

Pare-feu

Construction



Linux
Ubuntu 20.04
IP, TCP, UDP
80, 443, 53
OS
VERSION OS
PROTOCOLES ACTIFS
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Linux
Ubuntu 20.04
IP, TCP, UDP
80, 443, 53
OS
VERSION OS
PROTOCOLES ACTIFS
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Linux
Ubuntu 20.04
IP, TCP, UDP
80, 443, 53
OS
VERSION OS
PROTOCOLES ACTIFS
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Pare-feu

Construction



Linux
CentOS 7
IP, TCP, UDP
80, 443, 21
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Linux
CentOS 7
IP, TCP, UDP
80, 443, 21
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Linux
CentOS 7
IP, TCP, UDP
80, 443, 21
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Tunnel VPN

Construction

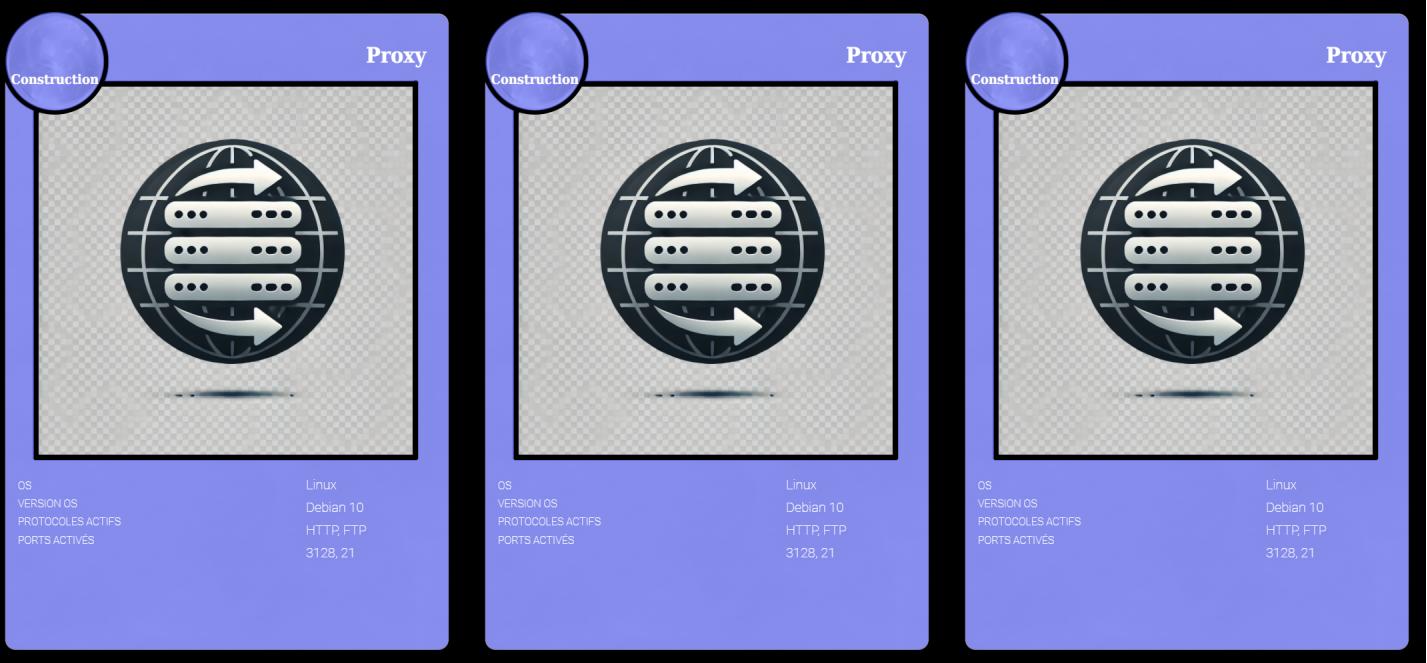
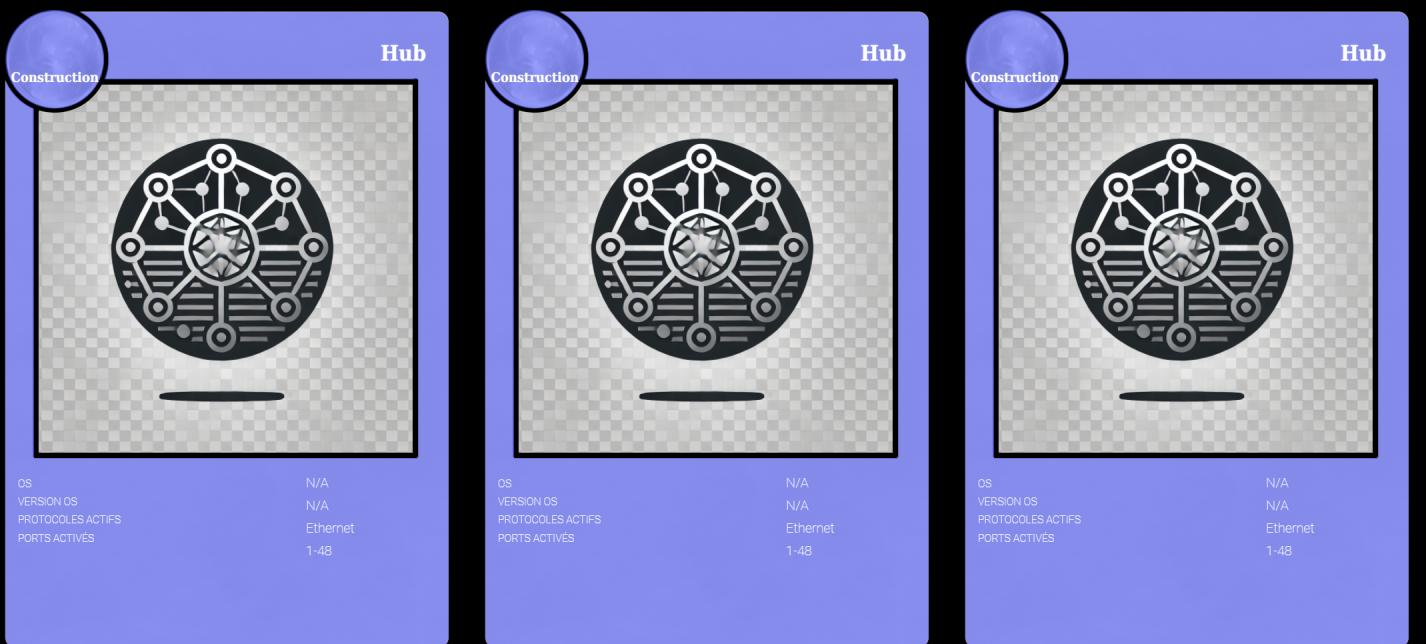
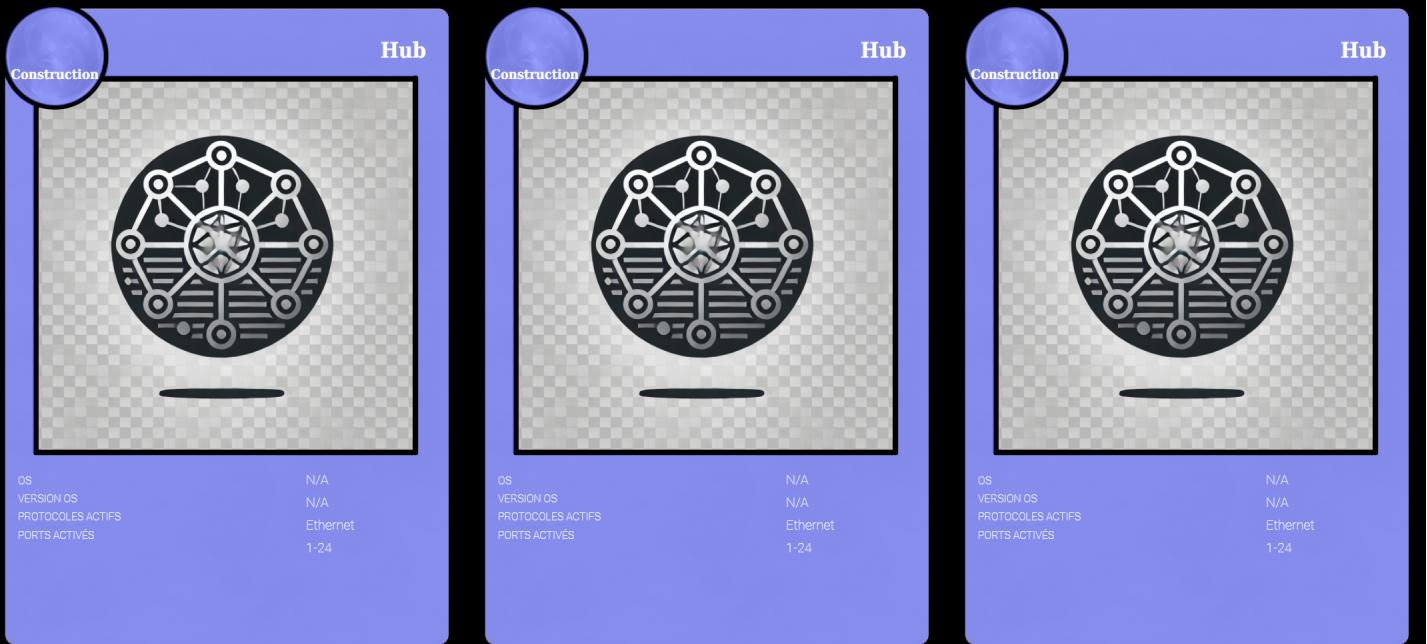


