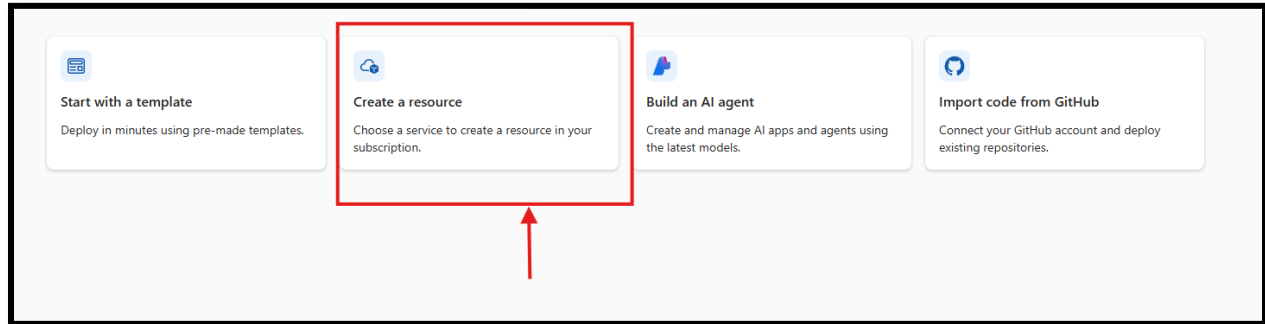


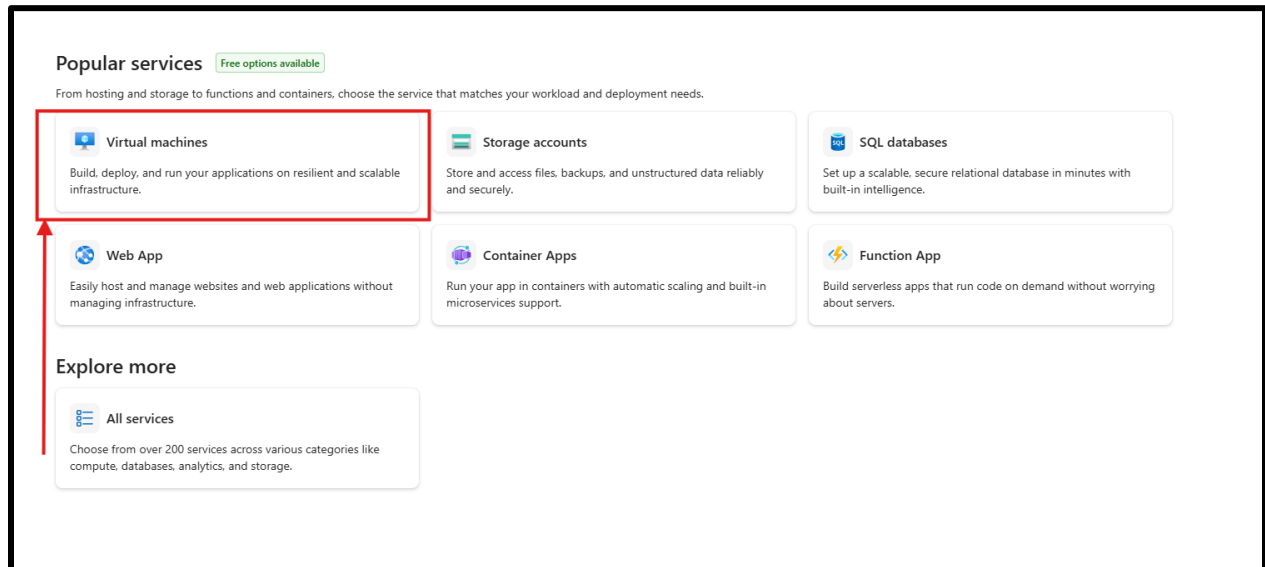
## Appendix A

### Creation and Deployment of Azure Virtual Machine with T-Pot

**Figure A-1. Select Create Resource in Microsoft Azure**



**Figure A-2. Select Create Virtual Machine**



**Figure A-3. Configure subscription, resource group, VM name, region, and Debian 12 x64 image**

## Create a virtual machine

[Help me create a low cost VM](#)[Help me create a VM optimized for high availability](#)[Help me choose the right VM size for my workload](#)

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Azure subscription 1

Resource group \* ⓘ

(New) Honey

[Create new](#)

