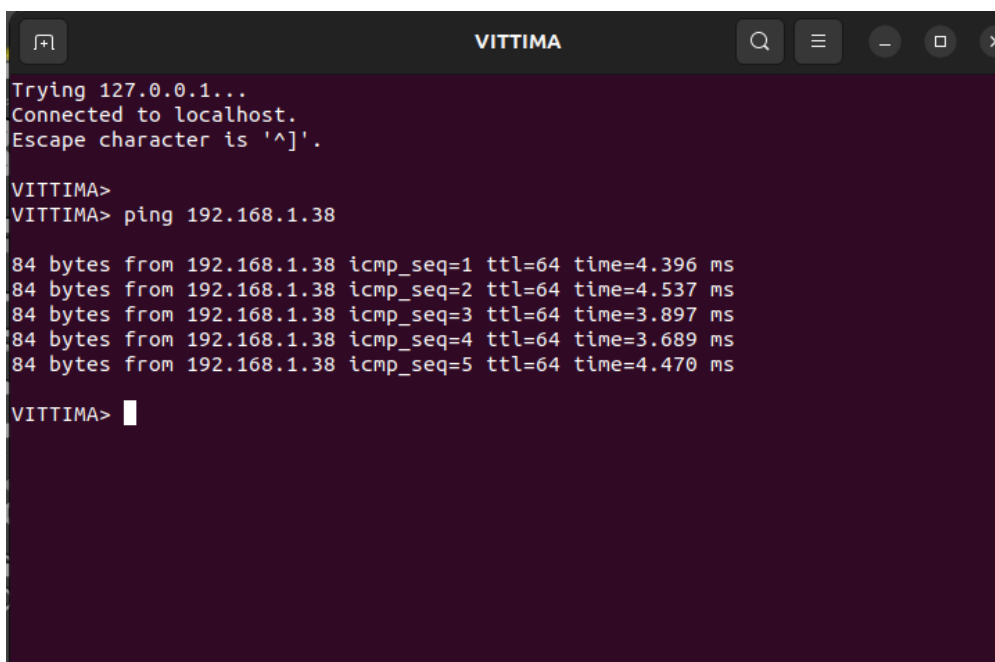
root@kali:~# ifconfig eth0.20 up
root@kali:~# ifconfig eth0.20 192.168.1.38 up
root@kali:~#
```

Con i comandi mostrati nella foto precedente abbiamo creato una nuova interfaccia VLAN impostando l'ID = 20, adesso non ci resta che riavviare la connessione e finalmente saremo in grado di pingare la macchina della vittima.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ping 192.168.1.3  
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.  
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=8.80 ms  
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=4.49 ms  
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=4.96 ms  
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=5.10 ms  
64 bytes from 192.168.1.3: icmp_seq=5 ttl=64 time=5.80 ms  
64 bytes from 192.168.1.3: icmp_seq=6 ttl=64 time=1.57 ms  
64 bytes from 192.168.1.3: icmp_seq=7 ttl=64 time=2.99 ms  
64 bytes from 192.168.1.3: icmp_seq=8 ttl=64 time=4.66 ms  
64 bytes from 192.168.1.3: icmp_seq=9 ttl=64 time=5.14 ms  
64 bytes from 192.168.1.3: icmp_seq=10 ttl=64 time=4.77 ms  
64 bytes from 192.168.1.3: icmp_seq=11 ttl=64 time=5.57 ms  
64 bytes from 192.168.1.3: icmp_seq=12 ttl=64 time=5.48 ms  
64 bytes from 192.168.1.3: icmp_seq=13 ttl=64 time=5.06 ms  
64 bytes from 192.168.1.3: icmp_seq=14 ttl=64 time=4.39 ms  
64 bytes from 192.168.1.3: icmp_seq=15 ttl=64 time=1.23 ms  
64 bytes from 192.168.1.3: icmp_seq=16 ttl=64 time=4.57 ms  
64 bytes from 192.168.1.3: icmp_seq=17 ttl=64 time=5.18 ms  
^Z  
[2]+  Stopped                  ping 192.168.1.3  
root@kali:~#
```

Ovviamente anche la macchina della vittima sarà in grado di pingare l'attaccante, come si evince dalla foto successiva.



```
VITTIMA  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^['.  
  
VITTIMA>  
VITTIMA> ping 192.168.1.38  
  
84 bytes from 192.168.1.38 icmp_seq=1 ttl=64 time=4.396 ms  
84 bytes from 192.168.1.38 icmp_seq=2 ttl=64 time=4.537 ms  
84 bytes from 192.168.1.38 icmp_seq=3 ttl=64 time=3.897 ms  
84 bytes from 192.168.1.38 icmp_seq=4 ttl=64 time=3.689 ms  
84 bytes from 192.168.1.38 icmp_seq=5 ttl=64 time=4.470 ms  
  
VITTIMA>
```

5 Conclusioni

Come abbiamo dimostrato sopra, per mezzo di questo attacco un “malintenzionato”, senza necessitare di particolari skills tecniche, è in grado di saltare da una VLAN all’altra. Questo tipo di attacco potrebbe risultare molto pericoloso poichè l’hacker, una volta introdotto nella VLAN della vittima, può intercettare il traffico avvalendosi di packet sniffer come **Wireshark** e ottenere informazioni private e dati sensibili. Nonostante ciò, occorre sapere, che con le giuste precauzioni è semplice proteggersi da questo tipo di attacco. Possiamo concludere dicendo che malgrado questa tipologia d’attacco possa risultare particolarmente pericolosa e infida il suo successo dipende unicamente dalla negligenza dell’amministratore di rete!

6 Bibliografia

- *Reti di calcolatori e internet Un approccio top-down: James F. Kurose - Keith W. Ross*
- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-2_2_e/vlan/configuration_guide/b_vlan_1522e_2960x_cg/b_vlan_152ex_2960-x_cg_chapter_011.html
- <https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=8>
- <https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKPREA4/vlan1-and-vlan-hopping-attack>
- <https://docs.gns3.com/docs/>
- <https://linux.die.net/man/8/yersinia>