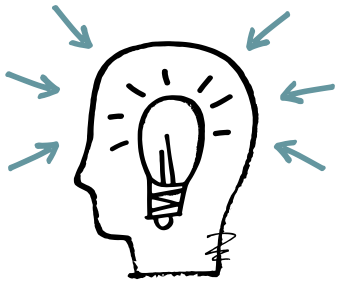
PETAQ

PURPLE TEAM C2 TOOLKIT

FATIH OZAVCI

JUNE'20

RED TEAM

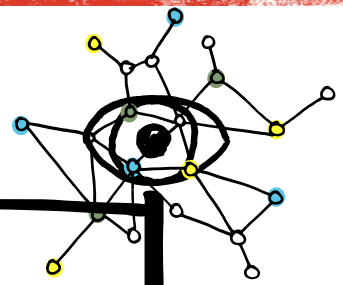


Simulating Adversaries

- Techniques
- Tactics
- Procedures

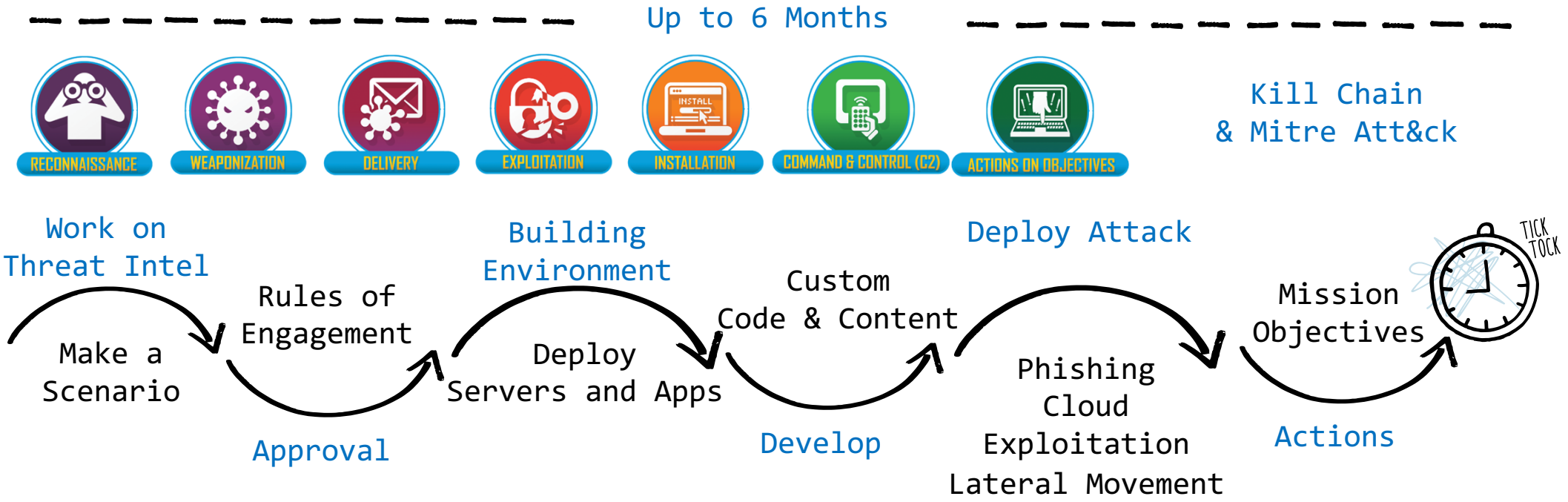
Definition: Red Teaming is the process of using tactics, techniques and procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of people, process, and technology used to defend an environment.

