Zero Trust Scan Report
On Premises EXSi Environment

Scan Date: 2025-05-12
Host: 192.168.0.148

Information

Below are the scan results from the on premises ESXi host(s) analysis. The script performs a number of check to ensure that the infrastructure aligns with the main principle of Zero Trust Architecture. The script verifies the following:

- Network Segmentation
- Encryption of VM's
- SSH and Shell Access
- Lockdown Mode Status
- ESXi Version Complaince
- VM operating System versions
- Firewall ststus
- more

Scan Overview

Resource	Check	Status	Notes
Network Segmentation	Check ESXi VLAN segmentation	Fail	Needs Review
Services Status	SSH & Shell services status	Fail	Needs Review
Lockdown Mode	Host lockdown status	Pass	OK
VM Encryption	VMs encryption check	Fail	Needs Review
ESXi Version	Check ESXi version against latest	Pass	OK
VM OS Info	Unsupported OS versions detection	Pass	OK
ESXi Permissions	Unauthorized full rights check	Pass	OK
Firewall Status	Firewall enabled check	Pass	OK
Log Forwarding	Verify Syslog forwarding	Pass	OK
Check SSH Access Restrictions	Checks if specified users are added to ssh config file to ensure least privilege access	Pass	OK
VM Snapshot Availability	Checks if VM's have snapshots	Pass	OK
SSH Root Login	PermitRootLogin check	Pass	OK
ESXI Host Password Complexity Policy	Checks if password complexity polices are set on host.	Pass	OK
ESXI Host Password Expiration Policy	Checks password expiration policy.	Pass	OK

Complaince Percent = 63.0 / 110

Detailed Information

Network Segmentation - Fail

Check: Check ESXi VLAN segmentation

Result: Fail - Needs Review

Details:

Port Group	VLAN ID
Isolation Network	70
VM Network	10
File Services	0
ESXi Management	0
Domain Services	0
Management Network	0
Monitoring Services	0

Services Status - Fail

Check: SSH & Shell services status

Result: Fail - Needs Review

Details:

Service	Status
DCUI	True
TSM	True
TSM-SSH	True
attestd	False
dpd	False
kmxd	False
lbtd	True
lwsmd	True
ntpd	False
pcscd	False
ptpd	False
sfcbd-watchdog	False
slpd	False
snmpd	False
vltd	False
vmsyslogd	True
vpxa	True
xorg	False

Lockdown Mode - Pass

Check: Host lockdown status

Result: Pass - OK

Details:

Lockdown Mode	lockdownNormal

VM Encryption - Fail

Check: VMs encryption check

Result: Fail - Needs Review

Details:

VM Name	Encryption Status
Domain Controller 1	False
Ubuntu-Log-Server	False
Wazuh-Siem	False
win-fileserver01	False
VMware vCenter Server	False

ESXi Version - Pass

Check: Check ESXi version against latest

Result: Pass - OK

Details:

ESXi Host Build Number	24585291
Latest ESXI Build	24585291

VM OS Info - Pass

Check: Unsupported OS versions detection

Result: Pass - OK

Details:

Operating System	Supported Status
Microsoft Windows Server 2019 (64-bit)	Supported
Ubuntu Linux (64-bit)	Supported
Other Linux (64-bit)	Supported
Other 3.x or later Linux (64-bit)	Supported

ESXi Permissions - Pass

Check: Unauthorized full rights check

Result: Pass - OK

Details:

User	Access Level

AliceJohnson	Full access rights
dcui	Full access rights
vpxuser	Full access rights

Firewall Status - Pass

Check: Firewall enabled check

Result: Pass - OK

Details:

Firewall Status	Enabled

Log Forwarding - Pass

Check: Verify Syslog forwarding

Result: Pass - OK

Details:

Syslog Forwarding	True
Log Server IP	udp://192.168.0.117:514

Check SSH Access Restrictions - Pass

Check: Checks if specified users are added to ssh config file to ensure least privilege access

Result: Pass - OK

Details:

Username	SSH Status
AliceJohnson	Allowed

VM Snapshot Availability - Pass

Check: Checks if VM's have snapshots

Result: Pass - OK

Details:

VM Name	Snapshot Name
Domain	Snapshots Found
Ubuntu-Log-Server	Snapshots Found
Wazuh-Siem	Snapshots Found
win-fileserver01	Snapshots Found
VMware	Snapshots Found

SSH Root Login - Pass

Check: PermitRootLogin check

Result: Pass - OK

Details:

SSH Root Login	Disabled

ESXI Host Password Complexity Policy - Pass

Check: Checks if password complexity polices are set on host.

