Activité 1 – Attaque MITM d'un service SSH et mise en place de contre-mesures

Propriétés	Description
Intitulé long	Ce TP a pour but de simuler une attaque de l'homme du milieu sur un service SSH afin de pointer différentes vulnérabilités et de proposer des contre-mesures.
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	Bloc 3 SISR – Cybersécurité des services informatiques
Présentation	Après avoir remobilisé les savoirs fondamentaux en matière de cryptographie, ce TP permet de mettre en évidence certaines vulnérabilités du service SSH. À travers l'exploitation de ces vulnérabilités, l'étudiant sera amené à approfondir le fonctionnement de certains protocoles réseaux et de certaines attaques informatiques puis à mettre en place des contre-mesures visant à améliorer son hygiène numérique et ses pratiques professionnelles.
Compétences	Protéger les données à caractère personnel. Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques. Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service. Assurer la cybersécurité d'une solution applicative.
Savoirs	Chiffrement symétrique, asymétrique et fonction de hachage ; appliquer le principe de Kerckhoffs ; respecter l'état de l'art en matière de choix d'algorithmes cryptographiques ; authentification faible, authentification forte ; exploitation de vulnérabilité du protocole ARP ; analyse de trames.
Prérequis	Connaissances de base concernant l'administration d'un système GNU/Linux, fondamentaux en matière de cryptographie, fondamentaux réseaux (Ethernet, IP, TCP).
Outils	Kali, Serveur et client SSH, serveur DNS, routeur. Conteneurs docker (laboratoire 1 mis à disposition) https://forge.aeif.fr/btssio-labos-kali/lab1
Mots-clés	cryptographie, chiffrement, exploitation de vulnérabilités, remédiations, hygiène numérique, respect des bonnes pratiques.
Durée	6 heures
Auteur.e(s)	Quentin Demoulière avec les précieuses relectures de Valérie Emin-Martinez, David Duron et Gilles Loiseau. Laboratoire sur Docker : Apollonie Raffalli avec les tests de Christelle Thiry

Préambule

Le TP proposé est uniquement à visée pédagogique. Son objectif est l'analyse de failles liées à l'usage de certains protocoles réseaux afin de proposer une amélioration de la sécurité informatique d'un système d'information et de l'hygiène numérique des étudiants. Il permet également l'acquisition de compétences associées au bloc 3 Cybersécurité SISR du BTS SIO.

↗️ **Les outils abordés dans ce support sont uniquement utilisés à des fins éthiques (Ethical Hacking) et pédagogiques. Leur usage est formellement interdit en dehors de ce cadre sur un réseau tiers sans autorisation explicite.**

