



Rapport d'audit Beretta

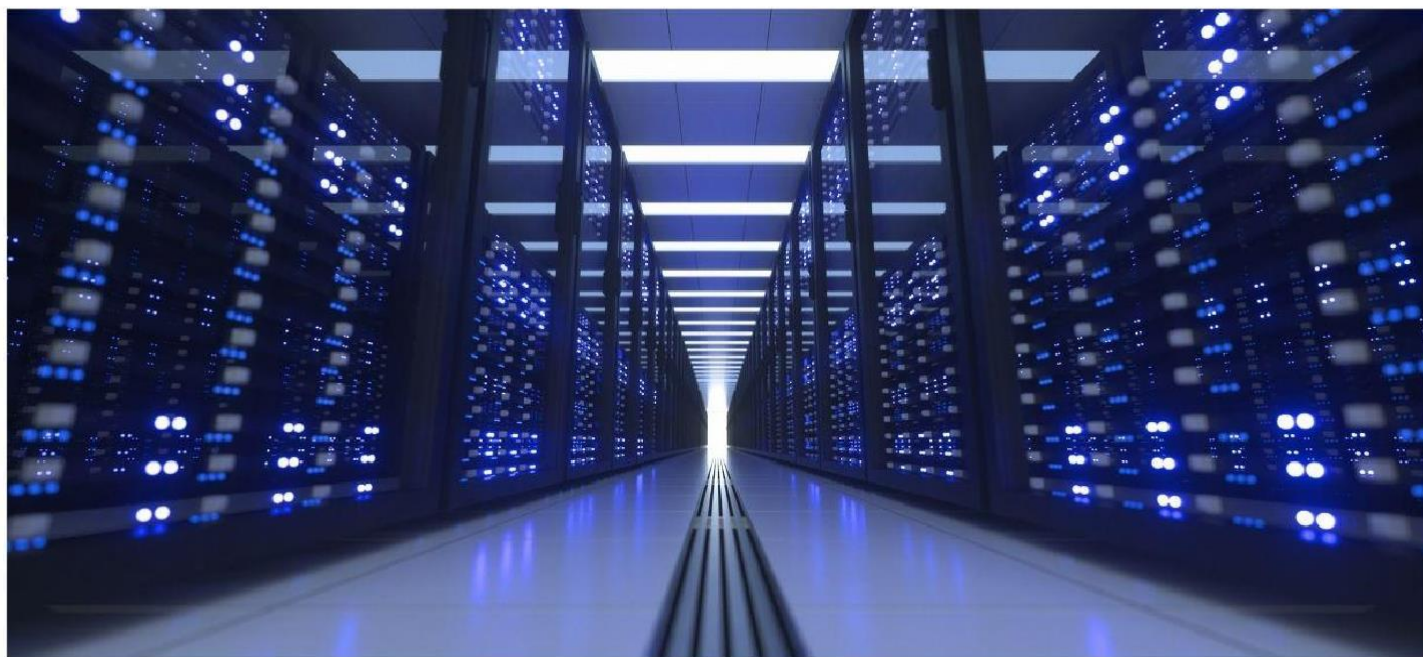


Table des matières

.....	1
Introduction	4
Contexte	4
Objectif de l'audit	4
Calendriers de maintenance et de surveillance	4
Périmètre de l'audit	4
Synthèse des vulnérabilités identifiées	5
Criticité des vulnérabilités	6
Principaux résultats de la phase d'enquête	8
Préconisations	12
Conclusion	12

Table des figures

Figure 1: OS activé.....	5
Figure 2: Antivirus Symantec installé.....	5
Figure 3: Liste des ports ouverts PC-RM.....	8
Figure 4: Liste des ports ouverts sur Hyper-V	8
Figure 5 : Ping normale.....	9
Figure 6: Etat normale du serveur	9
Figure 7: Liste des ports	10
Figure 8: Lancement de l'attaque	10
Figure 9: Résultat de l'attaque	11
Figure 10: Echec de Ping	11

Introduction

Contexte

La société BERETTA a fait appel à PROLOGIC Tunisie pour mener une évaluation de sécurité sous forme de test d'intrusion en effectuant des types d'attaques spécifiques. Ce document de compte rendu recense les vulnérabilités découvertes et les recommandations permettant de réduire les risques associés.

