SYNACKTIV

Compile Responder

Antoine Cervoise Rump PTS - 04/07/2023

Context

- Root access on a Linux IoT
 - No python
 - armhf7
- On the server LAN (with domain controllers)
- End of the assessment



Idea 1 - compile Python

Cross-compilation seems painful

- Basic compilation failed multiple times on a Debian armhf7
- Responder has dependencies



Idea 2 - compile Responder

Pyinstaller

- Not able to cross compile for amrhf7
- Compilation provides a dynamic binary
- Lets try on a "normal" Linux

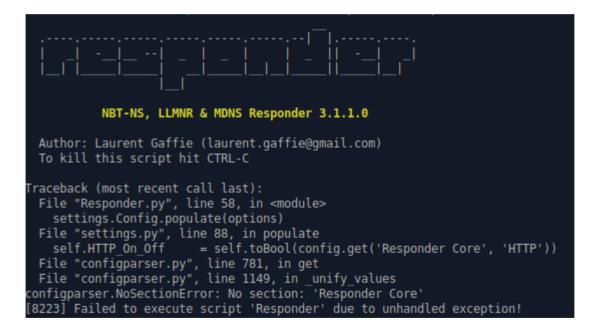
Prerequisite

apt install python3-netifaces pip install pyinstaller



Idea 2 – First attempt

\$ pyinstaller --onefile Responder.py





Idea 2 – First attempt

Error came from settings.py

config.read(os.path.join(self.ResponderPATH, 'Responder.conf'))



Idea 2 – First attempt

	certs	removed default certs	4 months ago
	files	Removed BindShell executable file	13 months ago
	logs	Added logs folder.	6 years ago
	poisoners	Added IPv6 support	4 months ago
	servers	added support for OPT EDNS	4 months ago
	tools	Added a check for MSSQL	4 months ago
۵	.gitignore	Removed logs folder.	6 years ago
۵	DumpHash.py	Added py3 and py2 compatibility + many bugfix	2 years ago
Ľ	LICENSE	Many changes, bug fixes and improvements. scripts in 'tools' still ne	7 years ago
Ľ	OSX_launcher.sh	Create OSX_launcher.sh	5 years ago
Ľ	README.md	Fixed options formating in README	2 months ago
Ľ	Report.py	Added a check for MSSQL	4 months ago
Ľ	Responder.conf	DHCP: Added auto WPADscript configuration with our IP instead of har	5 months ago
Ľ	Responder.py	Updated the README and Responder help flags	3 months ago
ß	odict.py	MutableMapping was moved to collections.abc	2 months ago
۵	packets.py	added support for OPT EDNS	4 months ago
Ľ	settings.py	Added IPv6 support	4 months ago
ß	utils.py	DE-RPC server status not correct #189	2 months ago

\$ pyinstaller --onefile Responder.py --add-data 'Responder.conf:.'

[!] Error starting SSL server on port 443, check permissions or other servers running.
[!] Error starting SSL server on port 5986, check permissions or other servers running.



	certs	removed default certs	4 months ago
	files	Removed BindShell executable file	13 months ago
	logs	Added logs folder.	6 years ago
	poisoners	Added IPv6 support	4 months ago
	servers	added support for OPT EDNS	4 months ago
	tools	Added a check for MSSQL	4 months ago
ß	.gitignore	Removed logs folder.	6 years ago
ß	DumpHash.py	Added py3 and py2 compatibility + many bugfix	2 years ago
Ľ	LICENSE	Many changes, bug fixes and improvements. scripts in 'tools' still ne	7 years ago
ß	OSX_launcher.sh	Create OSX_launcher.sh	5 years ago
ß	README.md	Fixed options formating in README	2 months ago
ß	Report.py	Added a check for MSSQL	4 months ago
Ľ	Responder.conf	DHCP: Added auto WPADscript configuration with our IP instead of har	5 months ago
ß	Responder.py	Updated the README and Responder help flags	3 months ago
ß	odict.py	MutableMapping was moved to collections.abc	2 months ago
Ľ	packets.py	added support for OPT EDNS	4 months ago
Ľ	settings.py	Added IPv6 support	4 months ago
ß	utils.py	DE-RPC server status not correct #189	2 months ago

These tips are also useful for Responder for Windows compilation ;)



Could we add ./certs to the binary?

- No sure the target has OpenSSL
- \$ bash certs/gen-self-signed-cert.sh
- \$ pyinstaller --add-data 'Responder.conf:.' -add-data 'certs:certs' --onefile Responder.py
- Be careful, the binary will always use the same CERT for all your assessments



Idea 2 – Now compile with qemu

- https://willhaley.com/blog/debian-arm-qemu/
- The binary requires a recent libC
 - Try to LD_PRELOAD the .so files
 - Issue: Responder drops *libpython3.9.so* which depends on others libs



Idea 2 – Now compile with qemu

Temporary solution: get an old ARM in your basement

 New issue: last PyInstaller vesion is not compatible with old Python 3 versions

Python 3.4 => pip install pyinstaller==3.5



SYNACKTIV



https://www.linkedin.com/company/synacktiv https://twitter.com/synacktiv Publications: https://synacktiv.com