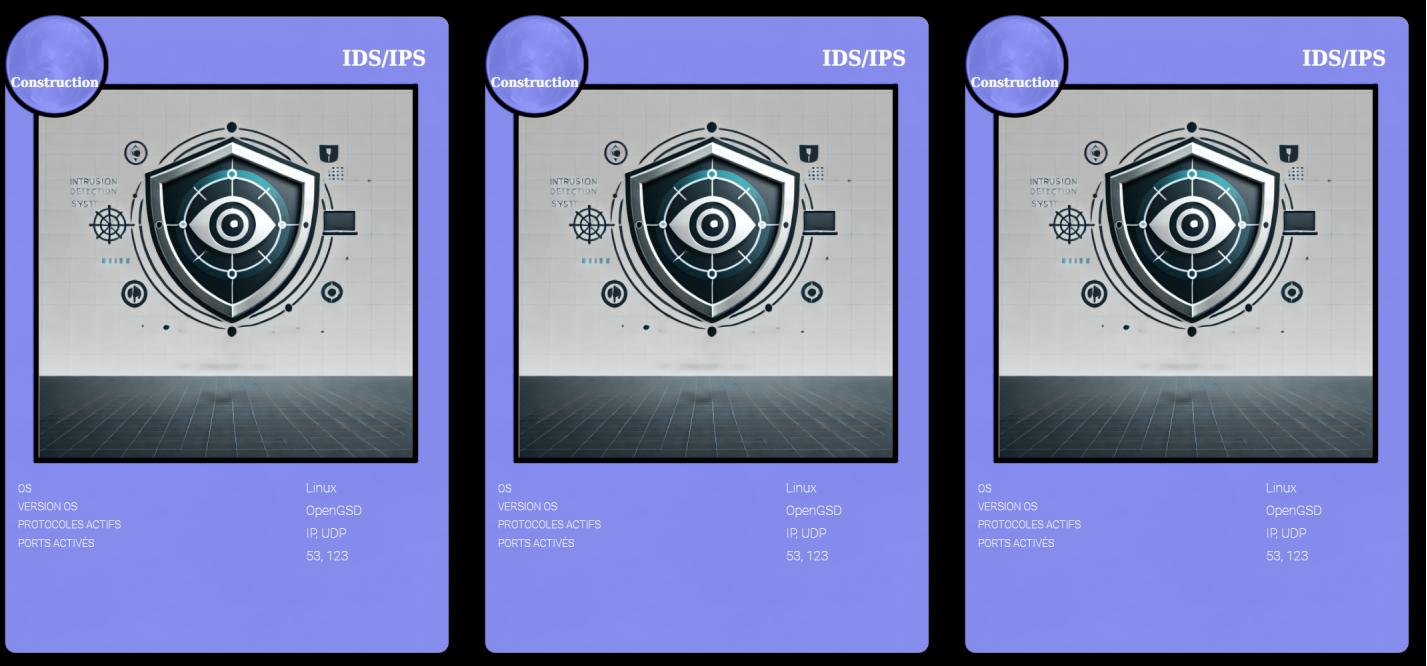
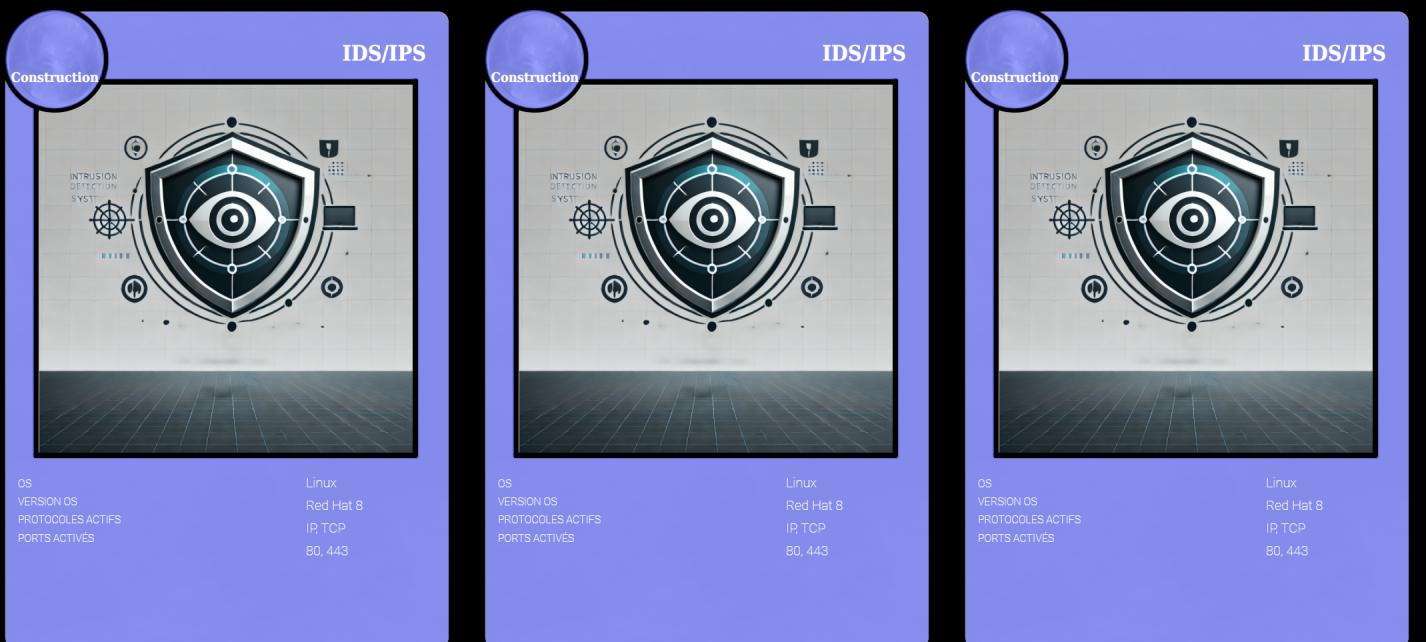
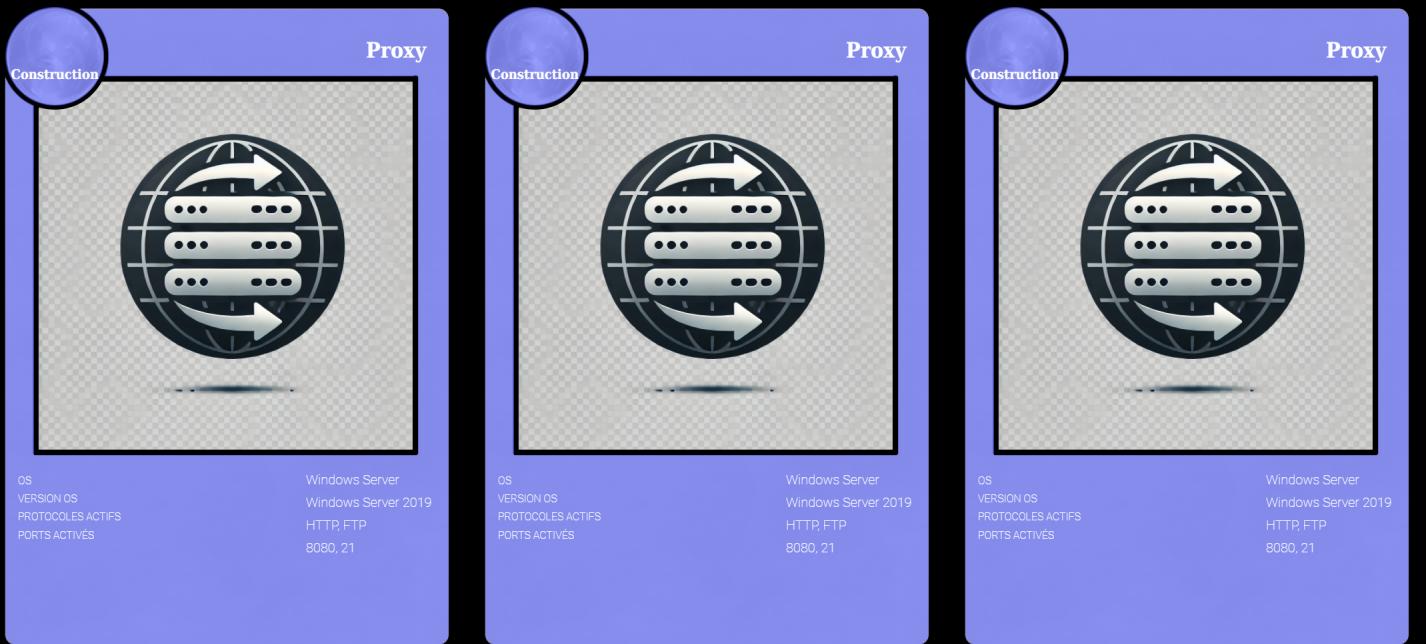
Linux
CentOS 8
PPTP
1723
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

