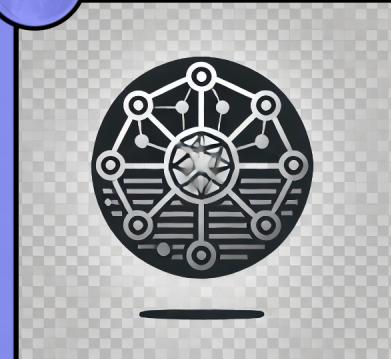
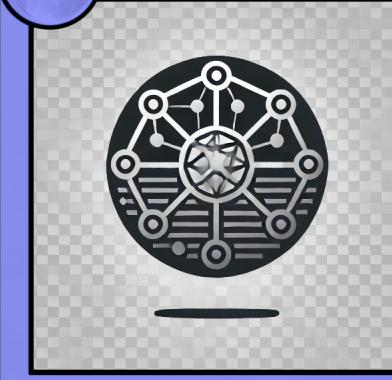
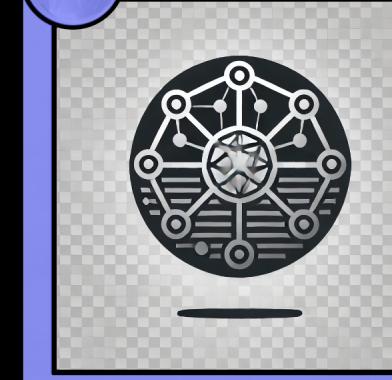
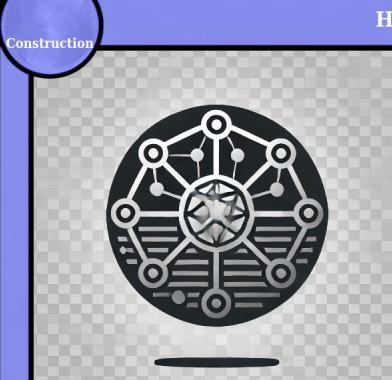
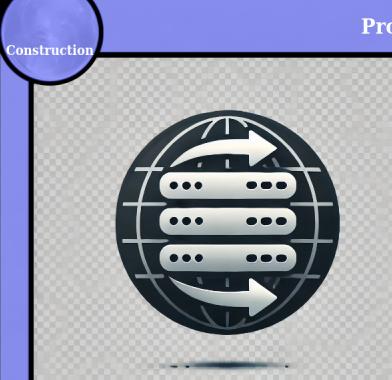
