RAPPORT DE TEST D’INTRUSION

Société : Cookfusion

SOMMAIRE :

1. Introduction

1.1 Objectifs du test d'intrusion :

Les objectifs de ce test d'intrusion étaient multiples. Premièrement, nous voulions évaluer le niveau de sécurité actuel de l'infrastructure informatique de CookFusion, y compris son réseau local et son site web. Deuxièmement, nous voulions identifier toute vulnérabilité potentiellement exploitable qui pourrait permettre à un attaquant de compromettre le système ou d'accéder à des informations sensibles. Enfin, nous voulions fournir des recommandations spécifiques pour améliorer la sécurité des systèmes de CookFusion.

1.2 Portée et limites du test :

La portée de ce test d'intrusion incluait tous les systèmes informatiques internes de CookFusion, ainsi que son site web public. Nous avons effectué des tests à la fois à partir d'un point de vue externe (c'est-à-dire en supposant le rôle d'un attaquant qui n'a pas accès au réseau de CookFusion) et à partir d'un point de vue interne (c'est-à-dire en supposant le rôle d'un utilisateur interne avec un accès de base au réseau). Les limites du test étaient définies de manière à éviter toute interruption des opérations commerciales normales. Par exemple, nous n'avons pas effectué de tests qui auraient pu causer un déni de service.

1.3 Méthodologie utilisée :

Pour ce test d'intrusion, nous avons suivi les meilleures pratiques et recommandations de plusieurs organisations de normes de sécurité reconnues, dont l'OWASP (Open Web Application Security Project) pour les tests de sécurité du site web, le CIS (Center for Internet Security) pour l'évaluation de la sécurité du réseau et du système, le NIST (National Institute of Standards and Technology) pour les recommandations de remédiation et Mitre ATT&CK pour l'analyse des tactiques, techniques et procédures que pourrait utiliser un attaquant.

2. Résumé exécutif

2.1 Aperçu des principales conclusions et recommandations :

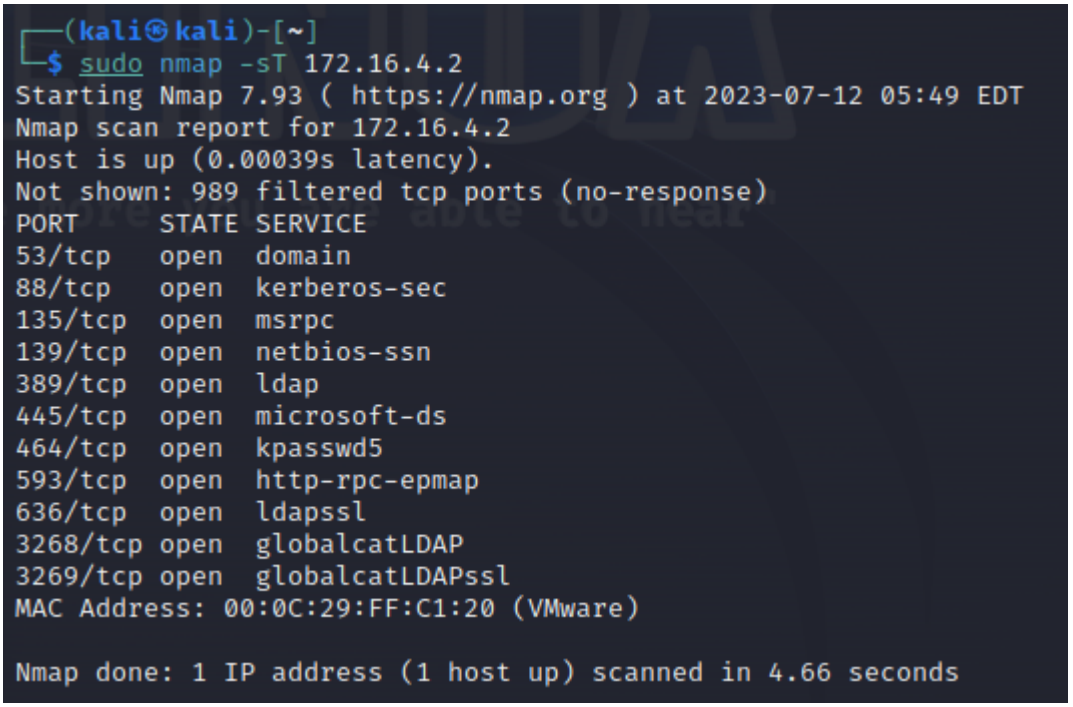
L'analyse de sécurité de l'infrastructure de CookFusion a révélé un niveau de sécurité solide, avec de nombreuses mesures de protection en place. Cependant, notre évaluation a également identifié plusieurs domaines d'amélioration potentiels.

