HTB Tentacle. Захватываем машину на Linux при помощи Kerberos

kafthack 23 ноя 2021 7 минут чтения 4K views 1 добавил в закладки

Сегодня я покажу, как проходить машину Tentacle с площадки Hack The Box. Для этого нам понадобится пробежаться через прокси-сервер с другого узла, а также использовать протокол шифрования Windows для получения доступа к машине на Linux и повышения привилегий на ней.

Содержание статьи

- Разведка
  - Сканирование портов
  - Перебор DNS
- Точка входа
- Закрепление
- Продвижение
  - Пользователь 1
  - Пользователь 2
- Локальное повышение привилегий

WARNING

Подготовка машины HTB рекомендуется новым перо HTB. Не делай этого с компанией, где есть важные для себя данные. Так же по возможности создай для этого отдельную сеть.

РАЗВЕДКА

Сканирование портов

Первым делом пропишем IP машины в файл /etc/hosts.

```
10.10.10.224    tentacle.htb
```

Сканируем порты скриптом в два прохода:

```
#!/bin/bash
ports=$(nmap -p- --min-rate=500 $1 | grep "^[0-9]" | cut -d '/' -f 1 | tr '\n' ',')
nmap -sC,sV,vulns -p$ports $1
```

Результат сканирования

Находим четыре открытых порта:

- порт 22 — служба SSH;
- порт 53 — служба DNS;
- порт 88 — служба Kerberos;
- порт 3128 — прокси-сервер Squid 4.11.

С SSH нам пока делать нечего, поэтому учитные данные у нас нет. С DNS и Kerberos тоже пока нечего не сделать. Однако в порту 3128, видим сообщение об ошибке, но из него получаем важные данные — домен и имя пользователя.

Ошибка, полученная при обращении к прокси-серверу

Информация доменных имен добавляем в /etc/hosts.

```
10.10.10.224    realcorp.htb
```

Перебор DNS

Больше нечего сделать на основе полезных материалов, поэтому попробуем поперебирать домены. Для этого используем dnsenum. В параметрах указываем количество потоков (-threads) и адрес сервера DNS (-dnsserver) и словарь. Берем из сборки SecLists.

```
dnsenum --threads 30 --dnsserver 10.10.10.224 -f /usr/share/seclists/Discovery/DNS
```

Результаты сканирования

Получаем несколько новых доменных имен в адресах.

ТОЧКА ВХОДА

Так как на хосте работает служба прокси-сервера и службы DNS, логично проверить, достучимся ли мы перебором до перебора адреса через этот прокси. Для этого сформируем цепочку прокси с помощью proxychains. Наши цепочки будет представлять профиль через последний хост в другом узле. Попытаемся добавить настройки для международных пакетов на внутренние сеть.

В конфигурационном файле /etc/proxychains.conf создаем три записи. Это и есть наша цепочка.

```
http    10.10.10.224 3128
socks4  127.0.0.1 9050
http    10.129.114.77 3128
```

Так как наш хостс — RFRED, есть конечно подозрение, что на нем работает одноименная служба. Попробуем достучаться до него и выполнить подсказывать пакет.

```
proxychains -q nmap -p 389,636,3268,3269
```

Результаты сканирования

Мы этот для получения для больше открытых портов, а так же и для сбора доменного веб-сервера порта 1.14.1. Также мы получаем имя хостс — wpad.realcorp.htb. Добавляем его в /etc/hosts.

```
10.129.141.51   wpad.realcorp.htb
```

Теперь на выхоль в службе настраивает на только доменное имя, но и имя хостс. Прописал в файле /etc/hosts. Теперь попробуем получить доступ к веб-серверу. Для этого в Firefox Сообщ — конфигурация прокси. Он предоставляет собой JavaScript с описанием логики, по которой браузер будет определять, как подключиться к нужному URL.

При сохранении запишется файлом выложит файлом /FindProxyForURL.pac. При файлы, передает туда URL и хост, а в результате заходит ответ, через какие прокси ходить на этот URL. Для этого нужно в конфигурации Firefox выставить «Автоматическая настройка прокси-сервера». Для Windows Server по умолчанию не поддерживается, а также отправляет HTTP-запросы на http://wpad.[domain].[zone] или на сохранит полученный файл. Значит, мы можем сами запускать файл wpad.dat с сервера.

```
proxychains -q curl wpad.realcorp.htb/wpad.dat
```

function FindProxyForURL(url, host) {
var resolved_ip = dnsResolve(host);
var myIpAddress = myIpAddress();
var dot = myIpAddress.lastIndexOf(".");
var subnet = myIpAddress.substring(0, dot);
if (resolved_ip == "10.129.141.51") {
return "PROXY 10.129.141.51:3128";
}
if (shExpMatch(host, "*.htb")) {
return "PROXY 10.10.10.224:3128";
}
if (shExpMatch(host, "*.10.10.10.*")) {
return "PROXY 10.10.10.224:3128";
}
if (shExpMatch(host, "*.10.129.*")) {
return "PROXY 10.129.114.77:3128";
}
if (shExpMatch(host, "*.127.0.0.1.nip.io")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.sslip.io")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.xip.io")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.traefik.me")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.lvh.me")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.localtest.me")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.vcap.me")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.drk.sc")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.lacolhost.com")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.iptest.io")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.ip.pm")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.ip.dnsdojo.net")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.sslip.io")) {
return "PROXY 127.0.0.1:9050";
}
if (shExpMatch(host, "*.127.0.0.1.n