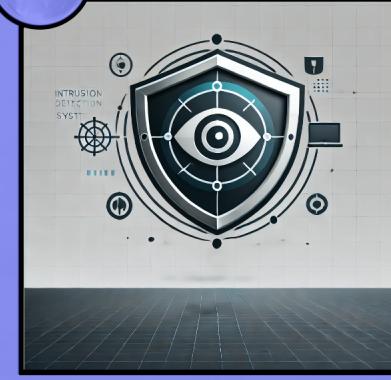
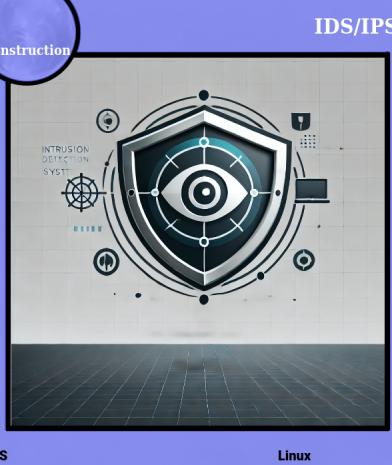
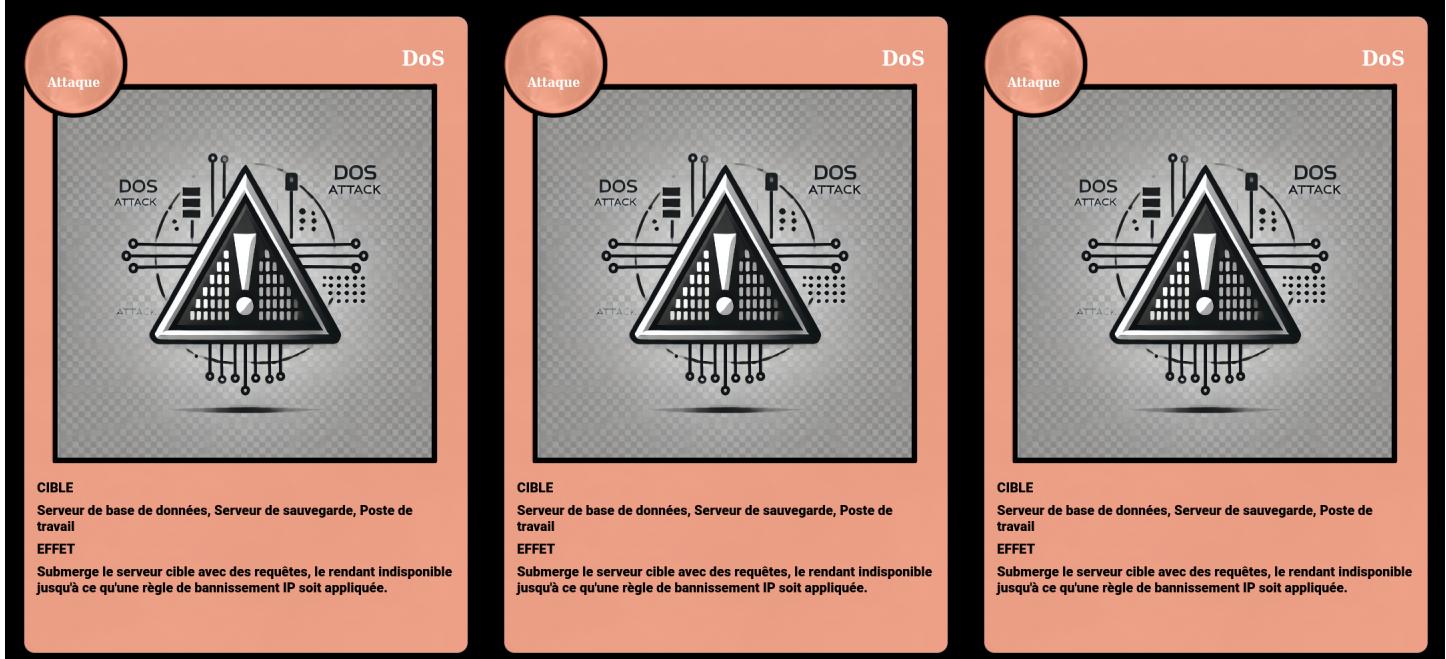
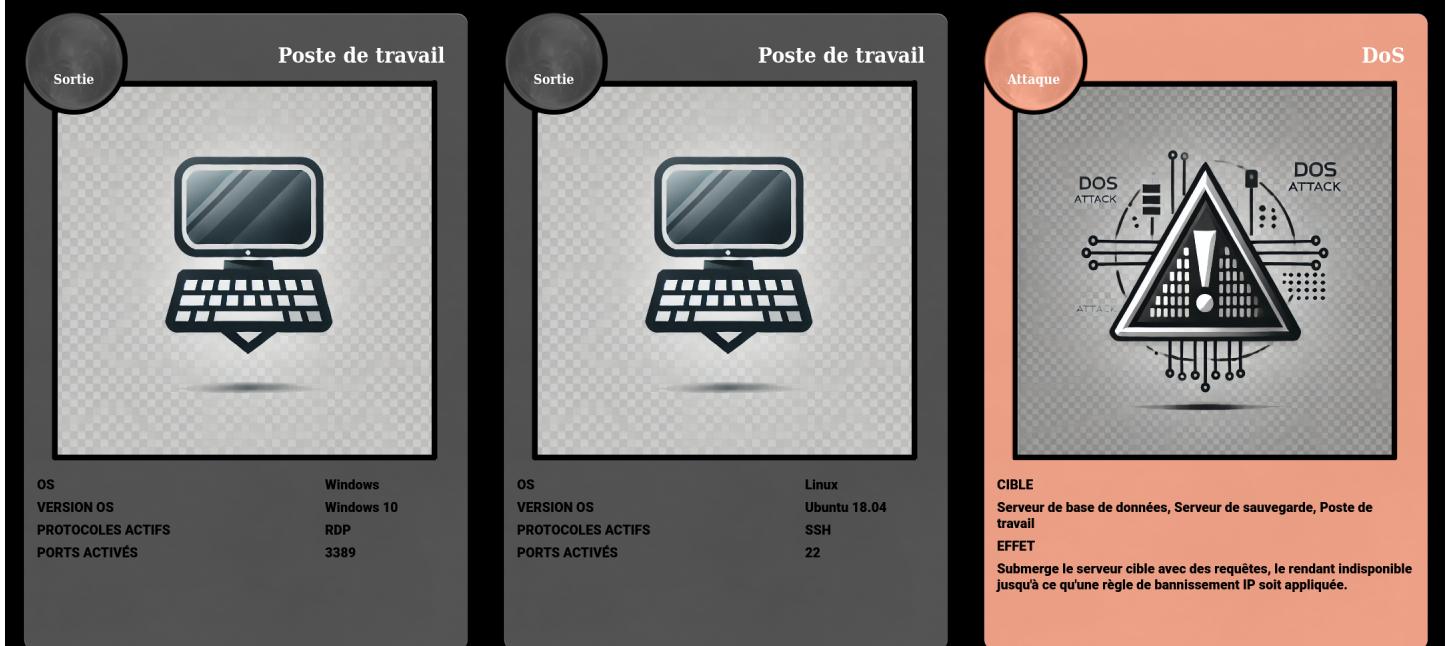