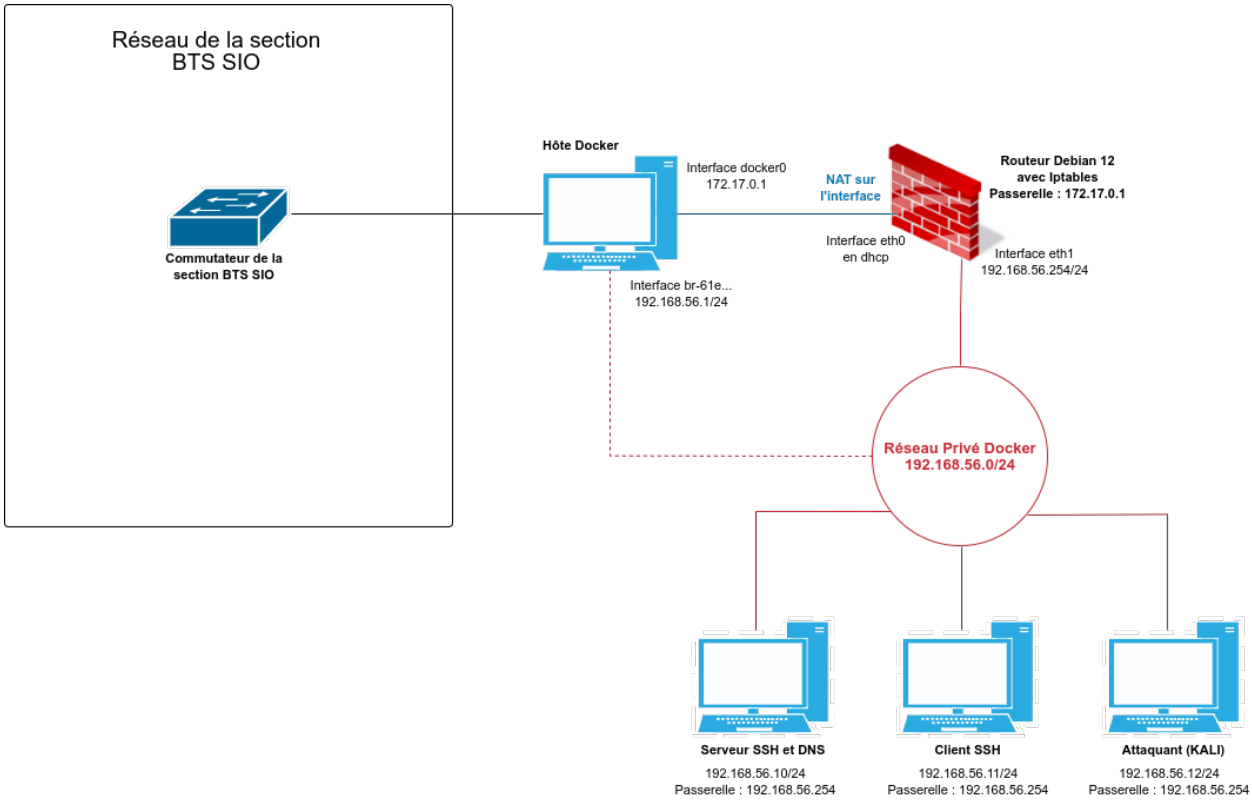
Pour rappel, l'article 323-1 du code pénal stipule que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Présentation

L**e TP qui vous est proposé utilise le « laboratoire 1 »** qui contient 4 conteneurs pré-configurées. Pour rappel :

Machine	Nom de domaine	Configuration réseau	Applications et services
Serveur sous Debian 12	srvssh.local.sio.fr	Adresse IPv4 : 192.168.56.10/24 Passerelle : 192.168.56.254 Serveur DNS : 192.168.56.10	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Client sous Debian 12	clissh.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 192.168.56.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Client OpenSSH
Attaquant sous Kali Linux	kali.local.sio.fr	Adresse IPv4 : 192.168.56.12/24 Passerelle :192.168.56.254 Serveur DNS :192.168.56.10	Environnement de bureau XFCE Service XRDP port 3389/TCP Ettercap Git ssh-mitm Netfilter/Iptables
Routeur sous Debian 12	routeur.local.sio.fr	Adresses IPv4 : eth0 – DHCP eth1 -192.168.56.254/24 Serveur DNS : 192.168.56.10	Netfilter/Iptables



Voici les comptes, les mots de passe et les numéros de ports **accessibles de l'extérieur**, vous permettant d'accéder aux différentes machines virtuelles :

Intitulé de la machine	Nom d'utilisateur	Mot de passe	Ports SSH	Port RDP
Serveur SSH sous Debian 12	etusio	Fghijkl1234*	12222	
Client SSH sous Debian 12	etusio	Fghijkl1234*	22222	23389
Attaquant sous Kali Linux 2023.3	etusio	Fghijkl1234*	32222	33389
Routeur sous Debian 12	etusio	Fghijkl1234*	42222	

Lorsque des commandes nécessitant des privilèges administrateurs seront utilisées, il sera nécessaire d'utiliser la commande **sudo**.

```
etusio@srvssh:~$ sudo service ssh restart
```

Représentation logique du réseau

↗ Lancer le laboratoire.

bash gestion_lab1.sh -c

↗ Vérifier que les 4 conteneurs sont actifs.

