Alan

A powerful and professional Post-Exploitation Framework

https://github.com/enkomio/AlanFramework/

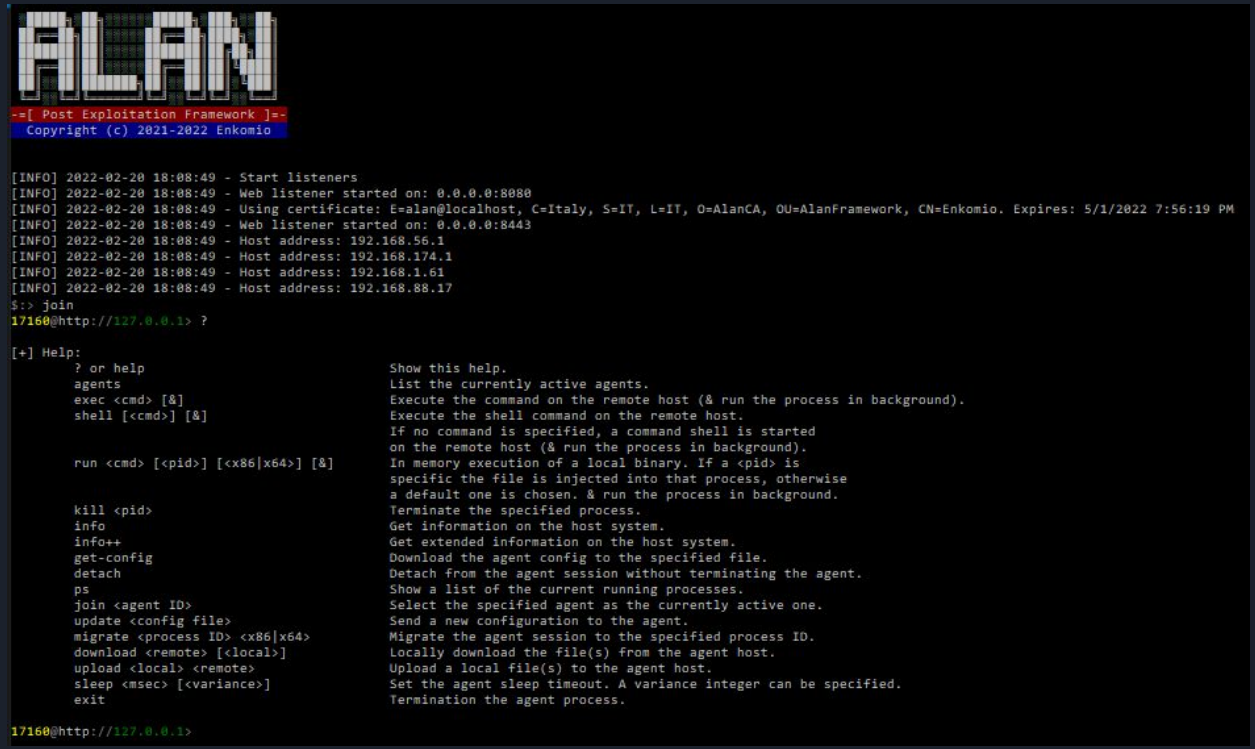
@s4tan - aparata@gmail.com

Problem Statement

Red-Team operators need a tool that:

- Allows the operator to use his/her preferred tools
- It is reliable
- It is easy to use
- It has a low system footprint
- It has a good operational security
- Can be extended in an easy way (no C/ASM development required)
- It is affordable
- Can help to simulate real-world threats to test the controls in place

Alan - Next Generation Post-Exploitation Framework



Download: https://github.com/enkomio/AlanFramework/

Alan - Features (1/2)

Currently supported features:

- Various kind of artefact formats are supported, such as: Executable, DLL, Shellcode, PowerShell (all types are provided in both x86 and x64 version).
- Execution of commands received from a Command-and-control server via HTTP/HTTPS (the certificate is automatically generated and can be customized).
- All traffic is encrypted in a strong way. A network dump or the reverse engineering of the binary is not enough to the decrypt the traffic.
- The Alan server can be executed on any OS supporting .NET core (such as Linux).
- Low network footprint and AV resistant.
- All code executed in memory (event third party programs).

Alan - Features (2/2)

Currently supported features:

- Execution of JavaScript script file to extend the Alan agent capabilities.
- The agent can be easily configure through JSON profiles.
- Fully customizable (eg. it is possible to change the used communication protocol at runtime).
- No dependency on third-party tools/software (DB, Web Server, TLS Certificate generation, …).
- Server can be customized to mimic a legitimate one.
- The operator sends command to the Alan agent by using a clean Command-line-interface.
- Fully documented.

Roadmap 2022

- SOCKS proxy (pivoting)
- Execution of PowerShell script
- New C2 channel: DNS
- Binary hardening and AV evasion
- Web UI for the Server (Only available in Alan Pro Edition)
- Additional JavaScript files to emulate a real-word adversary
- Additional commands (download from web url, agent customization, …)

Alan Early-Adopters

Who is an Alan early-adopter?

- Perform red-team activities
- Use post-exploitation tools but want more from them
- Willing to share TTPs used during the red-team activities

Alan Early-Adopters

What they receive:

- Alan agent source-code
- Early access to the new Alan version (included the Pro version when ready)
- Strict collaboration with the development team for the suggestion of new features
- “Real-time” support
- Sync-meeting (one meeting each one or two months)

Alan Early-Adopters

What they provide:

- Feedbacks
- Spread the word
- Support Alan development with a yearly contribute of 2k € equivalent in Bitcoin

Become an Alan Early-Adopter

How to become an Alan early-adopter?

1. Send an email to aparata@gmail.com specifying why you are interested in becoming an Alan early-adopter and your company name.
2. Receive the Alan binary in its latest version (this might include a release not yet published).
3. Schedule an introduction meeting.
4. Test Alan for 2 weeks.
5. Schedule a feedback meeting.
6. Become an effective Alan early-adopter by sending your contribute.
7. Receive the Alan agent source code.