### Instance details

Virtual machine name \* ⓘ

CapstoneHoney

Region \* ⓘ

(US) West US 3

[Deploy to an Azure Extended Zone](#)

Availability options ⓘ

Availability zone

Zone options ⓘ

☒ Self-selected zone

Choose up to 3 availability zones, one VM per zone

☐ Azure-selected zone (Preview)

Let Azure assign the best zone for your needs

Availability zone \* ⓘ

Zone 1

☒ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ

Trusted launch virtual machines

[Configure security features](#)

Image \* ⓘ

Debian 12 "Bookworm" - x64 Gen2 (free services eligible)

[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ

☐ Arm64

☒ x64

< Previous

Next : Disks >

Review + create

**Figure A-4. Set OS disk size to 128 GiB**

Basics

**Disks**

Networking

Management

Monitoring

Advanced

Tags

Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

**i** There is a charge for the underlying storage resources consumed by your virtual machine. [Learn more](#)

### VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ☐

**i** Encryption at host is not registered for the selected subscription. [Learn more](#)

### OS disk

OS disk size

**i** Some images are, by default, smaller than the selected OS disk size. [Click here to learn how to expand your disk partition size after you create your VM.](#)

OS disk type \*

Delete with VM ☒

Key management

Enable Ultra Disk compatibility ☐

### Data disks for CapstoneHoney

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

< Previous

Next : Networking >

Review + create

**Figure A-5. Ensure Auto-shutdown is unchecked**

Basics

Disks

Networking

Management

Monitoring

Advanced

Tags

Review + create

Configure management options for your VM.

### Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

Enable basic plan for free ⓘ ☒ This will apply to every VM in the selected subscription

### Identity

Enable system assigned managed identity ⓘ ☐

### Microsoft Entra ID

Login with Microsoft Entra ID ⓘ ☐ RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Microsoft Entra ID login. [Learn more](#)

⚠ This image does not support Login with Microsoft Entra ID.

ⓘ Microsoft Entra ID login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH certificates. You can use Azure CLI or Cloud Shell from the Azure Portal. [Learn more](#)

### Auto-shutdown

Enable auto-shutdown ⓘ ☐

### Guest OS updates

Enable periodic assessment ⓘ ☐

< Previous

Next : Monitoring >

Review + create

**Figure A-6. Review and create virtual machine**

Basics Disks Networking Management Monitoring Advanced Tags **Review + create**

**Price**

1 X Standard D2s v3  
by Microsoft  
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ  
**0.0960 USD/hr**  
[Pricing for other VM sizes](#)

**TERMS**

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Preferred e-mail address

Preferred phone number

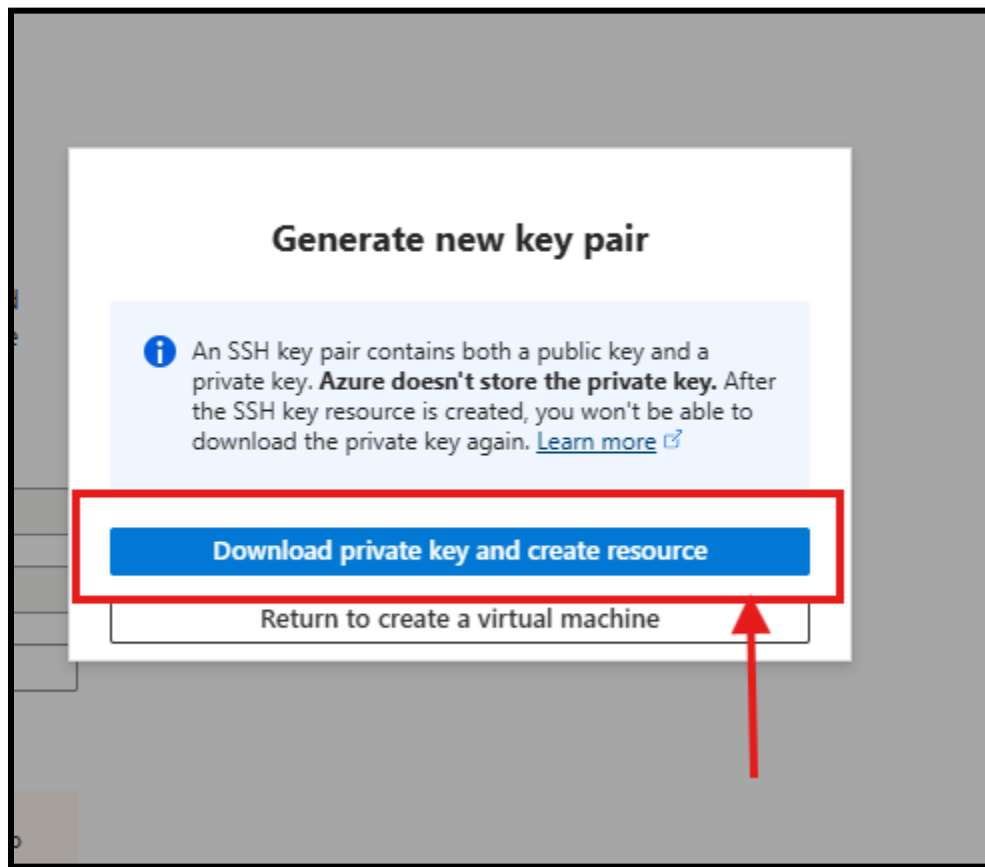
**⚠ You have set SSH port(s) open to the internet.** This is only recommended for testing. If you want to change this setting, go back to Basics tab.