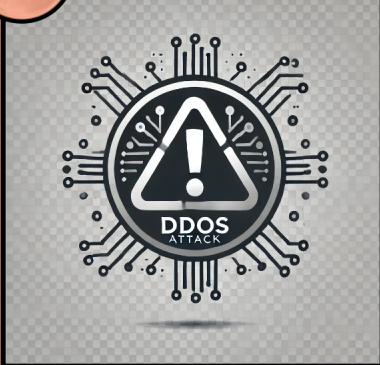
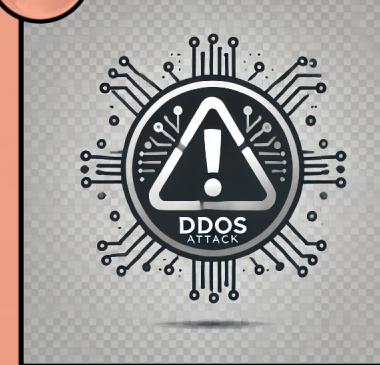
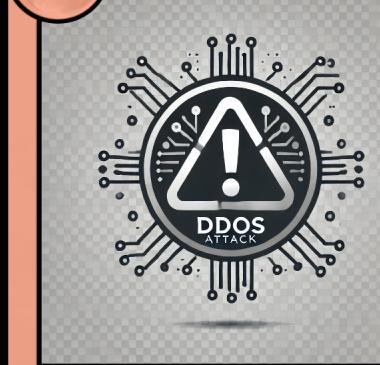
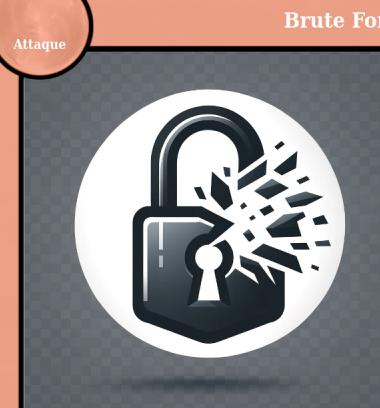
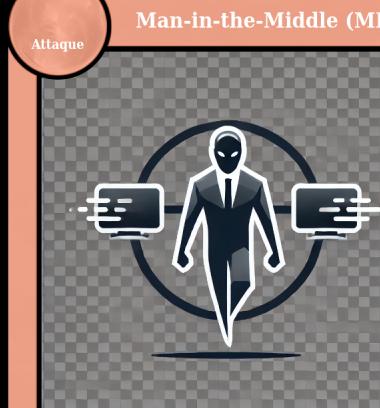
<p>Pare-feu</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux Ubuntu 20.04 IP, TCP, UDP 80, 443, 53</p>	<p>Pare-feu</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux Ubuntu 20.04 IP, TCP, UDP 80, 443, 53</p>	<p>Pare-feu</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux Ubuntu 20.04 IP, TCP, UDP 80, 443, 53</p>
<p>Pare-feu</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux CentOS 7 IP, TCP, UDP 80, 443, 21</p>	<p>Pare-feu</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux CentOS 7 IP, TCP, UDP 80, 443, 21</p>	<p>Tunnel VPN</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux CentOS 8 PPTP 1723</p>
<p>Tunnel VPN</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux CentOS 8 PPTP 1723</p>	<p>Tunnel VPN</p>  <p>Construction</p> <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>Linux CentOS 8 PPTP 1723</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>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 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 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>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 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 ACTIVÉS</p> <p>Juniper Junos Junos 18.4 IP, RIP 520, 23</p>	<p>Hub</p> <p>Construction</p>  <p>OS VERSION OS PROTOCOLES ACTIFS PORTS ACTIVÉS</p> <p>N/A N/A Ethernet 1-24</p>