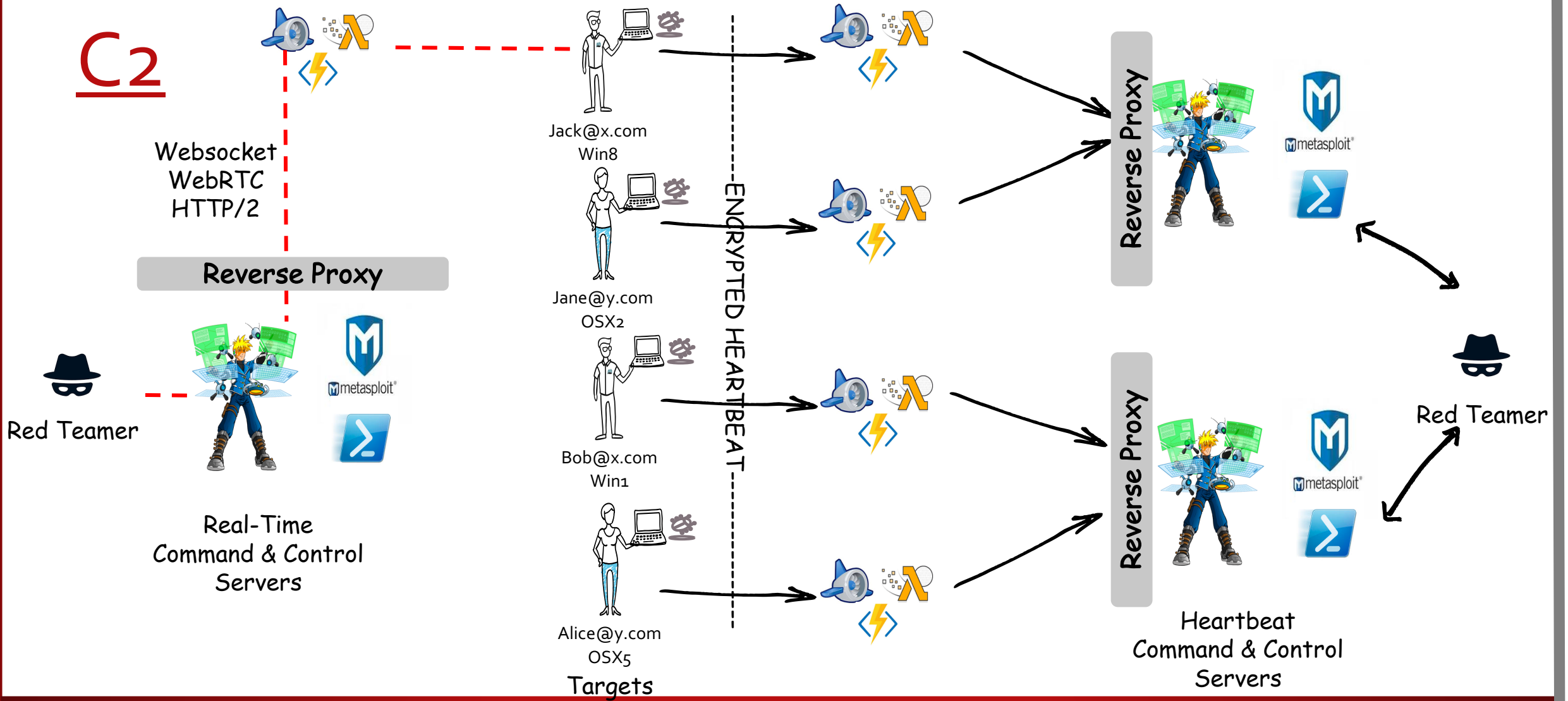
SANS



Intelligence-Led Penetration Testing

LONG RUN OF RED TEAM




C2
Websocket
WebRTC
HTTP/2
Reverse Proxy
Red Teamer
metasploit
Real-Time
Command & Control
Servers
Jack@x.com
Win8
Jane@y.com
OSX2
Bob@x.com
Win1
Alice@y.com
OSX5
Targets
ENCRYPTED HEARTBEAT
Reverse Proxy
Reverse Proxy
metasploit
metasploit
Red Teamer
Heartbeat
Command & Control
Servers