**Basics**

Subscription Azure subscription 1

< Previous Next > **Create**

**Figure A-7. Download and create private SSH keys**



**Figure A-8. Virtual machine successfully deployed and active**

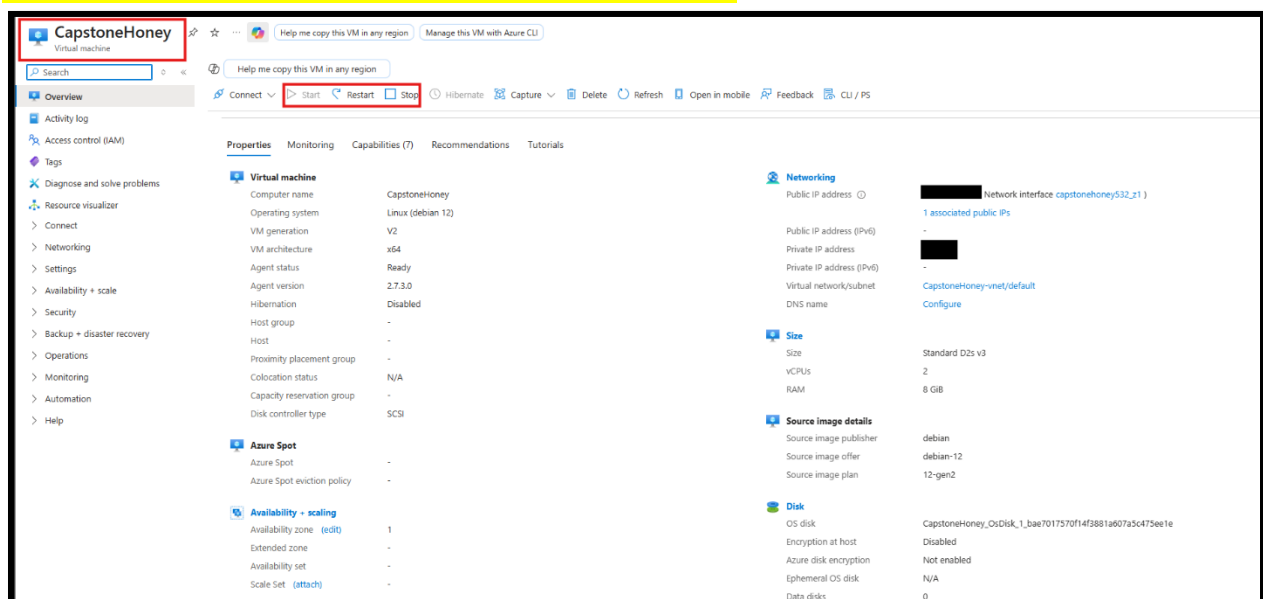


Figure A-9. Successful SSH connection to VM from local machine

```
PS C:\WINDOWS\system32> ssh -i "C:\Users\ [redacted] \Downloads\CapstoneHoney_key.pem" HoneyUser@ [redacted]
Linux CapstoneHoney 6.1.0-42-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.159-1 (2025-12-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
HoneyUser@CapstoneHoney:~$
```

Figure A-10. System maintenance command prior to installing T-Pot

```
HoneyUser@CapstoneHoney:~$ sudo apt update && sudo apt install git -y
Get:1 file:/etc/apt/mirrors/debian.list Mirrorlist [37 B]
Get:2 file:/etc/apt/mirrors/debian-security.list Mirrorlist [46 B]
```