<p>Construction</p>  <p>Hub</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>N/A</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>Ethernet</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>1-24</td> </tr> </tbody> </table>	OS	N/A	VERSION OS	N/A	PROTOCOLES ACTIFS	Ethernet	PORTS ACTIVÉS	1-24	<p>Construction</p>  <p>Hub</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>N/A</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>Ethernet</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>1-24</td> </tr> </tbody> </table>	OS	N/A	VERSION OS	N/A	PROTOCOLES ACTIFS	Ethernet	PORTS ACTIVÉS	1-24	<p>Construction</p>  <p>Hub</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>N/A</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>Ethernet</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>1-48</td> </tr> </tbody> </table>	OS	N/A	VERSION OS	N/A	PROTOCOLES ACTIFS	Ethernet	PORTS ACTIVÉS	1-48
OS	N/A																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	Ethernet																									
PORTS ACTIVÉS	1-24																									
OS	N/A																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	Ethernet																									
PORTS ACTIVÉS	1-24																									
OS	N/A																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	Ethernet																									
PORTS ACTIVÉS	1-48																									
<p>Construction</p>  <p>Hub</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>N/A</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>Ethernet</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>1-48</td> </tr> </tbody> </table>	OS	N/A	VERSION OS	N/A	PROTOCOLES ACTIFS	Ethernet	PORTS ACTIVÉS	1-48	<p>Construction</p>  <p>Hub</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>N/A</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>Ethernet</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>1-48</td> </tr> </tbody> </table>	OS	N/A	VERSION OS	N/A	PROTOCOLES ACTIFS	Ethernet	PORTS ACTIVÉS	1-48	<p>Construction</p>  <p>Proxy</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Linux</td> </tr> <tr> <td>VERSION OS</td> <td>Debian 10</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>HTTP, FTP</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>3128, 21</td> </tr> </tbody> </table>	OS	Linux	VERSION OS	Debian 10	PROTOCOLES ACTIFS	HTTP, FTP	PORTS ACTIVÉS	3128, 21
OS	N/A																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	Ethernet																									
PORTS ACTIVÉS	1-48																									
OS	N/A																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	Ethernet																									
PORTS ACTIVÉS	1-48																									
OS	Linux																									
VERSION OS	Debian 10																									
PROTOCOLES ACTIFS	HTTP, FTP																									
PORTS ACTIVÉS	3128, 21																									
<p>Construction</p>  <p>Proxy</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Linux</td> </tr> <tr> <td>VERSION OS</td> <td>Debian 10</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>HTTP, FTP</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>3128, 21</td> </tr> </tbody> </table>	OS	Linux	VERSION OS	Debian 10	PROTOCOLES ACTIFS	HTTP, FTP	PORTS ACTIVÉS	3128, 21	<p>Construction</p>  <p>Proxy</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Linux</td> </tr> <tr> <td>VERSION OS</td> <td>Debian 10</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>HTTP, FTP</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>3128, 21</td> </tr> </tbody> </table>	OS	Linux	VERSION OS	Debian 10	PROTOCOLES ACTIFS	HTTP, FTP	PORTS ACTIVÉS	3128, 21	<p>Construction</p>  <p>Proxy</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Windows Server</td> </tr> <tr> <td>VERSION OS</td> <td>Windows Server 2019</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>HTTP, FTP</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>8080, 21</td> </tr> </tbody> </table>	OS	Windows Server	VERSION OS	Windows Server 2019	PROTOCOLES ACTIFS	HTTP, FTP	PORTS ACTIVÉS	8080, 21
OS	Linux																									
VERSION OS	Debian 10																									
PROTOCOLES ACTIFS	HTTP, FTP																									
PORTS ACTIVÉS	3128, 21																									
OS	Linux																									
VERSION OS	Debian 10																									
PROTOCOLES ACTIFS	HTTP, FTP																									
PORTS ACTIVÉS	3128, 21																									
OS	Windows Server																									
VERSION OS	Windows Server 2019																									
PROTOCOLES ACTIFS	HTTP, FTP																									
PORTS ACTIVÉS	8080, 21																									