Dans le cadre de notre test, nous avons effectué des scans de ports à l'aide de l'outil Nmap pour déterminer les services qui étaient exposés sur votre réseau. Nos scans ont révélé plusieurs ports ouverts qui pourraient potentiellement être exploités par des attaquants. Bien que les ports ouverts ne soient pas en soi une vulnérabilité, selon les services qui y sont associés, ils pourraient présenter un risque.

En outre, nous avons également effectué des tests de résistance du site web de CookFusion face à des attaques de type DoS (Denial of Service). Nos tests ont montré que, bien que le site web puisse gérer un volume de trafic élevé, des améliorations pourraient être apportées pour augmenter sa résilience à des attaques DoS plus intenses.

Les détails spécifiques de ces vulnérabilités, ainsi que nos recommandations pour y remédier, sont présentés plus loin dans ce rapport. Des captures d'écran et des preuves supplémentaires seront également fournies pour étayer nos constatations.

Voici ci dessous les différents screens mettant à l'appui les test effectué pour ce rapport :



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -p- 172.16.4.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-12 05:51 EDT
Nmap scan report for 172.16.4.2
Host is up (0.00045s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49664/tcp open  unknown
49668/tcp open  unknown
54973/tcp open  unknown
54974/tcp open  unknown
54980/tcp open  unknown
54988/tcp open  unknown
55132/tcp open  unknown
MAC Address: 00:0C:29:FF:C1:20 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 104.73 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 172.16.4.2
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-12 05:53 EDT
Nmap scan report for 172.16.4.2
Host is up (0.00046s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-07-12 09:54:01Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cookfusion.fr0., Site: De
fault-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: cookfusion.fr0., Site: De
fault-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:0C:29:FF:C1:20 (VMware)
Service Info: Host: SRVAD4; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.62 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 172.16.4.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-12 06:00 EDT
Nmap scan report for 172.16.4.2
Host is up (0.00069s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-07-12 10:00:39Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cookfusion.fr0., Site: De
fault-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: cookfusion.fr0., Site: De
fault-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:0C:29:FF:C1:20 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|10|2012|Vista (93%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_serve
r_2012:r2 cpe:/o:microsoft:windows_vista::sp1:home_premium
Aggressive OS guesses: Microsoft Windows Server 2016 (93%), Microsoft Windows 10 (89%), Microsoft Windo
ws Server 2012 or Windows Server 2012 R2 (87%), Microsoft Windows Vista Home Premium SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: SRVAD4; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
|_nbstat: NetBIOS name: SRVAD4, NetBIOS user: <unknown>, NetBIOS MAC: 000c29ffc120 (VMware)
|_clock-skew: -1s
| smb2-time:
|   date: 2023-07-12T10:00:43
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.69 ms 172.16.4.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.26 seconds
```