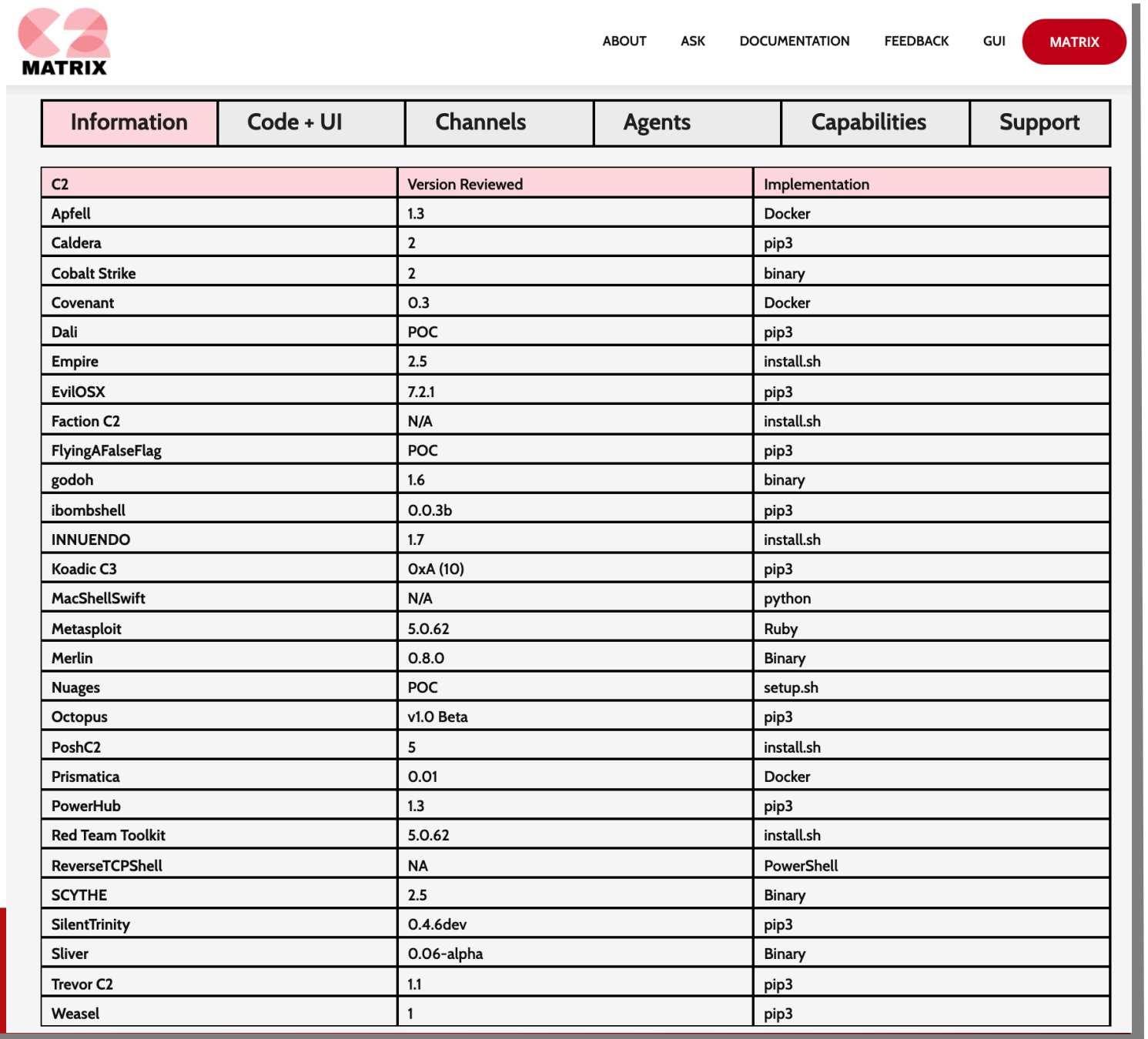
PETAQ

- P'TAKH (PETAQ) IS A KLINGON INSULT, MEANING SOMETHING LIKE "WEIRDO," DERIVING FROM THE VERB "TO BE WEIRD" (TAQ), WITH AND [SIC] YOU (PLURAL) IMPERATIVE PREFIX (PE-). ALTERNATIVE ROMANIZATIONS INCLUDE PAHTAK, P'TAK, PATAHK, AND PAHTK.