	Proxy	Proxy	IDS/IPS
Construction			
OS	Windows Server	Windows Server	Linux
VERSION OS	Windows Server 2019	Windows Server 2019	Red Hat 8
PROTOCOLES ACTIFS	HTTP, FTP	HTTP, FTP	IP, TCP
PORTS ACTIVÉS	8080, 21	8080, 21	80, 443
Construction			
OS	Linux	Linux	Linux
VERSION OS	Red Hat 8	Red Hat 8	OpenGSD
PROTOCOLES ACTIFS	IP, TCP	IP, TCP	IP, UDP
PORTS ACTIVÉS	80, 443	80, 443	53, 123
Construction			Serveur de base de données
OS	Linux	Linux	Linux
VERSION OS	OpenGSD	OpenGSD	Ubuntu 20.04
PROTOCOLES ACTIFS	IP, UDP	IP, UDP	MySQL
PORTS ACTIVÉS	53, 123	53, 123	3306



Attaque	DDoS	DDoS	DDoS
			
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 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.	
Attaque	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	
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.	
Attaque	Brute Force	Brute Force	Man-in-the-Middle (MITM)
			
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 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 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

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

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.

Attaque

IP Spoofing



CIBLE

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

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.

Attaque

IP Spoofing



CIBLE

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

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.

Attaque

IP Spoofing



CIBLE

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

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.

Attaque

ARP Poisoning



CIBLE

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

EFFET

Envoye 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.

Attaque

ARP Poisoning



CIBLE

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

EFFET

Envoye 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.

Attaque

ARP Poisoning



CIBLE

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

EFFET

Envoye 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.

Attaque

Phishing



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.

Attaque

Phishing



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.

Attaque

Phishing



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.

Attaque

Phishing



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.

Attaque

Ransomware



CIBLE

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

EFFET

Chiffre les données du système ciblé 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

Ransomware



CIBLE

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

EFFET

Chiffre les données du système ciblé 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

Ransomware



CIBLE

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

EFFET

Chiffre les données du système ciblé 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

Ransomware



CIBLE

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

EFFET

Chiffre les données du système ciblé 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



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.

Attaque

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.

Attaque

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.

Attaque

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.

Règle de bannissement IP

Événement



MATÉRIEL POSSIBLE
Pare-feu, Routeur

EFFET
Bloque les adresses IP spécifiques pour empêcher les attaques de type DoS et DDoS.

ATTAQUE(S) CONTRÉE(S)
DoS

Règle de bannissement IP

Événement



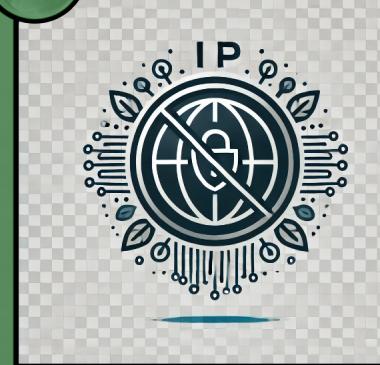
MATÉRIEL POSSIBLE
Pare-feu, Routeur

EFFET
Bloque les adresses IP spécifiques pour empêcher les attaques de type DoS et DDoS.