```
┌──(kali㉿kali)-[~/slowloris]
└─$ python slowloris.py https://cookfusion.azurewebsites.net/
[12-07-2023 07:19:10] Attacking https://cookfusion.azurewebsites.net/ with 150 sockets.
[12-07-2023 07:19:10] Creating sockets...
[12-07-2023 07:19:10] Sending keep-alive headers...
[12-07-2023 07:19:10] Socket count: 0
[12-07-2023 07:19:10] Creating 150 new sockets...
[12-07-2023 07:19:25] Sending keep-alive headers...
[12-07-2023 07:19:25] Socket count: 0
[12-07-2023 07:19:25] Creating 150 new sockets...
^CTraceback (most recent call last):
  File "/home/kali/slowloris/slowloris.py", line 231, in <module>
    main()
  File "/home/kali/slowloris/slowloris.py", line 227, in main
    time.sleep(args.sleeptime)
KeyboardInterrupt
```

3. Informations sur le système

3.1 Description du système testé :

L'évaluation de la sécurité a été menée sur l'infrastructure Active Directory (AD DS) de CookFusion. Active Directory est une technologie de Microsoft qui fournit une variété de services réseau, y compris l'authentification et l'autorisation des utilisateurs et des ordinateurs dans un réseau Windows. Le bon fonctionnement de l'AD est crucial pour la sécurité et le fonctionnement de l'infrastructure informatique de CookFusion.

3.2 Configuration du réseau :

Le réseau de CookFusion est configuré dans une plage d'adresses IP privées 172.16.4.0/25. Notre machine Kali Linux, qui a été utilisée pour effectuer le test d'intrusion, était située à l'adresse 172.16.4.20 dans le réseau local (LAN) de CookFusion. Le réseau est conçu pour isoler efficacement les différents systèmes et services, minimisant ainsi la surface d'attaque et limitant l'exposition de chaque système.

3.3 Inventaire des systèmes et des services :

Les systèmes et services pertinents dans le cadre de ce test d'intrusion comprennent l'infrastructure Active Directory de CookFusion, les serveurs associés, les postes de travail des utilisateurs, et les divers services réseau qui sont offerts aux utilisateurs internes. Un accent particulier a été mis sur l'évaluation de la sécurité de ces systèmes, étant donné leur importance pour les opérations quotidiennes de CookFusion.

4. Résultats du test d'intrusion

4.1 Résumé des vulnérabilités identifiées, triées par niveau de gravité :

Notre test d'intrusion a révélé plusieurs vulnérabilités. Ces vulnérabilités sont énumérées ci-dessous par ordre de gravité :

Utilisation de NTLMv1 : Gravité - Élevée
Absence de certificat SMB : Gravité - Moyenne
LLMNR activé : Gravité - Moyenne

4.2 Détails des vulnérabilités, y compris les descriptions, les preuves et les impacts potentiels :

Utilisation de NTLMv1 : Le protocole NTLM v1 est connu pour être vulnérable à diverses attaques, y compris les attaques de l'homme du milieu et les attaques par force brute. L'utilisation de ce protocole peut permettre à un attaquant de voler des informations d'identification et d'obtenir un accès non autorisé à des ressources réseau.

Absence de certificat SMB : L'absence de certificat SMB signifie que les communications entre les clients et le serveur ne sont pas sécurisées. Cela peut permettre à un attaquant d'intercepter et de manipuler les données transmises entre les clients et le serveur.