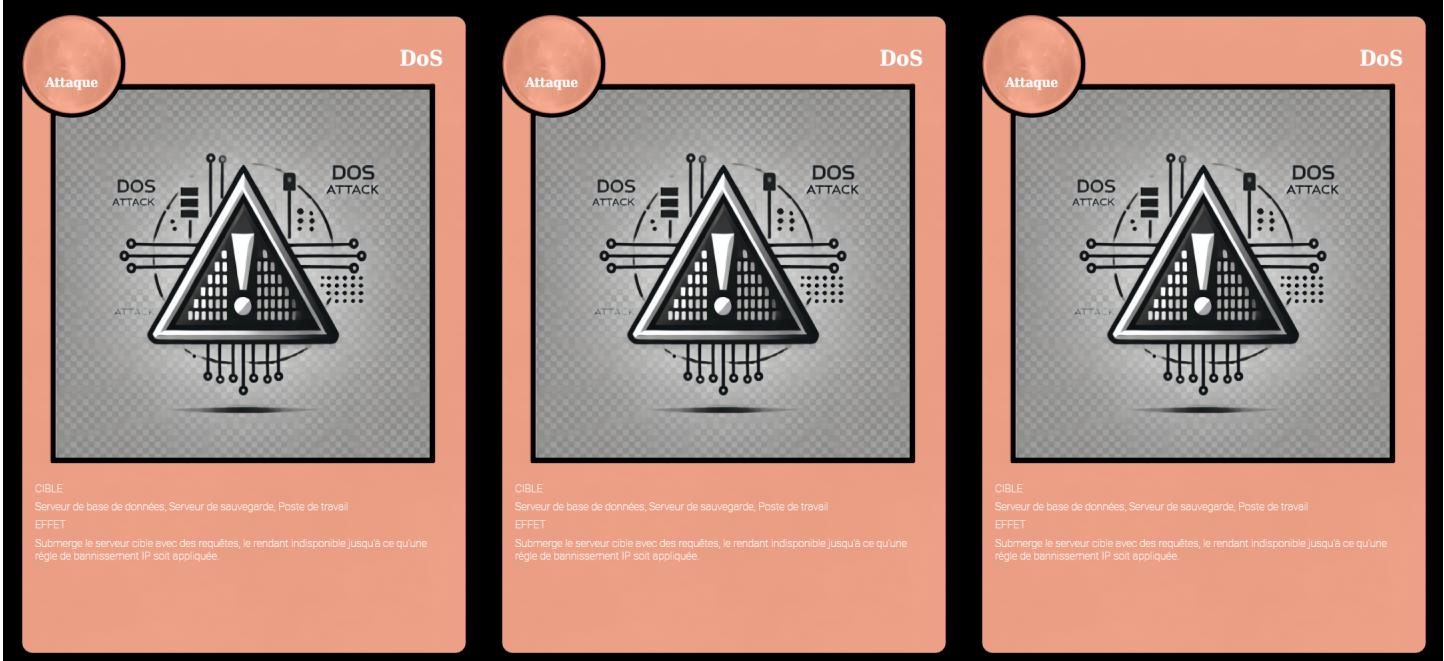
Linux
CentOS 8
PPTP
1723
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