Objectif de l'audit

Cet audit a pour objectif d'évaluer le niveau de sécurité de l'infrastructure réseau et système de client Beretta, et de valider le bon cloisonnement des différents comptes utilisateurs en fonction de leurs droits d'accès sur les données.

Calendriers de maintenance et de surveillance

Fonctionnalités	OWNER	START DATE	deadline
Vérifier le matériel actifs	prologic	25/09/2023	02/10/2023
vérifier l'état des équipements, l'adressage ...	prologic	25/09/2023	02/10/2023
vérifier les logiciels utilisés dans l'entreprise	prologic	25/09/2023	02/10/2023
vérifier l'état de l'AD, les droits d'accès des utilisateurs	prologic	26/09/2023	02/10/2023
collecter les informations sur les ports ouverts de chaque	prologic	26/09/2023	02/10/2023
Test d'intrusion pour tester les vulnérabilités	prologic	02/10/2023	02/10/2023

Périmètre de l'audit

Le rapport d'audit examine la gestion des droits d'accès concernant Active Directory (AD) et les objets de stratégie de groupe (GPO), ainsi que la création de dossiers spécifiques pour chaque utilisateur.

L'audit est conçu pour déterminer les différentes vulnérabilités existantes dans cette infrastructure (réseaux, Sécurité et système).

Le check des équipements actifs est aussi une partie de cet audit pour déterminer s'il y'avait des logiciels malveillants parmi les logiciels installés sur chaque équipement.

Synthèse des vulnérabilités identifiées

Cet audit inclut deux parties principales.

- Audit sur la partie Système

Cet audit est dédié pour définir les logiciels installés sur les différents équipements, les droits d'accès des users sur AD et leurs accès au dossier partagé.

Lors de l'analyse des PC on a constaté que cette partie ne comporte pas des vulnérabilités :

- ❖ Chaque user sur l'AD a un accès défini au dossier partagé.
- ❖ Il n'y a pas de logiciels malveillants parmi les logiciels installés.
- ❖ Microsoft 365 est activé pour tous les utilisateurs.
- ❖ Les pare-feux des PCs et VMs sont activés.
- ❖ Les OS des PCs et des VM sont tous activés.