ATTAQUE(S) CONTRÉE(S)
DoS

Règle de bannissement IP

Événement



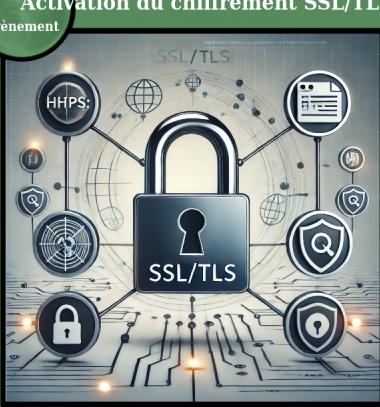
MATÉRIEL POSSIBLE
Pare-feu, Routeur

EFFET
Bloque les adresses IP spécifiques pour empêcher les attaques de type DoS et DDoS.

ATTAQUE(S) CONTRÉE(S)
DoS

Activation du chiffrement SSL/TLS

Événement



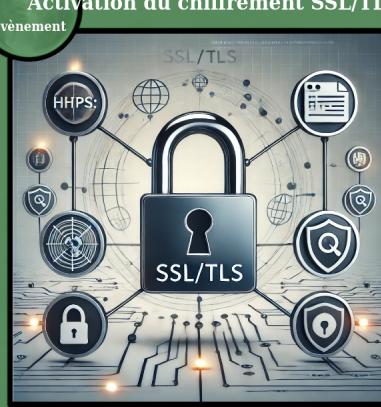
MATÉRIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Chiffre les communications pour empêcher les attaques Man-in-the-Middle (MITM).

ATTAQUE(S) CONTRÉE(S)
MITM

Activation du chiffrement SSL/TLS

Événement



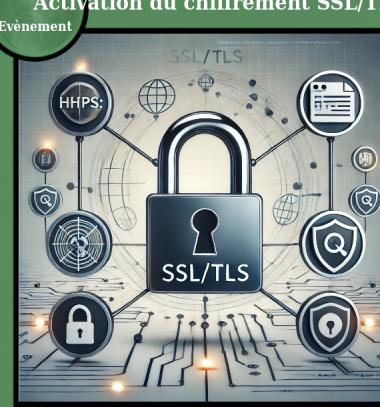
MATÉRIEL POSSIBLE
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET
Chiffre les communications pour empêcher les attaques Man-in-the-Middle (MITM).

ATTAQUE(S) CONTRÉE(S)
MITM

Activation du chiffrement SSL/TLS

Événement



MATÉRIEL 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



MATÉRIEL 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



MATÉRIEL 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



MATÉRIEL 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

Règle de routage sécurisée

Événement

MATÉRIEL 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

MATÉRIEL 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

MATÉRIEL 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

MATÉRIEL 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

MATÉRIEL 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

MATÉRIEL 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

MATÉRIEL 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)

Politiques de mot de passe

Événement

MATÉRIEL 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)

Politiques de mot de passe

Événement

MATÉRIEL 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)

Protocole VPN

Évènement



VPN
PROTOCOL



MATÉRIEL POSSIBLE
Routeur, Pare-feu
EFFET
Chiffre les connexions réseau pour protéger contre les attaques MITM.
ATTAQUE(S) CONTRÉE(S)
MITM

Protocole VPN

Évènement



VPN
PROTOCOL



MATÉRIEL POSSIBLE
Routeur, Pare-feu
EFFET
Chiffre les connexions réseau pour protéger contre les attaques MITM.
ATTAQUE(S) CONTRÉE(S)
MITM

Protocole VPN

Évènement



VPN
PROTOCOL



MATÉRIEL POSSIBLE
Routeur, Pare-feu
EFFET
Chiffre les connexions réseau pour protéger contre les attaques MITM.
ATTAQUE(S) CONTRÉE(S)
MITM

Liste blanche IP

Évènement



IP WHITELIST

MATÉRIEL POSSIBLE
Pare-feu, Routeur
EFFET
Autorise uniquement les adresses IP spécifiques, bloquant les autres pour prévenir les attaques de type IP Spoofing et DoS.
ATTAQUE(S) CONTRÉE(S)
IP Spoofing
DoS

Liste blanche IP

Évènement



IP WHITELIST

MATÉRIEL POSSIBLE
Pare-feu, Routeur
EFFET
Autorise uniquement les adresses IP spécifiques, bloquant les autres pour prévenir les attaques de type IP Spoofing et DoS.
ATTAQUE(S) CONTRÉE(S)
IP Spoofing
DoS

