专注APT攻击与防御

https://micropoor.blogspot.com/

Tunna简介：

Tunna1.1是secforce在2014年11月出品的一款基于HTTP隧道工具。其中v1.1中支持了

SOCKS4a。

Tunna演示稿：https://drive.google.com/open?id=1PpB8\_ks93isCaQMEUFf\_cNvbDsBcsWzE Github：

https://github.com/SECFORCE/Tunna

攻击机： 192.168.1.5 Debian

192.168.1.4 Windows 7

靶机： 192.168.1.119 Windows 2003

安装：

1 root@John:~# git clone https://github.com/SECFORCE/Tunna.git

2 Cloning into 'Tunna'...

3 remote: Enumerating objects: 6, done.

4 remote: Counting objects: 100% (6/6), done.

5 remote: Compressing objects: 100% (6/6), done.

6 remote: Total 156 (delta 0), reused 2 (delta 0), pack‐reused 150

7 Receiving objects: 100% (156/156), 8.93 MiB | 25.00 KiB/s, done.

8 Resolving deltas: 100% (84/84), done.

靶机执行：

以aspx为demo。

攻击机执行：

1 python proxy.py ‐u http://192.168.1.119/conn.aspx ‐l 1234 ‐r 3389 ‐s ‐ v

附录：

解决：General Exception: [Errno 104] Connection reset by peer

1 [+] Spawning keep‐alive thread

2 [‐] Keep‐alive thread not required

3 [+] Checking for proxy: False

连接后，出现

1 General Exception: [Errno 104] Connection reset by peer

等待出现：无法验证此远程计算机的身份，是否仍要连接？

再次运行，在点击是(Y)

1 python proxy.py ‐u http://192.168.1.119/conn.aspx ‐l 1234 ‐r 3389 ‐s ‐ v

如果：没有出现“无法验证此远程计算机的身份，是否仍要连接？”

注册表键值：

HKEY\_CURRENT\_USER\Software\Microsoft\Terminal Server Client\Servers删除对应IP键值即可。

非常遗憾的是，Tunna对PHP的支持并不是太友好。

Micropoor