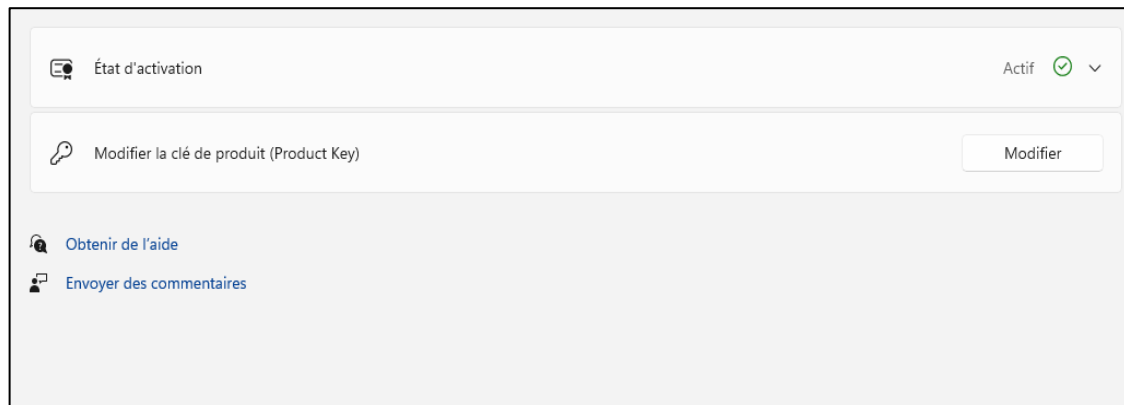


Figure 1: OS activé

❖ Symantec l'antivirus est installé et activé sur les machines

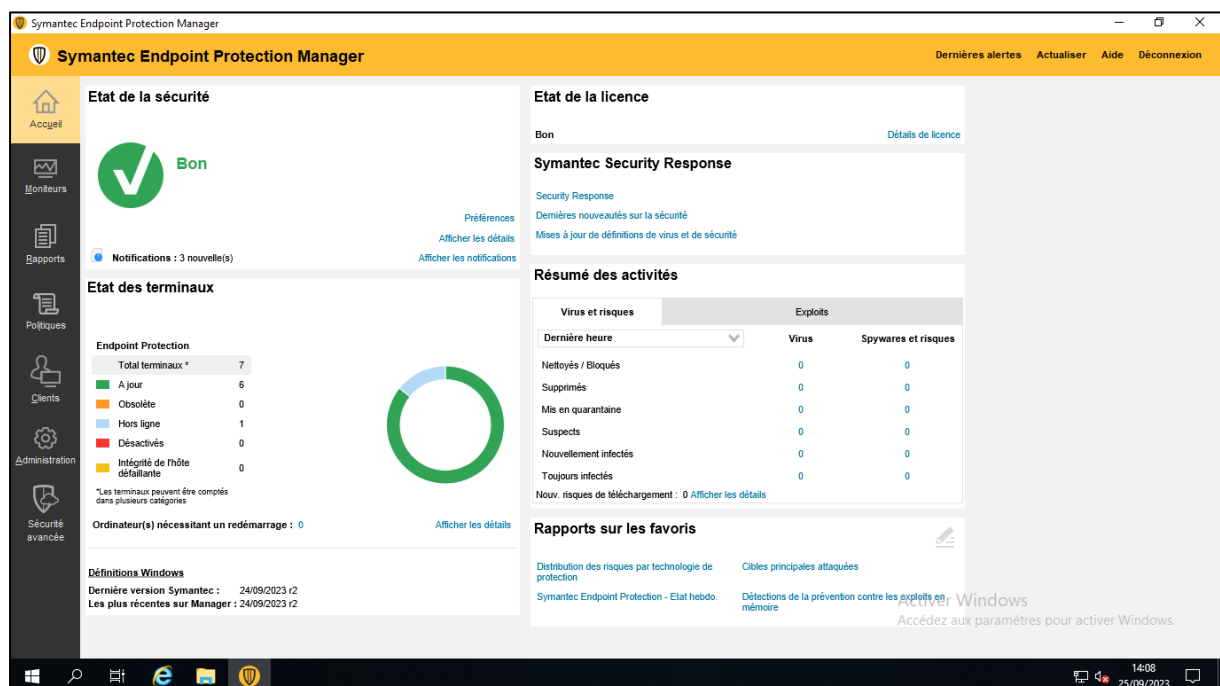


Figure 2: Antivirus Symantec installé

- Audit sur les équipements réseau et sécurité

Cet audit a comme but de vérifier l'état des équipements réseaux et sécurité actifs. Lors de cet audit on a prélevé quelques vulnérabilités :

- Firewall sans licence
- Absence de la segmentation réseau (des VLAN)
- Quelques ports exploitables sont ouverts sur des machines

Criticité des vulnérabilités

• L'absence de licence dans un pare-feu (Firewall)

L'absence de licence dans un pare-feu (firewall) peut entraîner plusieurs risques et inconvénients, notamment :

- **Exposition aux vulnérabilités non corrigées :** Il a été observé que le pare-feu ne bénéficie pas des mises à jour de sécurité périodiques fournies par le fabricant, exposant ainsi le système à des vulnérabilités connues non traitées.
- **Manque de support technique :** L'absence de licence a été relevée comme un facteur limitant l'accès au support technique du fabricant en cas de problèmes ou d'incidents, potentiellement affectant la résolution rapide des problèmes critiques.
- **Restriction des fonctionnalités :** Notre audit a révélé que l'absence de licence prive le pare-feu de fonctionnalités avancées, notamment l'inspection SSL/TLS, la prévention des intrusions (IPS) et la détection des logiciels malveillants, compromettant ainsi sa capacité à détecter et à contrer efficacement les menaces.
- **Conformité aux réglementations :** Il a été constaté que le pare-feu non mis à jour et non pris en charge pourrait entraver la conformité aux réglementations en matière de sécurité des données et de protection de la vie privée, ce qui pourrait entraîner des sanctions légales et financières.
- **Augmentation des risques de sécurité :** Un pare-feu non mis à jour et non pris en charge est plus susceptible d'être compromis par des attaquants. Cela peut entraîner des violations de données, des perturbations de service et d'autres problèmes de sécurité.
- **Perte de visibilité :** Les licences de pare-feu peuvent également inclure des outils de gestion et de surveillance avancés qui offrent une visibilité sur le trafic réseau, les menaces potentielles et les activités suspectes. Sans licence, vous perdrez cette visibilité, ce qui peut rendre difficile la

détection des activités malveillantes.