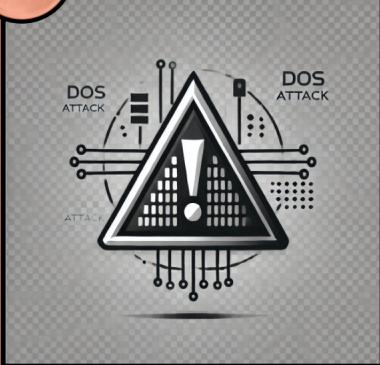
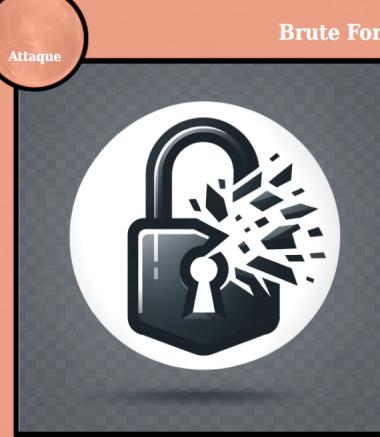
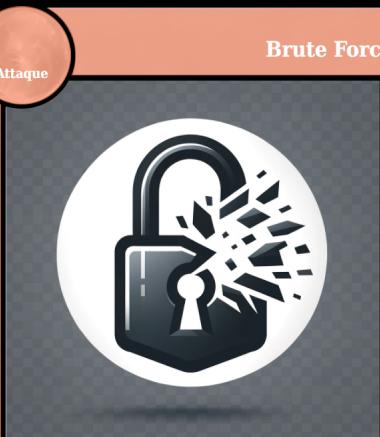
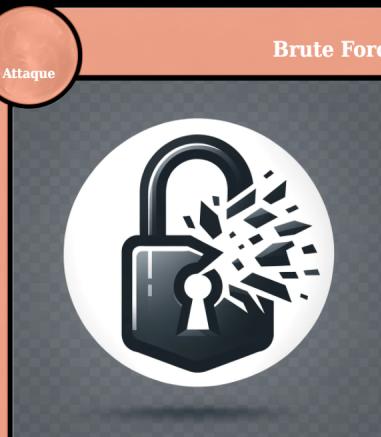
Linux
CentOS 8
PPTP
1723
OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