Result: Pass - OK

Details:

Password Complexity Status	Required Password Length
True	12

ESXI Host Password Expiration Policy - Pass

Check: Checks password expiration policy.

Result: Pass - OK

Details:

Username	Password Expires after x days
root	60
dcui	60
vpxuser	60
ciaran	60
ExploitedUser	60
AliceJohnson	60
BrandonFoster	60
CharlieDavis	60
CindyMorris	60
DanielleMorris	60
FionaMartin	60
IanThompson	60
OscarRamirez	60
PatriciaScott	60
QuintinBrooks	60
StephenHarris	60
TinaEdwards	60

Recommendations

Some areas passed, some could use a bit of fixing. Keeping things locked down is an ongoing thing, so regular checks are a good idea

Azure Security Report

Scan Date: 2025-05-12
Azure Subscription: 38915259-0faa-4784-a49a-5b4fcd1ef2b6

Information

This is a basic scan to check if some important Zero Trust rules are being followed. Stuff like network rules, user permissions, and encryption were looked at.

Scan Overview

Resource	Check	Status	Notes
Network Segmentation	Check if VNets are segmented	Pass	OK
NSG Rules	Check for overly permissive NSG rules	Pass	OK
Public IP Exposure	Check for public IPs assigned to resources	Pass	OK
Azure Bastion	Check if Azure Bastion is deployed for secure access	Fail	Needs Review
VNet Encryption	Check if VNets and peerings have encryption enabled	Pass	OK
VM Inbound NSG Rules	Chekcs if VM's have service ports open for all inbound IP addresses	Fail	Needs Review
VM Encryption	Check if VMs have encryption at host enabled	Pass	OK
Key Vault Security	Check Key Vault RBAC, Soft Delete, and Purge Protection	Pass	OK
Azure Firewall	Check if Azure Firewall is deployed for perimeter security	Fail	Needs Review
Azure Snapshots	Checks if snapshots are taken of VM's	Fail	Needs Review
Azure Backups	Checks if Azure backups are configured for VM's	Fail	Needs Review
Subsctiption Owners	Checks the number of owners on the subscription, Microsoft reccomends less than 3	Pass	OK
Group Membership	Check if users belong to too many groups	Pass	OK

Azure Complaince Percent = 80.0 / 100

Extra Details

Network Segmentation - Pass

Check: Check if VNets are segmented

Result: Pass - OK

Details:

Name	Address
HubVnet	['10.0.0.0/24']
GatewaySubnet	['10.0.0.0/27']
AzureFirewallManagementSubnet	['10.0.0.64/26']

AzureBastionSubnet	['10.0.0.128/26']
Production-VNET	['10.4.0.0/16']
default	['10.5.0.0/24']
Isolation-Subnet	['10.5.1.0/29']
Testing-VNET	['10.5.0.0/16']

NSG Rules - Pass

Check: Check for overly permissive NSG rules

Result: Pass - OK

Details:

NSG Name	Rule/Destination
nsg-hub-uaen-001	{'access': 'Allow', 'destinationAddressPrefix': '*', 'destinationAddressPrefixes': [], 'destinationPortRange': '*', 'destinationPortRanges': [], 'direction': 'Inbound', 'etag': 'W/"e1308dbb-4147-449e-88ec-afcf5a05af36"', 'id': '/subscriptions/38915259-0faa-4784-a49a-5b4fcd1ef2b6/resourceGroups/HubSpoke-RG/providers/Microsoft.Network/networkSecurityGroups/nsg-hub-uaen-001/securityRules/AllowAnyCustomAnyInbound', 'name': 'AllowAnyCustomAnyInbound', 'priority': 141, 'protocol': 'ICMP', 'provisioningState': 'Succeeded', 'resourceGroup': 'HubSpoke-RG', 'sourceAddressPrefix': '*', 'sourceAddressPrefixes': [], 'sourcePortRange': '*', 'sourcePortRanges': [], 'type': 'Microsoft.Network/networkSecurityGroups/securityRules'}
nsg-spoke-uaen-001	{'access': 'Allow', 'destinationAddressPrefix': '*', 'destinationAddressPrefixes': [], 'destinationPortRange': '*', 'destinationPortRanges': [], 'direction': 'Outbound', 'etag': 'W/"6a139743-70b5-460e-a695-b96b776963a0"', 'id': '/subscriptions/38915259-0faa-4784-a49a-5b4fcd1ef2b6/resourceGroups/HubSpoke-RG/providers/Microsoft.Network/networkSecurityGroups/nsg-spoke-uaen-001/securityRules/AllowAnyCustomAnyOutbound', 'name': 'AllowAnyCustomAnyOutbound', 'priority': 110, 'protocol': 'ICMP', 'provisioningState': 'Succeeded', 'resourceGroup': 'HubSpoke-RG', 'sourceAddressPrefix': '*', 'sourceAddressPrefixes': [], 'sourcePortRange': '*', 'sourcePortRanges': [], 'type': 'Microsoft.Network/networkSecurityGroups/securityRules'}
azure-production-server02-nsg	{'access': 'Allow', 'destinationAddressPrefix': '*', 'destinationAddressPrefixes': [], 'destinationPortRange': '3389', 'destinationPortRanges': [], 'direction': 'Inbound', 'etag': 'W/"79811ae7-1cf2-432d-8573-14409e1df902"', 'id': '/subscriptions/38915259-0faa-4784-a49a-5b4fcd1ef2b6/resourceGroups/RG-Prod-Vms/providers/Microsoft.Network/networkSecurityGroups/azure-production-server02-nsg/securityRules/RDP', 'name': 'RDP', 'priority': 300, 'protocol': 'TCP', 'provisioningState': 'Succeeded', 'resourceGroup': 'RG-Prod-Vms', 'sourceAddressPrefix': '*', 'sourceAddressPrefixes': [], 'sourcePortRange': '*', 'sourcePortRanges': [], 'type': 'Microsoft.Network/networkSecurityGroups/securityRules'}
Isolation-NSG	{'access': 'Deny', 'destinationAddressPrefix': '*', 'destinationAddressPrefixes': [], 'destinationPortRange': '*', 'destinationPortRanges': [], 'direction': 'Outbound', 'etag': 'W/"b79e27d0-43de-446d-bb80-c3f891275fc8"', 'id': '/subscriptions/38915259-0faa-4784-a49a-5b4fcd1ef2b6/resourceGroups/RG-Prod-Vms/providers/Microsoft.Network/networkSecurityGroups/Isolation-NSG/securityRules/Deny-All-Outbound', 'name': 'Deny-All-Outbound', 'priority': 100, 'protocol': '*', 'provisioningState': 'Succeeded', 'resourceGroup': 'RG-Prod-Vms', 'sourceAddressPrefix': '*', 'sourceAddressPrefixes': [], 'sourcePortRange': '*', 'sourcePortRanges': [], 'type': 'Microsoft.Network/networkSecurityGroups/securityRules'}
azure-testing-kali01-nsg	{'access': 'Allow', 'destinationAddressPrefix': '*', 'destinationAddressPrefixes': [], 'destinationPortRange': '22', 'destinationPortRanges': [], 'direction': 'Inbound', 'etag': 'W/"df70adfc-5b44-47bc-be81-6cca89d6ee95"', 'id': '/subscriptions/38915259-0faa-4784-a49a-5b4fcd1ef2b6/resourceGroups/RG-test-vms/providers/Microsoft.Network/networkSecurityGroups/azure-testing-kali01-nsg/securityRules/SSH', 'name': 'SSH', 'priority': 300, 'protocol': 'TCP', 'provisioningState': 'Succeeded', 'resourceGroup': 'RG-test-vms', 'sourceAddressPrefix': '*', 'sourceAddressPrefixes': [], 'sourcePortRange': '*', 'sourcePortRanges': [], 'type': 'Microsoft.Network/networkSecurityGroups/securityRules'}