- **L'absence de segmentation réseau (VLANs)**

L'absence de segmentation réseau, notamment par l'utilisation de VLANs (Virtual Local Area Networks), peut entraîner plusieurs risques et vulnérabilités dans un environnement informatique, notamment :

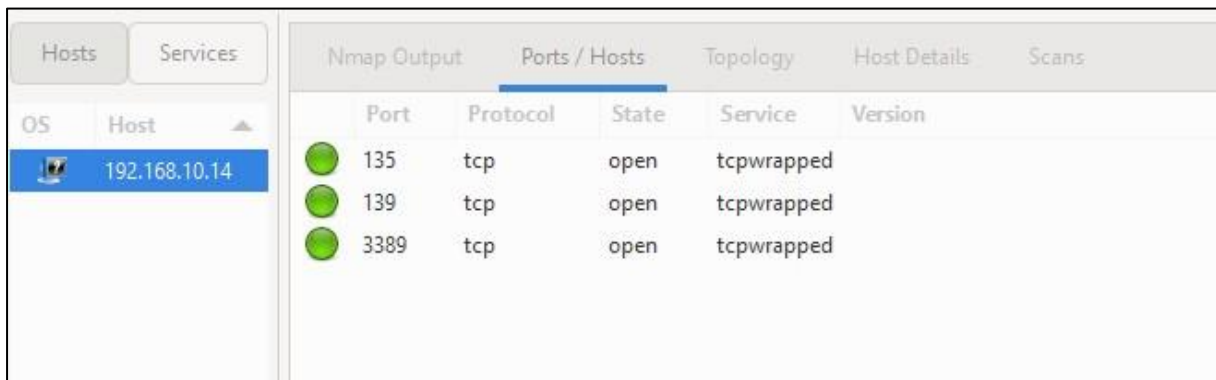
- **Augmentation des risques de sécurité :** En l'absence de segmentation, tous les dispositifs du réseau sont regroupés dans le même domaine de diffusion (broadcast domain), ce qui signifie que toute menace ou compromission potentielle peut se propager plus facilement à travers l'ensemble du réseau. Les attaquants ont ainsi un accès potentiel à une plus grande surface d'attaque.
- **Risque d'accès non autorisé :** Les VLANs sont un moyen efficace de séparer les utilisateurs, les services et les données en fonction de leur niveau de confiance et de leurs autorisations. L'absence de segmentation peut entraîner un accès non autorisé à des segments sensibles du réseau, augmentant ainsi le risque de violations de données et d'exploitations malveillantes.
- **Isolation des problèmes :** La segmentation réseau permet d'isoler les problèmes potentiels à l'intérieur d'un VLAN spécifique, ce qui facilite la détection et la résolution des problèmes sans perturber l'ensemble du réseau. En l'absence de segmentation, un problème sur un seul appareil peut affecter l'ensemble du réseau.
- **Contrôle de la bande passante :** Les VLANs permettent de gérer la bande passante de manière plus granulaire en attribuant des priorités et des quotas de bande passante aux différents segments du réseau. Sans segmentation, il peut être difficile de contrôler efficacement la répartition de la bande passante, ce qui peut entraîner des problèmes de performance du réseau.
- **Conformité aux réglementations :** Dans de nombreux secteurs, des réglementations strictes en matière de protection des données et de sécurité des réseaux sont en vigueur. L'absence de segmentation adéquate peut rendre difficile la conformité à ces réglementations, ce qui peut entraîner des conséquences juridiques et financières.
- **Difficulté de gestion :** Un réseau non segmenté peut être plus difficile à gérer, notamment en ce qui concerne la gestion des autorisations, des politiques de sécurité et des modifications de configuration. La segmentation facilite la gestion en permettant une séparation logique des ressources et des utilisateurs.

Principaux résultats de la phase d'enquête

Le scan des ports sur les machines actives nous donne ces résultats :