<p>Tunnel VPN</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Windows Server Windows Server 2016 L2TP 1701</p>	<p>Tunnel VPN</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>Windows Server Windows Server 2016 L2TP 1701</p>	<p>Tunnel VPN</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Windows Server Windows Server 2016 L2TP 1701</p>
<p>Routeur</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Cisco IOS IOS 15.2 IP, OSPF 179, 23</p>	<p>Routeur</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>Cisco IOS IOS 15.2 IP, OSPF 179, 23</p>	<p>Routeur</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Cisco IOS IOS 15.2 IP, OSPF 179, 23</p>
<p>Routeur</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Juniper Junos Junos 18.4 IP, RIP 520, 23</p>	<p>Routeur</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>Juniper Junos Junos 18.4 IP, RIP 520, 23</p>	<p>Routeur</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Juniper Junos Junos 18.4 IP, RIP 520, 23</p>







Attaque	DoS	DDoS	DDoS	Brute Force	Brute Force	Brute Force
						
	DoS	DDoS	DDoS	Brute Force	Brute Force	Brute Force
CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail
EFFET Submerge le serveur cible avec des requêtes, le rendant indisponible jusqu'à ce qu'une règle de bannissement IP soit appliquée.	EFFET Inonde le serveur cible avec un trafic massif provenant de multiples sources, le rendant indisponible jusqu'à ce que des mesures de limitation du taux de connexion soient mises en place.	EFFET Inonde le serveur cible avec un trafic massif provenant de multiples sources, le rendant indisponible jusqu'à ce que des mesures de limitation du taux de connexion soient mises en place.	EFFET Inonde le serveur cible avec un trafic massif provenant de multiples sources, le rendant indisponible jusqu'à ce que des mesures de limitation du taux de connexion soient mises en place.	EFFET Tente de deviner les mots de passe en essayant de nombreuses combinaisons jusqu'à réussir, rendant les comptes vulnérables jusqu'à ce que l'authentification à deux facteurs (2FA) soit activée.	EFFET Tente de deviner les mots de passe en essayant de nombreuses combinaisons jusqu'à réussir, rendant les comptes vulnérables jusqu'à ce que l'authentification à deux facteurs (2FA) soit activée.	EFFET Tente de deviner les mots de passe en essayant de nombreuses combinaisons jusqu'à réussir, rendant les comptes vulnérables jusqu'à ce que l'authentification à deux facteurs (2FA) soit activée.

Attaque

Man-in-the-Middle (MITM)

CIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Intercepte et modifie les communications entre deux parties, compromettant les données jusqu'à ce que le chiffrement SSL/TLS soit activé.

Attaque

Man-in-the-Middle (MITM)

CIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Intercepte et modifie les communications entre deux parties, compromettant les données jusqu'à ce que le chiffrement SSL/TLS soit activé.

Attaque

Man-in-the-Middle (MITM)

CIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Intercepte et modifie les communications entre deux parties, compromettant les données jusqu'à ce que le chiffrement SSL/TLS soit activé.

Attaque

Man-in-the-Middle (MITM)

CIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Intercepte et modifie les communications entre deux parties, compromettant les données jusqu'à ce que le chiffrement SSL/TLS soit activé.

Attaque

Injection SQL

CIBLE
Serveur de base de données

EFFET
Exploite les failles des bases de données pour exécuter des requêtes SQL malveillantes, compromettant les données jusqu'à ce que la mise à jour des logiciels soit effectuée.

Attaque

Injection SQL

CIBLE
Serveur de base de données

EFFET
Exploite les failles des bases de données pour exécuter des requêtes SQL malveillantes, compromettant les données jusqu'à ce que la mise à jour des logiciels soit effectuée.

Attaque

Injection SQL

CIBLE
Serveur de base de données

EFFET
Exploite les failles des bases de données pour exécuter des requêtes SQL malveillantes, compromettant les données jusqu'à ce que la mise à jour des logiciels soit effectuée.

Attaque

IP Spoofing

CIBLE
Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Utilise l'adresse IP d'un autre appareil pour masquer l'identité de l'attaquant et détourner le trafic, affectant le réseau jusqu'à ce qu'une règle de routage sécurisée soit définie.

IP Spoofing	IP Spoofing	IP Spoofing
 <p>Attaque</p>	 <p>Attaque</p>	 <p>Attaque</p>
<p>CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Usurpe l'adresse IP d'un autre appareil pour masquer l'identité de l'attaquant et détourner le trafic, affectant le réseau jusqu'à ce qu'une règle de routage sécurisée soit définie.</p>	<p>CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Usurpe l'adresse IP d'un autre appareil pour masquer l'identité de l'attaquant et détourner le trafic, affectant le réseau jusqu'à ce qu'une règle de routage sécurisée soit définie.</p>	<p>CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Usurpe l'adresse IP d'un autre appareil pour masquer l'identité de l'attaquant et détourner le trafic, affectant le réseau jusqu'à ce qu'une règle de routage sécurisée soit définie.</p>
ARP Poisoning	ARP Poisoning	ARP Poisoning
 <p>Attaque</p>	 <p>Attaque</p>	 <p>Attaque</p>
<p>CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Envie des messages ARP falsifiés pour associer l'adresse MAC de l'attaquant à une adresse IP légitime, détournant ainsi le trafic jusqu'à ce que le filtrage des paquets ARP soit mis en place.</p>	<p>CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Envie des messages ARP falsifiés pour associer l'adresse MAC de l'attaquant à une adresse IP légitime, détournant ainsi le trafic jusqu'à ce que le filtrage des paquets ARP soit mis en place.</p>	<p>CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Envie des messages ARP falsifiés pour associer l'adresse MAC de l'attaquant à une adresse IP légitime, détournant ainsi le trafic jusqu'à ce que le filtrage des paquets ARP soit mis en place.</p>
ARP Poisoning	Phishing	Phishing
 <p>Attaque</p>	 <p>Attaque</p>	 <p>Attaque</p>
<p>CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Envie des messages ARP falsifiés pour associer l'adresse MAC de l'attaquant à une adresse IP légitime, détournant ainsi le trafic jusqu'à ce que le filtrage des paquets ARP soit mis en place.</p>	<p>CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Trompe les utilisateurs pour qu'ils divulguent des informations sensibles via des faux emails ou sites web, exposant les données jusqu'à ce que des politiques de sécurité des e-mails soient appliquées.</p>	<p>CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail</p> <p>EFFET Trompe les utilisateurs pour qu'ils divulguent des informations sensibles via des faux emails ou sites web, exposant les données jusqu'à ce que des politiques de sécurité des e-mails soient appliquées.</p>