LLMNR activé : LLMNR est un protocole qui peut permettre à un attaquant de se faire passer pour un serveur sur le réseau. Bien que la gravité de cette vulnérabilité soit généralement considérée comme faible, il est recommandé de la désactiver pour réduire la surface d'attaque.

Vulnérabilité	Score CVSS	Sévérité	Recommendation	Status
LLMNR Activé	4.2	Moyen	désactivé LLMNR	Fixé
Pas de signature SMB	6.4	Moyen	Implémenté le certificat	Fixé
NTLMv1 activé	8.1	Élevé	Passer au NTLMv2 ou Kerberos (ANSSI)	Fixé

5. Recommandations

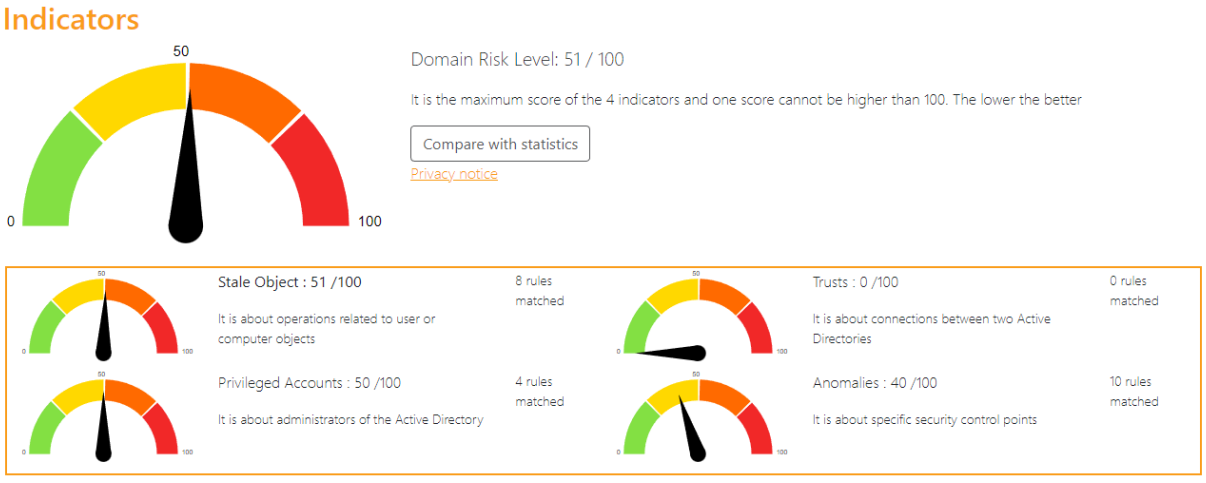
5.1 Actions spécifiques pour remédier aux vulnérabilités identifiées :

- **Utilisation de NTLMv1 :** Nous avons recommandé de désactiver NTLMv1 et de passer à NTLMv2 ou à Kerberos, qui sont des protocoles d'authentification plus sécurisés. Nous sommes heureux de constater que cette modification a été effectuée par le sysadmin et que NTLMv1 n'est plus utilisé dans l'environnement.
- **Absence de signature SMB :** Pour sécuriser les communications SMB, nous avons recommandé de mettre en place des signatures SMB. Cela permet de chiffrer les communications entre les clients et le serveur, rendant beaucoup plus difficile pour un attaquant d'intercepter ou de manipuler les données. Cette recommandation a été suivie et les signatures SMB sont maintenant en place.
- **LLMNR activé :** Nous avons recommandé la désactivation du LLMNR pour réduire la surface d'attaque et augmenter la sécurité du réseau. Cette action a été réalisée avec succès par le sysadmin.

5.2 Améliorations de la politique de sécurité et des procédures :

La réactivité de l'équipe à mettre en œuvre ces recommandations démontre un engagement fort à maintenir une politique de sécurité solide. Nous recommandons de continuer à suivre les meilleures pratiques de l'industrie en matière de sécurité, y compris la mise en place d'une politique de révision et de mise à jour régulière des protocoles de sécurité utilisés au sein de votre infrastructure.

Voici ci dessous un Audit de Ping Castle :



6. Conclusion

6.1 Récapitulation des résultats clés et des recommandations :

Notre test d'intrusion a révélé un niveau de sécurité globalement solide au sein de CookFusion. Cependant, nous avons identifié plusieurs vulnérabilités, notamment l'utilisation du protocole NTLMv1, l'absence de certificat SMB et le LLMNR activé. Nous avons recommandé des mesures pour remédier à ces vulnérabilités, et nous sommes heureux de constater que l'équipe système a réagi rapidement et a mis en œuvre ces recommandations.

6.2 Perspectives d'amélioration continue de la sécurité :

La sécurité informatique est un domaine en constante évolution, avec de nouvelles vulnérabilités et attaques qui apparaissent régulièrement. Par conséquent, il est essentiel pour CookFusion de maintenir une approche proactive et de poursuivre les efforts d'amélioration continue de la sécurité. Cela peut inclure la mise en place d'une politique de mise à jour et de révision régulière des protocoles de sécurité, ainsi que la réalisation de tests d'intrusion réguliers pour identifier et corriger les nouvelles vulnérabilités. De plus, il pourrait être bénéfique d'investir dans des formations de sécurité pour le personnel, afin de renforcer la sensibilisation à la sécurité et de réduire le risque d'erreurs humaines menant à des violations de la sécurité.