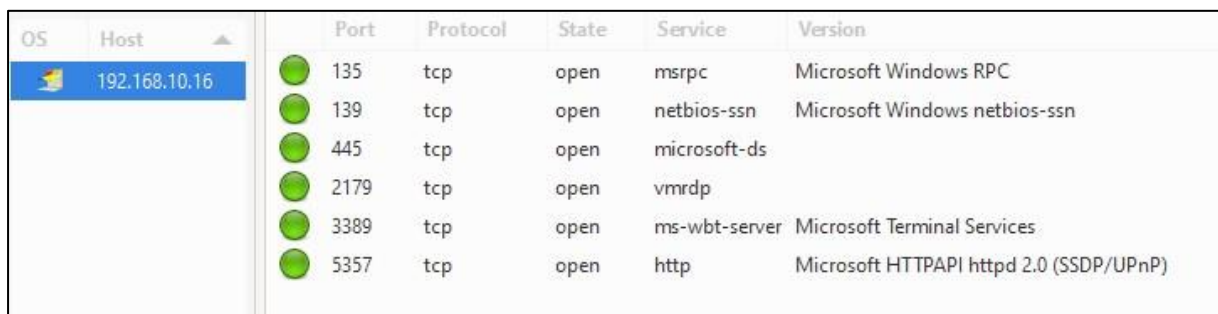
Equipement	OS	Ports ouverts
SRV-HYP	Windows server 2019	135/139/445/2179/3389/5357
SRV-DC (AD)	Windows server 2019	139/2000/3389/5060
SRV-VEEAM	Windows server 2019	111/135/139/445/1058/2000/2049/ 3389/5060/10001/10002/10003
Symantec	Windows server 2019	135/139/443/445/2638/3389/5357/ 8443/9090
VEEAMTEST	Windows server 2019	111/135/139/445/1058/2000/2049/ 3389/5060
Zabbix	Centos 8	22/80/2000/5060
PC-RM	Windows 11	135/139/3389
PC-Général- Manager(Gérant)	Windows 11	135/139/3389
PC-R-RMQ-A	Windows 10	135/139/3389
Les autres PC	Windows 10	135/139/3389
NVR	-	80/554
imprimante	-	80/443/515/631/8080/9100

Exemples :



Hosts		Nmap Output				
Services		Ports / Hosts				
OS	Host	Port	Protocol	State	Service	Version
	192.168.10.14	135	tcp	open	tcpwrapped	
		139	tcp	open	tcpwrapped	
		3389	tcp	open	tcpwrapped	

Figure 3: Liste des ports ouverts PC-RM



OS	Host	Port	Protocol	State	Service	Version
	192.168.10.16	135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
		445	tcp	open	microsoft-ds	
		2179	tcp	open	vmrpd	
		3389	tcp	open	ms-wbt-server	Microsoft Terminal Services
		5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Figure 4: Liste des ports ouverts sur Hyper-V

Lors de cet audit on a essayé de lancer une attaque sur l'un des ports ouverts, on a exploité le port 3389 (RDP) du serveur DC pour lancer une attaque DDOS sur ce port et voir le comportement du PC.

Comme le montre la figure je peux atteindre le serveur AD (ping OK).

```
# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=127 time=2.70 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=127 time=2.35 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=127 time=1.88 ms
^C
--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.884/2.310/2.701/0.334 ms
```

Figure 5 : Ping normale

Le comportement du serveur AD est normal (CPU < 5% + Flux reçu < 450 kbits)