Attaque	Phishing	Ransomware
CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Trompe les utilisateurs pour qu'ils divulguent des informations sensibles via des faux emails ou sites web, exposant les données jusqu'à ce que des politiques de sécurité des e-mails soient appliquées.	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Trompe les utilisateurs pour qu'ils divulguent des informations sensibles via des faux emails ou sites web, exposant les données jusqu'à ce que des politiques de sécurité des e-mails soient appliquées.	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Chiffre les données du système cible et demande une rançon pour les déchiffrer, rendant les données inaccessibles jusqu'à ce que des sauvegardes sécurisées et des mises à jour de sécurité soient appliquées.
CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Chiffre les données du système cible et demande une rançon pour les déchiffrer, rendant les données inaccessibles jusqu'à ce que des sauvegardes sécurisées et des mises à jour de sécurité soient appliquées.	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Chiffre les données du système cible et demande une rançon pour les déchiffrer, rendant les données inaccessibles jusqu'à ce que des sauvegardes sécurisées et des mises à jour de sécurité soient appliquées.	CIBLE Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Chiffre les données du système cible et demande une rançon pour les déchiffrer, rendant les données inaccessibles jusqu'à ce que des sauvegardes sécurisées et des mises à jour de sécurité soient appliquées.
Attaque	Fragmentation IP	Fragmentation IP
CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Envie des paquets IP fragmentés pour contourner les dispositifs de sécurité et provoquer des dysfonctionnements jusqu'à ce que le filtrage des ports soit activé.	CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Envie des paquets IP fragmentés pour contourner les dispositifs de sécurité et provoquer des dysfonctionnements jusqu'à ce que le filtrage des ports soit activé.	CIBLE Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail EFFET Envie des paquets IP fragmentés pour contourner les dispositifs de sécurité et provoquer des dysfonctionnements jusqu'à ce que le filtrage des ports soit activé.

Fragmentation IP

Attaque

CIBLE
Routeur, Serveur de base de données, Serveur de sauvegarde, Poste de travail
EFFET
Envie des paquets IP fragmentés pour contourner les dispositifs de sécurité et provoquer des dysfonctionnements jusqu'à ce que le filtrage des ports soit activé.

Règle de Bannissement IP

Événement

MATERIEL POSSIBLE
Pare-feu, Routeur
EFFET
Bloque les adresses IP spécifiques pour empêcher les attaques de type DoS et DDoS.
ATTAQUE(S) CONTRÉE(S)
DoS
DdoS

Règle de Bannissement IP

Événement

MATERIEL POSSIBLE
Pare-feu, Routeur
EFFET
Bloque les adresses IP spécifiques pour empêcher les attaques de type DoS et DDoS.
ATTAQUE(S) CONTRÉE(S)
DoS
DdoS

Règle de Bannissement IP

Événement

MATERIEL POSSIBLE
Pare-feu, Routeur
EFFET
Bloque les adresses IP spécifiques pour empêcher les attaques de type DoS et DDoS.
ATTAQUE(S) CONTRÉE(S)
DoS
DdoS

Activation du Chiffrement SSL/TLS

Événement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail
EFFET
Chiffre les communications pour empêcher les attaques Man-in-the-Middle (MITM).
ATTAQUE(S) CONTRÉE(S)
MITM

Activation du Chiffrement SSL/TLS

Événement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail
EFFET
Chiffre les communications pour empêcher les attaques Man-in-the-Middle (MITM).
ATTAQUE(S) CONTRÉE(S)
MITM

Activation du Chiffrement SSL/TLS

Événement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail
EFFET
Chiffre les communications pour empêcher les attaques Man-in-the-Middle (MITM).
ATTAQUE(S) CONTRÉE(S)
MITM

Filtrage des Paquets ARP

Événement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail
EFFET
Chiffre les communications pour empêcher les attaques Man-in-the-Middle (MITM).
ATTAQUE(S) CONTRÉE(S)
MITM

Filtrage des Paquets ARP

Événement

MATERIEL POSSIBLE
Routeur, IDS/IPS
EFFET
Déetecte et bloque les paquets ARP malveillants pour prévenir les attaques par ARP Poisoning.
ATTAQUE(S) CONTRÉE(S)
ARP Poisoning

Filtrage des Paquets ARP

Événement

MATERIEL POSSIBLE
Routeur, IDS/IPS
EFFET
DéTECTe et bloque les paquets ARP malveillants pour prévenir les attaques par ARP Poisoning.
ATTAQUE(S) CONTRÉE(S)
ARP Poisoning

Filtrage des Paquets ARP

Événement

MATERIEL POSSIBLE
Routeur, IDS/IPS

EFFET
Détecte et bloque les paquets ARP malveillants pour prévenir les attaques par ARP Poisoning.

ATTAQUE(S) CONTRÉE(S)
ARP Poisoning

Règle de Routage Sécurisée

Événement

MATERIEL POSSIBLE
Routeur, Pare-feu

EFFET
Redirige le trafic de manière sécurisée pour empêcher les attaques de type IP Spoofing.