Liste blanche IP

Évènement



IP WHITELIST

MATÉRIEL POSSIBLE
Pare-feu, Routeur
EFFET
Autorise uniquement les adresses IP spécifiques, bloquant les autres pour prévenir les attaques de type IP Spoofing et DoS.
ATTAQUE(S) CONTRÉE(S)
IP Spoofing
DoS

Surveillance active des logs

Évènement



ACTIVE LOG
ACTIVE LOG MONITORING

MATÉRIEL 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.
ATTAQUE(S) CONTRÉE(S)
Attaque par Fragmentation IP

Surveillance active des logs

Évènement



ACTIVE LOG
ACTIVE LOG MONITORING

MATÉRIEL 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.
ATTAQUE(S) CONTRÉE(S)
Attaque par Fragmentation IP

Surveillance active des logs

Évènement



ACTIVE LOG
ACTIVE LOG MONITORING

MATÉRIEL 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.
ATTAQUE(S) CONTRÉE(S)
Attaque par Fragmentation IP

Proxy inverse

Évènement

MATÉRIEL POSSIBLE
Proxy, Routeur

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

ATTAQUE(S) CONTRÉE(S)
DoS
DdoS

Proxy inverse

Évènement

MATÉRIEL POSSIBLE
Proxy, Routeur

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

ATTAQUE(S) CONTRÉE(S)
DoS
DdoS

Proxy inverse

Évènement

MATÉRIEL POSSIBLE
Proxy, Routeur

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

ATTAQUE(S) CONTRÉE(S)
DoS
DdoS

Filtrage web

Évènement

MATÉRIEL POSSIBLE
Proxy

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

ATTAQUE(S) CONTRÉE(S)
Phishing
Atttaques web

Filtrage web

Évènement

MATÉRIEL POSSIBLE
Proxy

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

ATTAQUE(S) CONTRÉE(S)
Phishing
Atttaques web

Filtrage web

Évènement

MATÉRIEL POSSIBLE
Proxy

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

ATTAQUE(S) CONTRÉE(S)
Phishing
Atttaques web

Chiffrement de la base de données

Évènement

MATÉRIEL POSSIBLE
Serveur de base de données

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

ATTAQUE(S) CONTRÉE(S)
Injection SQL

Chiffrement de la base de données

Évènement

MATÉRIEL POSSIBLE
Serveur de base de données

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

ATTAQUE(S) CONTRÉE(S)
Injection SQL

Chiffrement de la base de données

Évènement

MATÉRIEL POSSIBLE
Serveur de base de données

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

ATTAQUE(S) CONTRÉE(S)
Injection SQL

Limitation du nombres de connexion

Évènement



MATÉRIEL POSSIBLE

Routeur, Pare-feu

EFFET

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

ATTAQUE(S) CONTRÉE(S)

DoS

DdoS

Limitation du nombres de connexion

Évènement



MATÉRIEL POSSIBLE

Routeur, Pare-feu

EFFET

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

ATTAQUE(S) CONTRÉE(S)

DoS

DdoS

Limitation du nombres de connexion

Évènement



MATÉRIEL POSSIBLE

Routeur, Pare-feu

EFFET

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

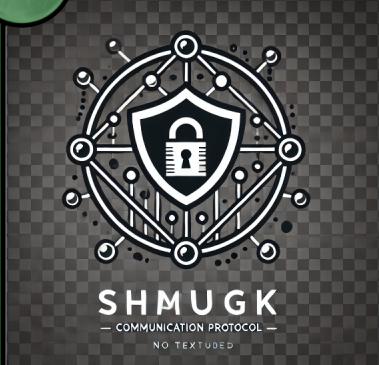
ATTAQUE(S) CONTRÉE(S)

DoS

DdoS

Protocoles sécurisés

Évènement



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.