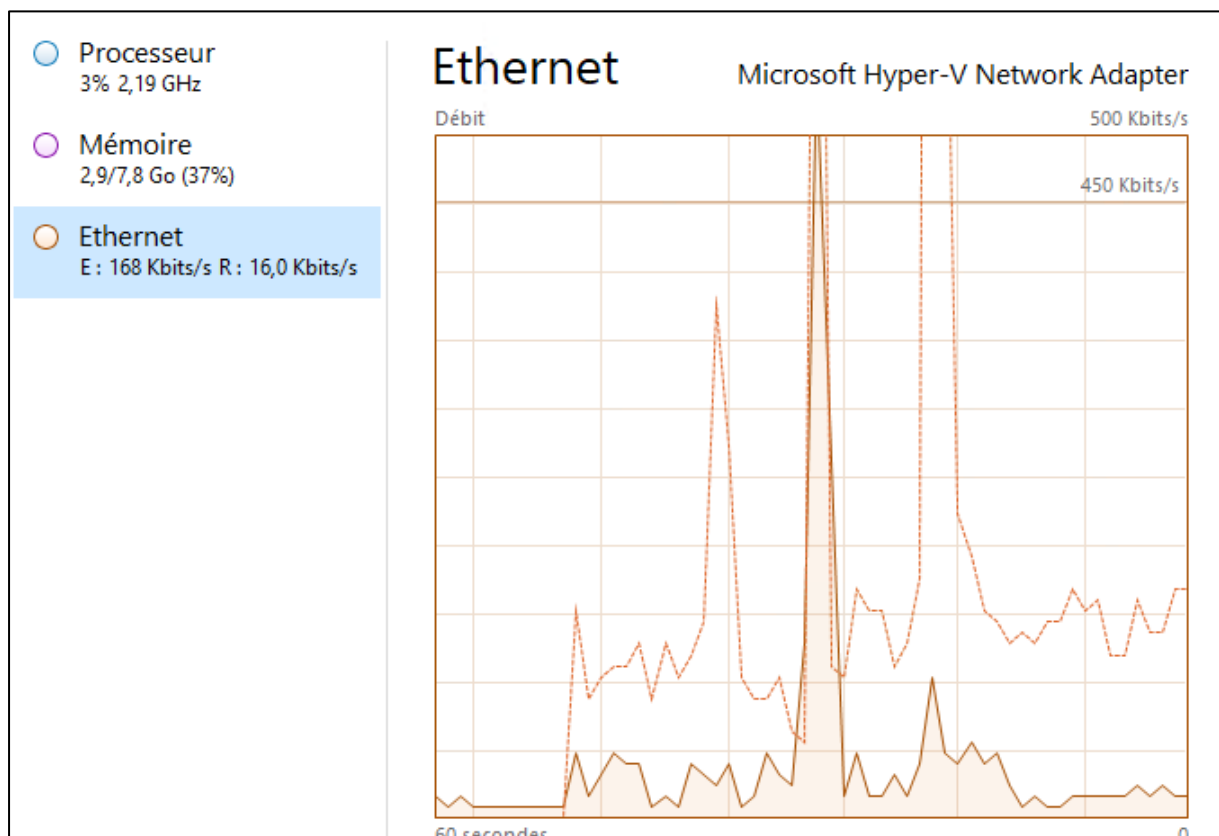


Figure 6: Etat normale du serveur

On a lancé un scan de ports pour déterminer les ports ouverts sur le serveur.

```

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-02 13:48 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.100.1
Host is up (0.0017s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
113/tcp    closed ident
139/tcp    open  netbios-ssn
2000/tcp   open  cisco-sccp
3389/tcp   open  ms-wbt-server
5060/tcp   open  sip

Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds

```

Figure 7: Liste des ports

On lance une attaque DDOS sur le port 3389 (bombarder le serveur par l'envoi des plusieurs paquets).

```

len=46 ip=192.168.100.1 ttl=127 DF id=20590 sport=3389 flags=SA seq=29695 win=64000 rtt=12.6 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20591 sport=3389 flags=SA seq=29696 win=64000 rtt=12.6 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20589 sport=3389 flags=SA seq=29697 win=64000 rtt=12.5 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20592 sport=3389 flags=SA seq=29698 win=64000 rtt=12.4 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20593 sport=3389 flags=SA seq=29699 win=64000 rtt=12.4 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20594 sport=3389 flags=SA seq=29700 win=64000 rtt=12.0 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20595 sport=3389 flags=SA seq=29701 win=64000 rtt=11.9 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20596 sport=3389 flags=SA seq=29702 win=64000 rtt=11.7 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20597 sport=3389 flags=SA seq=29703 win=64000 rtt=11.7 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20598 sport=3389 flags=SA seq=29704 win=64000 rtt=11.6 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20599 sport=3389 flags=SA seq=29705 win=64000 rtt=10.1 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20600 sport=3389 flags=SA seq=29706 win=64000 rtt=10.0 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20601 sport=3389 flags=SA seq=29707 win=64000 rtt=9.9 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20603 sport=3389 flags=SA seq=29709 win=64000 rtt=6.9 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20602 sport=3389 flags=SA seq=29708 win=64000 rtt=7.1 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20604 sport=3389 flags=SA seq=29710 win=64000 rtt=6.5 ms
len=46 ip=192.168.100.1 ttl=127 DF id=20605 sport=3389 flags=SA seq=29711 win=64000 rtt=6.4 ms
^C
--- 192.168.100.1 hping statistic ---
29730 packets transmitted, 26087 packets received, 13% packet loss
round-trip min/avg/max = 1.6/28.0/1095.4 ms

```

Figure 8: Lancement de l'attaque

Voilà le résultat le nombre de flux augmente > 12 Mbit/s et le CPU augmente > 30%).