docker ps

```
CONTAINER ID   IMAGE                              COMMAND                  CREATED       STATUS       PORTS
                                                                                                                                                              NAMES
6c2336493ae6   reseaucerta/kalirolling:lab1       "/lib/systemd/system…"   2 hours ago   Up 2 hours   22/tcp, 3389/tcp
                                                                                                                                                              kali-lab1
54c442cd6bab   reseaucerta/clientdebian12:lab1    "/lib/systemd/system…"   2 hours ago   Up 2 hours   22/tcp, 3389/tcp
                                                                                                                                                              client-lab1
2b8b19465eac   reseaucerta/serveurdebian12:lab1   "/lib/systemd/system…"   3 hours ago   Up 3 hours   22/tcp, 53/tcp, 53/udp
                                                                                                                                                              serveur-lab1
997eb685fcc8   reseaucerta/routeurdebian12:lab1   "/lib/systemd/system…"   3 hours ago   Up 3 hours   0.0.0.0:12222->12222/tcp, :::12222->12222/tcp, 0.0.0.0:22222->22222/tcp, :::22222->22222/tcp, 0.
0.0.0:23389->23389/tcp, :::23389->23389/tcp, 0.0.0.0:32222->32222/tcp, :::32222->32222/tcp, 0.0.0.0:33389->33389/tcp, :::33389->33389/tcp, 0.0.0.0:42222->22/tcp, :::42222->22/tcp   routeur-lab1
```

Activités

Partie 1 : Attaque MITM d'un service SSH

Partie 2 : Mise en place de contre-mesures

Partie 3 : Respect des bonnes pratiques et amélioration de la sécurité du service OpenSSH sur le serveur

Sources et références ayant permis l'élaboration de ce TP

Recommandations pour un usage sécurisé d'(Open)SSH, publié par l'ANSSI le 17 août 2015

SSH, The Secure Shell : The definitive guide, de Daniel Barrett et Richard Silverman aux éditions O'Reilly, publié en février 2001

La fin annoncée des autorités de certification, alternatives : TOFU, Convergence, CATA, Clés souveraines, DANE publié en 2011 par Florian Maury, spécialiste sécurité des services et des réseaux

Les supports pédagogiques cybersécurité proposés par le label CyberÉdu.

Logiciel permettant de réaliser un SSH MITM
https://github.com/jtesta/ssh-mitm

Informations sur les différents fichiers clients et serveurs nécessaires au fonctionnement de SSH
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/4/html/reference_guide/s1-ssh-configfiles

Directives qu'il est possible d'ajouter dans le fichier de configuration du serveur SSH
https://man.openbsd.org/OpenBSD-6.0/sshd_config.5

Les bonnes pratiques à adopter pour améliorer la sécurité d'un serveur SSH
https://www.cyberciti.biz/tips/linux-unix-bsd-openssh-server-best-practices.html

La liste des algorithmes cryptographiques recommandée par l'entreprise Mozilla
https://infosec.mozilla.org/guidelines/openssh.html

Pourquoi est-il recommandé de ne plus utiliser l'algorithme RSA quand cela est possible pour générer une paire de clés SSH ?
https://blog.g3rt.nl/upgrade-your-ssh-keys.html

Définition Wikipédia de l'échange de clés Diffie-Hellman
https://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman

Guide d'utilisation de l'outil nmap
https://nmap.org/man/fr/

Définition Wikipédia de l'attaque MITM
https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu

Définition Wikipédia de l'attaque ARP Poisoning
https://fr.wikipedia.org/wiki/ARP_poisoning

Définition Wikipédia du principe de Kerckoffs
https://fr.wikipedia.org/wiki/Principe_de_Kerckhoffs

Définition Wikipédia du principe de l'entropie de Shannon
https://fr.wikipedia.org/wiki/Entropie_de_Shannon

Quelques mots sur la cryptographie, exposé au séminaire étudiant du LSP, de Djalil Chafaï, 1999
https://repo.zenk-security.com/Cryptographie%20.%20Algorithmes%20.%20Steganographie/Quelques%20mots%20sur%20la%20cryptographie.pdf

Comment augmenter l'entropie sur un serveur ?
https://www.yakati.com/art/comment-augmenter-l-entropie-sur-un-serveur-avec-havaged.html

Article expliquant le principe de la génération d'une entropie externe lors de la création de clés de chiffrement sur un ordinateur
https://www.deltasight.fr/entropie-linux-generation-nombres-aleatoires/

Définition Wikipédia du protocole SSHFP
https://fr.wikipedia.org/wiki/Enregistrement_DNS_SSHFP

Explications concernant la RFC 4255 sur le protocole SSHFP
https://www.bortzmeyer.org/4255.html

Article qui décrit la mise en œuvre de la technologie SSHFP
https://quentin.demouliere.eu/2016/03/20/sshfp-faciliter-l-authentification-d-un-serveur-ssh-depuis-un-client.html