ATTAQUE(S) CONTRÉE(S)
IP Spoofing

Règle de Routage Sécurisée

Événement

MATERIEL POSSIBLE
Routeur, Pare-feu

EFFET
Redirige le trafic de manière sécurisée pour empêcher les attaques de type IP Spoofing.

ATTAQUE(S) CONTRÉE(S)
IP Spoofing

Règle de Routage Sécurisée

Événement

MATERIEL POSSIBLE
Routeur, Pare-feu

EFFET
Redirige le trafic de manière sécurisée pour empêcher les attaques de type IP Spoofing.

ATTAQUE(S) CONTRÉE(S)
IP Spoofing

Filtrage de Ports

Événement

MATERIEL POSSIBLE
Pare-feu, Routeur

EFFET
Ferme les ports non utilisés pour réduire la surface d'attaque et prévenir diverses attaques réseau.

ATTAQUE(S) CONTRÉE(S)
Brute Force

Filtrage de Ports

Événement

MATERIEL POSSIBLE
Pare-feu, Routeur

EFFET
Ferme les ports non utilisés pour réduire la surface d'attaque et prévenir diverses attaques réseau.

ATTAQUE(S) CONTRÉE(S)
Brute Force

Filtrage de Ports

Événement

MATERIEL POSSIBLE
Pare-feu, Routeur

EFFET
Ferme les ports non utilisés pour réduire la surface d'attaque et prévenir diverses attaques réseau.

ATTAQUE(S) CONTRÉE(S)
Brute Force

Politiques de Mot de Passe

Événement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Exige des mots de passe complexes pour empêcher les attaques par Brute Force.

ATTAQUE(S) CONTRÉE(S)
Brute Force

Politiques de Mot de Passe

Événement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Exige des mots de passe complexes pour empêcher les attaques par Brute Force.

ATTAQUE(S) CONTRÉE(S)
Brute Force

Politiques de Mot de Passe



Évènement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Exige des mots de passe complexes pour empêcher les attaques par Brut Force.

ATTACQUE(S) CONTRÉE(S)
Brute Force

Protocole VPN



Évènement

MATERIEL POSSIBLE
Routeur, Pare-feu

EFFET
Chiffre les connexions réseau pour protéger contre les attaques MITM.

ATTACQUE(S) CONTRÉE(S)
MITM

Protocole VPN



Évènement

MATERIEL POSSIBLE
Routeur, Pare-feu

EFFET
Chiffre les connexions réseau pour protéger contre les attaques MITM.

ATTACQUE(S) CONTRÉE(S)
MITM

Protocole VPN



Évènement

MATERIEL POSSIBLE
Routeur, Pare-feu

EFFET
Chiffre les connexions réseau pour protéger contre les attaques MITM.

ATTACQUE(S) CONTRÉE(S)
MITM

Liste Blanche IP



Évènement

MATERIEL POSSIBLE
Pare-feu, Routeur

EFFET
Autorise uniquement les adresses IP spécifiques, bloquant les autres pour prévenir les attaques de type IP Spoofing et DoS

ATTACQUE(S) CONTRÉE(S)
IP Spoofing
DoS

Liste Blanche IP



Évènement

MATERIEL POSSIBLE
Pare-feu, Routeur

EFFET
Autorise uniquement les adresses IP spécifiques, bloquant les autres pour prévenir les attaques de type IP Spoofing et DoS

ATTACQUE(S) CONTRÉE(S)
IP Spoofing
DoS

Liste Blanche IP



Évènement

MATERIEL POSSIBLE
Pare-feu, Routeur

EFFET
Autorise uniquement les adresses IP spécifiques, bloquant les autres pour prévenir les attaques de type IP Spoofing et DoS

ATTACQUE(S) CONTRÉE(S)
IP Spoofing
DoS

Surveillance Active des Logs



Évènement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Analyse en continu les journaux pour détecter et répondre rapidement aux activités suspectes.

ATTACQUE(S) CONTRÉE(S)
Attaque par Fragmentation IP
Attaque Phishing

Surveillance Active des Logs



Évènement

MATERIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Analyse en continu les journaux pour détecter et répondre rapidement aux activités suspectes.

ATTACQUE(S) CONTRÉE(S)
Attaque par Fragmentation IP
Attaque Phishing

Surveillance Active des Logs

Événement



ACTIVE LOG
ACTIVE LOG MONITORING

MATÉRIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Analyses en continu les journaux pour détecter et répondre rapidement aux activités suspectes.

ATTACQUE(S) CONTRÉE(S)
Attaque par Fragmentation IP
Attaque Phishing

Proxy Inverse

Événement



MATERIEL POSSIBLE
Proxy, Routeur

EFFET
Cache et protège les serveurs derrière le proxy pour empêcher les attaques directes (ex: DoS, DDoS).

ATTACQUE(S) CONTRÉE(S)
DoS
DdoS

Proxy Inverse

Événement



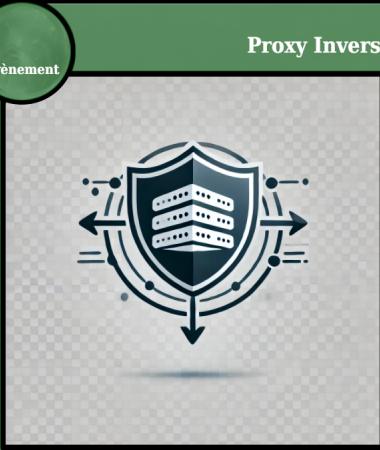
MATÉRIEL POSSIBLE
Proxy, Routeur

EFFET
Cache et protège les serveurs derrière le proxy pour empêcher les attaques directes (ex: DoS, DDoS).

ATTACQUE(S) CONTRÉE(S)
DoS
DdoS

Proxy Inverse

Événement



MATERIEL POSSIBLE
Proxy, Routeur

EFFET
Cache et protège les serveurs derrière le proxy pour empêcher les attaques directes (ex: DoS, DDoS).

ATTACQUE(S) CONTRÉE(S)
DoS
DdoS

Filtrage Web

Événement



MATERIEL POSSIBLE
Proxy

EFFET
Bloque les sites web malveillants pour prévenir les attaques par phishing et autres attaques web.