C2 MATRIX

- LOTS OF C2 ALTERNATIVES
- VARIOUS DEV LANGUAGES
- VARIOUS C2 PROTOCOLS
- VARIOUS PRODUCTION FEATURES
  - MULTI USER
  - REPORTING
  - TASK MANAGEMENT

https://www.thec2matrix.com/matrix



C2	Version Reviewed	Implementation
Apfell	1.3	Docker
Caldera	2	pip3
Cobalt Strike	2	binary
Covenant	0.3	Docker
Dali	POC	pip3
Empire	2.5	install.sh
EvilOSX	7.2.1	pip3
Faction C2	N/A	install.sh
FlyingAFalseFlag	POC	pip3
godoh	1.6	binary
ibombshell	0.0.3b	pip3
INNUENDO	1.7	install.sh
Koadic C3	0xA (10)	pip3
MacShellSwift	N/A	python
Metasploit	5.0.62	Ruby
Merlin	0.8.0	Binary
Nuages	POC	setup.sh
Octopus	v1.0 Beta	pip3
PoshC2	5	install.sh
Prismatica	0.01	Docker
PowerHub	1.3	pip3
Red Team Toolkit	5.0.62	install.sh
ReverseTCPShell	NA	PowerShell
SCYTHE	2.5	Binary
SilentTrinity	0.4.6dev	pip3
Sliver	0.06-alpha	Binary
Trevor C2	1.1	pip3
Weasel	1	pip3

MOTIVATION

- HAVING A CUSTOM C2 FOR PURPLE TEAM TRAININGS AND DEVELOPMENT WORKSHOPS
- CLEAN COMMAND & CONTROL AND IMPLANT FOR PURPLE TEAMS
  - NO TROUBLE WITH EDR/AV (UNLESS INTENTION IS TROUBLE, E.G. PROCESS INJECTION)
  - NO DETECTION ON NETWORK MONITORING AND CONTROLS
- FAST, RELIABLE AND LIGHTWEIGHT C2 (.NET FRAMEWORK & .NET CORE)
- LEVERAGING .NET AND WIN API
- EASY MALWARE DEVELOPMENT ENVIRONMENT
  - KERNEL DRIVER AND WIN API PET PROJECTS

COMMUNICATION FEATURES

- IMPLANT -> C2 CHANNELS (REAL-TIME WEBSOCKET ON HTTP/HTTPS)
- IMPLANT -> IMPLANT CHANNELS (SMB NAMED PIPES, TCP, UDP) – TESTED UP TO 8 LEVELS
- SKELETON COMMUNICATION SOCKETS FOR EASY CHANNEL EXTENSIONS
- AES ENCRYPTION ON DATA IN TRANSIT
- DEVELOPMENT
  - I->C2 CHANNELS: AWS S3, AWS DYNAMODB, AZURE BLOB, AZURE SQL, TLS/AES INTEGRATION
  - I->I CHANNELS: ACTIVE DIRECTORY, EXCHANGE EWS, TLS/AES INTEGRATION