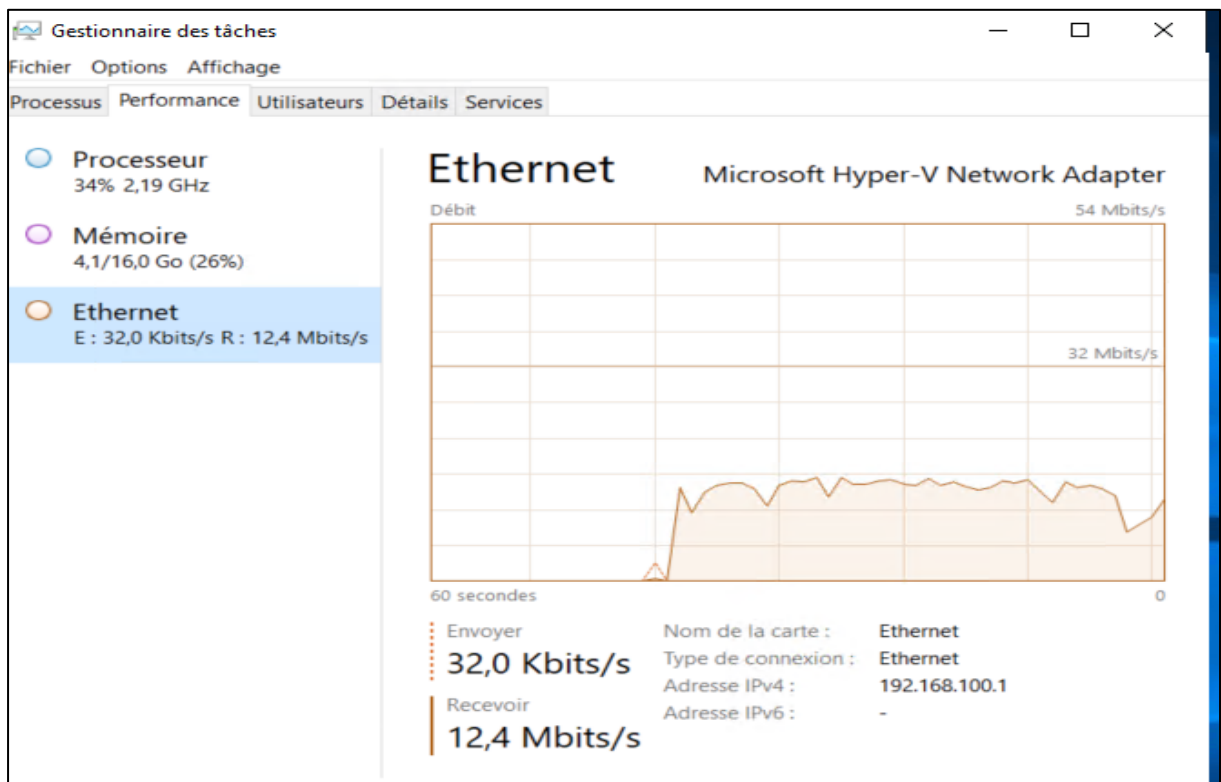


Figure 9: Résultat de l'attaque

Après quelques instants, le serveur devient inaccessible.

```
(root@kali)-[ ]
# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
From [ ] icmp_seq=1 Destination Host Unreachable
From [ ] icmp_seq=2 Destination Host Unreachable
From [ ] icmp_seq=3 Destination Host Unreachable
From [ ] icmp_seq=4 Destination Host Unreachable
From [ ] icmp_seq=5 Destination Host Unreachable
From [ ] icmp_seq=6 Destination Host Unreachable
^C
--- 192.168.100.1 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6147ms
pipe 4
```

Figure 10: Echec de Ping

Préconisations

Pour éviter toute type de vulnérabilité, il faut effectuer ces tâches :

- **Le firewall doit avoir une licence pour défendre contre toute type de menace ou attaque (DDOS ...)**
- **Segmenter les réseaux si c'est possible sur les switches actuels pour éviter la propagation des virus en cas d'attaque Ransomware.**
- **Essayer de minimiser le nombre des ports ouverts sur les machines critiques (fermer les ports non nécessaires)**

Conclusion

Pour conclure, la sécurité de l'infrastructure est l'un des facteurs les plus critique que le client doit donner une grande importance. Avoir un milieu de travail sécurisé c'est avoir un milieu plus productif.