ATTAQUE(S) CONTRÉE(S)

Protocoles sécurisés

Évènement



MATÉRIEL POSSIBLE

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

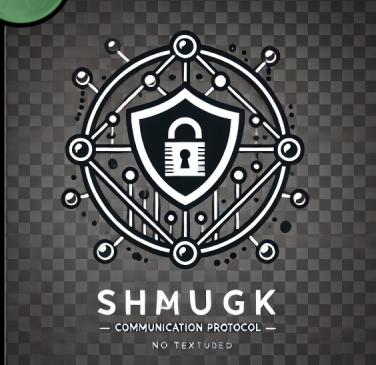
EFFET

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

ATTAQUE(S) CONTRÉE(S)

Protocoles sécurisés

Évènement



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.

ATTAQUE(S) CONTRÉE(S)

Limitation des priviléges utilisateurs

Évènement



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.

ATTAQUE(S) CONTRÉE(S)

Limitation des priviléges utilisateurs

Évènement



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.

ATTAQUE(S) CONTRÉE(S)

Limitation des priviléges utilisateurs

Évènement



MATÉRIEL POSSIBLE

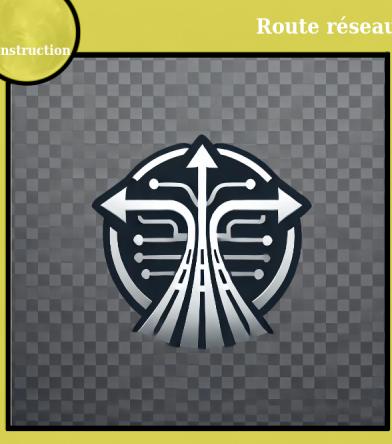
Serveur de base de données, Serveur de sauvegarde, Poste de travail

EFFET

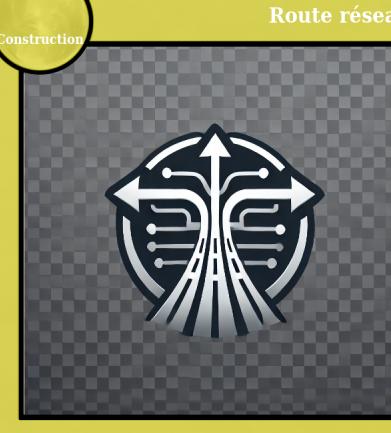
Restreint les priviléges des utilisateurs pour réduire la portée des attaques internes.

ATTAQUE(S) CONTRÉE(S)

 <p>Modem</p> <p>Entrée</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Modem</td> </tr> <tr> <td>VERSION OS</td> <td>Embedded OS</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>Firmware 1.0</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Modem	VERSION OS	Embedded OS	PROTOCOLES ACTIFS	Firmware 1.0	PORTS ACTIVÉS	N/A	 <p>Modem</p> <p>Entrée</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Modem</td> </tr> <tr> <td>VERSION OS</td> <td>Embedded OS</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>Firmware 1.0</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Modem	VERSION OS	Embedded OS	PROTOCOLES ACTIFS	Firmware 1.0	PORTS ACTIVÉS	N/A	 <p>Route réseau</p> <p>Construction</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A
OS	Modem																									
VERSION OS	Embedded OS																									
PROTOCOLES ACTIFS	Firmware 1.0																									
PORTS ACTIVÉS	N/A																									
OS	Modem																									
VERSION OS	Embedded OS																									
PROTOCOLES ACTIFS	Firmware 1.0																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
 <p>Route réseau</p> <p>Construction</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	 <p>Route réseau</p> <p>Construction</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	 <p>Route réseau</p> <p>Construction</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
 <p>Route réseau</p> <p>Construction</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	 <p>Route réseau</p> <p>Construction</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	 <p>Route réseau</p> <p>Construction</p> <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									

<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A	<p>Route réseau</p> <p>Construction</p>  <table border="1"> <tbody> <tr> <td>OS</td> <td>Route réseau</td> </tr> <tr> <td>VERSION OS</td> <td>N/A</td> </tr> <tr> <td>PROTOCOLES ACTIFS</td> <td>N/A</td> </tr> <tr> <td>PORTS ACTIVÉS</td> <td>N/A</td> </tr> </tbody> </table>	OS	Route réseau	VERSION OS	N/A	PROTOCOLES ACTIFS	N/A	PORTS ACTIVÉS	N/A
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									
OS	Route réseau																									
VERSION OS	N/A																									
PROTOCOLES ACTIFS	N/A																									
PORTS ACTIVÉS	N/A																									

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

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

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

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