Public IP Exposure - Pass

Check: Check for public IPs assigned to resources

Result: Pass - OK

Details:

Resource Name:	IP address / Resource Group

Gub-gateway-publicip	74.243.247.177 : HubSpoke-RG
HubVnet-ip	20.233.231.247 : HubSpoke-RG

Azure Bastion - Fail

Check: Check if Azure Bastion is deployed for secure access

Result: Fail - Needs Review

Details:

Bastion Name	Location

VNet Encryption - Pass

Check: Check if VNets and peerings have encryption enabled

Result: Pass - OK

Details:

VNET Resource	Encryption Status
HubVnet	Enabled
hub-topro	Enabled
hub-to-test	Enabled
Production-VNET	Enabled
hub-to-prod	Enabled
Testing-VNET	Enabled
hub-totest	Enabled

VM Inbound NSG Rules - Fail

Check: Chekcs if VM's have service ports open for all inbound IP addresses

Result: Fail - Needs Review

Details:

VM Name / NSG	Open Port / Source
azure-production-server02 / azure-production-server02-nsg	allows inbound from * / on port 3389
azure-testing-kali01 / azure-testing-kali01-nsg	allows inbound from * / on port 22

VM Encryption - Pass

Check: Check if VMs have encryption at host enabled

Result: Pass - OK

Details:

RG-PROD-VMS/azure-production-server02	Encrypted
RG-TEST-VMS/azure-testing-kali01	Encrypted

Key Vault Security - Pass

Check: Check Key Vault RBAC, Soft Delete, and Purge Protection

Result: Pass - OK

Details:

Vault name	Key-Vault-VMs-Zero-Trust
RBAC Status	True
Soft Delete name	True
Purge Proetction	True

Azure Firewall - Fail

Check: Check if Azure Firewall is deployed for perimeter security

Result: Fail - Needs Review

Details:

Name	Location

Azure Snapshots - Fail

Check: Checks if snapshots are taken of VM's

Result: Fail - Needs Review

Details:

VM Name/Resource Group	Snapshot Ststus / Name
azure-production-server02 : RG-PROD-VMS	False :None
azure-testing-kali01 : RG-TEST-VMS	False :None

Azure Backups - Fail

Check: Checks if Azure backups are configured for VM's

Result: Fail - Needs Review

Details:

VM Name / Resource Group	Backup Vault Name
azure-production-server02 / RG-PROD-VMS	No Backups Configured
azure-testing-kali01 / RG-TEST-VMS	No Backups Configured

Subsctiption Owners - Pass

Check: Checks the number of owners on the subscription, Microsoft reccomends less than 3

Result: Pass - OK

Details:

Username	Admin Role
obrienciaran4_gmail.com#EXT#@obrienciaran4gmail.onmicrosoft.com	Owner

ajohnson@obrienciaran4gmail.onmicrosoft.com	Owner

Group Membership - Pass

Check: Check if users belong to too many groups

Result: Pass - OK

Details:

Username	Group Memberships
Alice Johnson	['ZTA_IT_Admins']
Bob Smith	['ZTA_Azure_Admins']
Charlie Davis	['ZTA_RemoteDesktopUsers', 'ZTA_Network_Team']
Danielle Williams	['ZTA_ESXi_Admins']
Edward Brown	['ZTA_Security_Team']
Fiona Martin	['ZTA_Systems_Team']
George Lee	['ZTA_DevOps_Team']
Kevin Martinez	['ZTA_App_Developers']

Recommendations

Some areas passed, some could use a bit of fixing. Keeping things locked down is an ongoing thing, so regular checks are a good idea!