IMPLANT CAPABILITIES

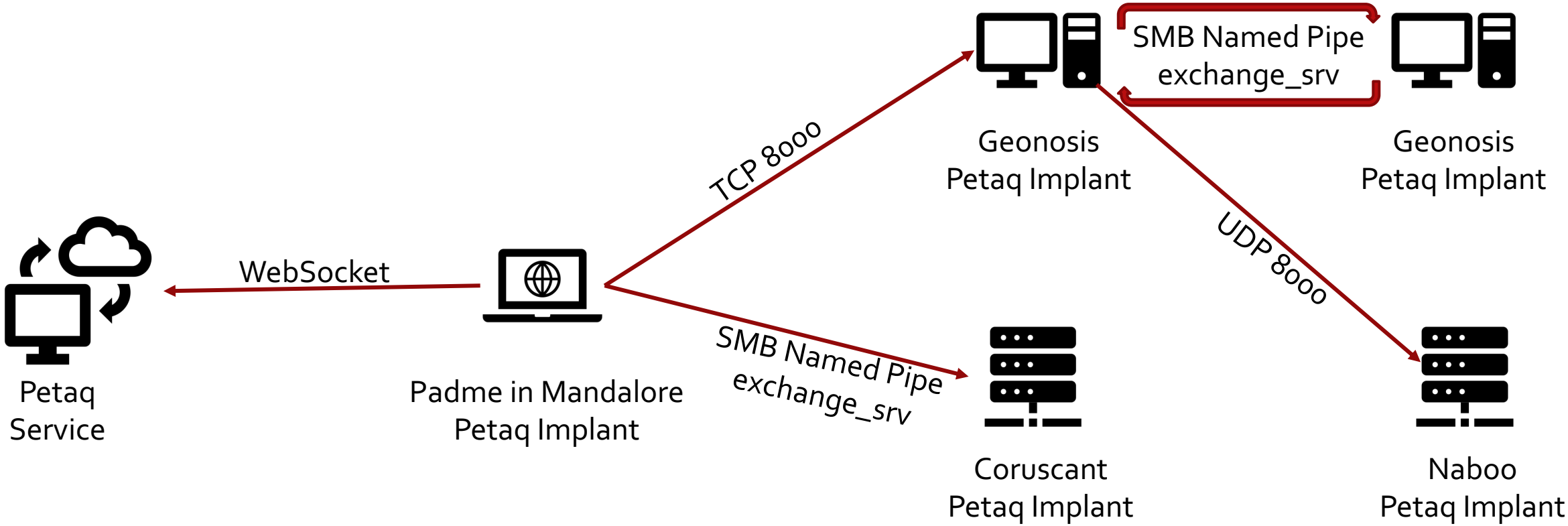
- LINKING AND CONNECTING OTHER IMPLANTS SEAMLESSLY
- START PROCESS (CMD, POWERSHELL ETC.)
- EXECUTE .NET ASSEMBLY
- COMPILE .NET C# AND RUN
- INLINE .NET C# SHELL
- EXECUTE SHELLCODE
- WMI EXEC FOR LATERAL MOVEMENT

EVASION CAPABILITIES (IN PROGRESS)

- SECURING THE TARGET SYSTEM BEFORE ACTIONS ON OBJECTIVES
  - EVADING ETW (EVENT TRACING FOR WINDOWS)
  - EDR AND AV BYPASS/UNHOOK/DISABLE
  - SAFER .NET CLR LOADING VIA UNMANAGED PROCESS INJECTION
  - EXPERIMENTING MOBIUS – .NET RUNTIME RUNNING ON .NET CORE, IRONPYTHON AND .NET SCRIPTING LANGUAGES
- PROCESS MANIPULATION
  - DEDICATED INJECTOR FOR VARIOUS INJECTIONS TO ANALYSE EDRS
  - MODULAR APPROACH (E.G. INJECTION, EVASION, PRIVILEGE ESCALATION, ACTIONS ON OBJECTIVES)
- KERNEL MODULES
  - GOING OFF-LAND, UNHOOK/DISABLE EDRS IN KERNEL, ACTIONS ON OBJECTIVES

DEMO

JUNE'20


SMB Named Pipe
exchange_srv
Geonosis
Petaq Implant
Geonosis
Petaq Implant
TCP 8000
UDP 8000
WebSocket
Petaq
Service
Padme in Mandalore
Petaq Implant
SMB Named Pipe
exchange_srv
Coruscant
Petaq Implant
Naboo
Petaq Implant

THANKS

JUNE'20