ATTACQUE(S) CONTRÉE(S)
Phishing
Atttaques web

Filtrage Web

Événement



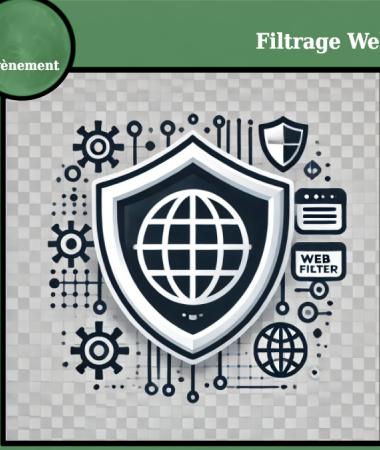
MATÉRIEL POSSIBLE
Proxy

EFFET
Bloque les sites web malveillants pour prévenir les attaques par phishing et autres attaques web.

ATTACQUE(S) CONTRÉE(S)
Phishing
Atttaques web

Filtrage Web

Événement



MATERIEL POSSIBLE
Proxy

EFFET
Bloque les sites web malveillants pour prévenir les attaques par phishing et autres attaques web.

ATTACQUE(S) CONTRÉE(S)
Phishing
Atttaques web

Chiffrement de la Base de Données

Événement



MATERIEL POSSIBLE
Serveur de base de données

EFFET
Protège les données sensibles en les chiffrant pour empêcher les accès non autorisés.

ATTACQUE(S) CONTRÉE(S)
Injection SQL

Chiffrement de la Base de Données

Événement



MATERIEL POSSIBLE
Serveur de base de données

EFFET
Protège les données sensibles en les chiffrant pour empêcher les accès non autorisés.

ATTACQUE(S) CONTRÉE(S)
Injection SQL

Chiffrement de la Base de Données

Événement



MATÉRIEL POSSIBLE

Serveur de base de données

EFFET

Protège les données sensibles en les chiffrant pour empêcher les accès non autorisés.

ATTACQUE(S) CONTRÉE(S)

Injection SQL

Limitation du Taux de Connexion

Événement



MATÉRIEL POSSIBLE

Routeur, Pare-feu

EFFET

Limite le nombre de connexions simultanées pour prévenir les attaques de type DoS et DDoS.

ATTACQUE(S) CONTRÉE(S)

DoS

DDoS

Limitation du Taux de Connexion

Événement



MATÉRIEL POSSIBLE

Routeur, Pare-feu

EFFET

Limite le nombre de connexions simultanées pour prévenir les attaques de type DoS et DDoS.

ATTACQUE(S) CONTRÉE(S)

DoS

DDoS

Limitation du Taux de Connexion

Événement



MATÉRIEL POSSIBLE

Routeur, Pare-feu

EFFET

Limite le nombre de connexions simultanées pour prévenir les attaques de type DoS et DDoS.

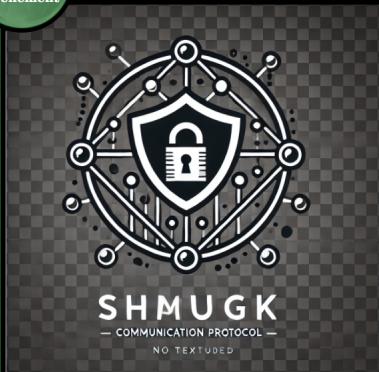
ATTACQUE(S) CONTRÉE(S)

DoS

DDoS

Protocoles sécurisés

Événement



SHMUGK

— COMMUNICATION PROTOCOL —

NO TEXTURED

MATÉRIEL POSSIBLE

Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET

Protège les protocoles de communication pour prévenir les attaques MITM et IP Spoofing.

ATTACQUE(S) CONTRÉE(S)

MITM

IP Spoofing

Protocoles sécurisés

Événement



SHMUGK

— COMMUNICATION PROTOCOL —

NO TEXTURED

MATÉRIEL POSSIBLE

Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET

Protège les protocoles de communication pour prévenir les attaques MITM et IP Spoofing.

ATTACQUE(S) CONTRÉE(S)

MITM

IP Spoofing

Protocoles sécurisés

Événement



SHMUGK

— COMMUNICATION PROTOCOL —

NO TEXTURED

MATÉRIEL POSSIBLE

Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET

Protège les protocoles de communication pour prévenir les attaques MITM et IP Spoofing.

ATTACQUE(S) CONTRÉE(S)

MITM

IP Spoofing

Limitation des Priviléges Utilisateurs

Événement



MATÉRIEL POSSIBLE

Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET

Restreint les priviléges des utilisateurs pour réduire la portée des attaques internes.

ATTACQUE(S) CONTRÉE(S)

Ransomware

Limitation des Priviléges Utilisateurs

Événement



MATÉRIEL POSSIBLE

Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET

Restreint les priviléges des utilisateurs pour réduire la portée des attaques internes.

ATTACQUE(S) CONTRÉE(S)

Ransomware

Limitation des Privileges Utilisateurs

Événement



MATERIEL POSSIBLE

Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET

Restreint les priviléges des utilisateurs pour réduire la portée des attaques internes.

ATTAQUE(S) CONTRE(E)S

Ransomware

Entrée

Modem



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Modern
Embedded OS
Firmware 1.0
N/A

Entrée

Modem



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Modern
Embedded OS
Firmware 1.0
N/A

Route réseau

Construction



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Route réseau
N/A
N/A
N/A

Construction



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Route réseau

Construction



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Route réseau
N/A
N/A
N/A

Route réseau

Construction



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Route réseau
N/A
N/A
N/A

Construction



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Route réseau

Construction



OS
VERSION OS
PROTOCOLES ACTIFS
PORTS ACTIVÉS

Route réseau
N/A
N/A
N/A

<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>

<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>

<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>

<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVES</p> <p>N/A N/A N/A N/A</p>

<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>
<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>	<p>Route réseau</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A N/A N/A</p>	