Figure A-11. Downloading T-Pot from the GitHub repository

```
HoneyUser@CapstoneHoney:~$ git clone https://github.com/telekom-security/tpotce
Cloning into 'tpotce'...
remote: Enumerating objects: 17694, done.
remote: Total 17694 (delta 0), reused 0 (delta 0), pack-reused 17694 (from 1)
Receiving objects: 100% (17694/17694), 351.89 MiB | 42.21 MiB/s, done.
Resolving deltas: 100% (9879/9879), done.
HoneyUser@CapstoneHoney:~$
```

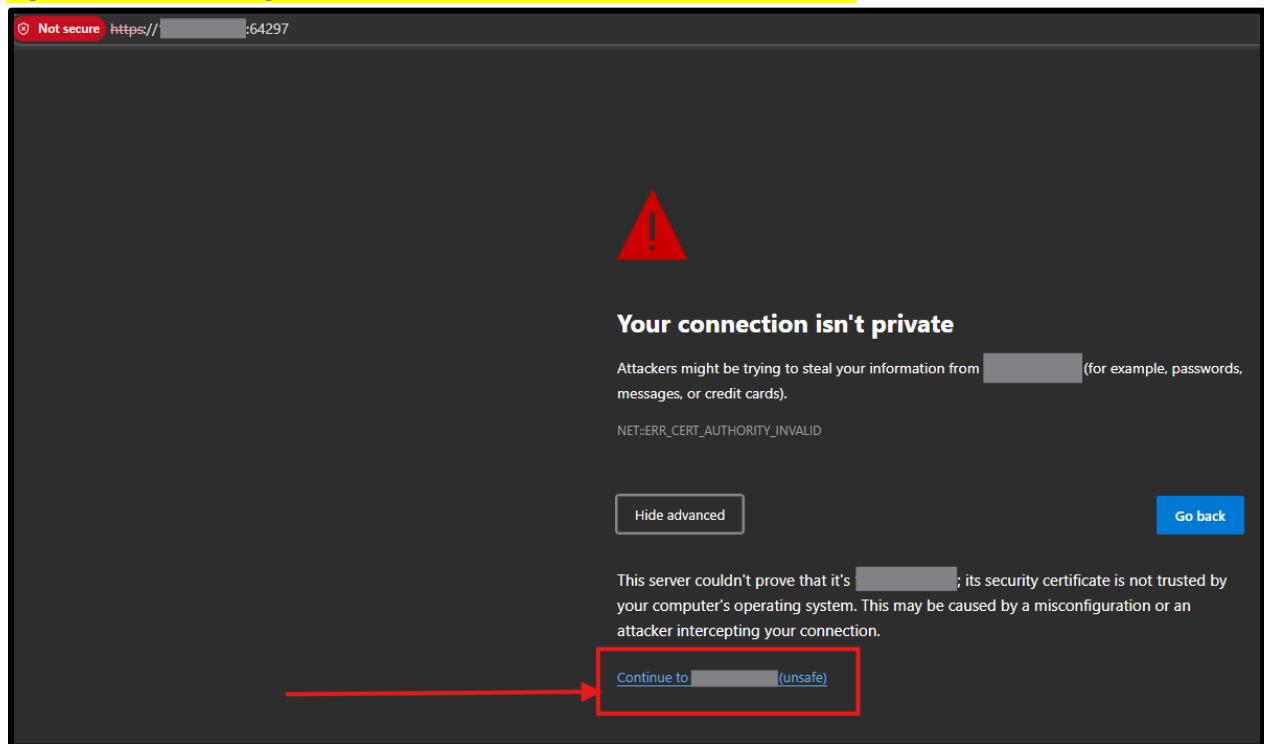
Figure A-12. Running the T-Pot installer from the tpotce directory

```
HoneyUser@CapstoneHoney:~/tpotce$ ./install.sh -t h -u [redacted] -p [redacted]

TPOT Installer

### This script will now install T-Pot and all of its dependencies.
### Install? (y/n)
```

**Figure A-13. Accessing the T-Pot web interface via <IP address>:64297**



**Figure A-14. T-Pot authentication using configured credentials**

A screenshot of a sign-in form titled "Sign in to access this site". Below the title, it says "Authorization required by https://[redacted]:64297". There are two input fields: "Username" and "Password". At the bottom, there are two buttons: "Sign in" and "Cancel".



Figure A-15. Successful T-Pot deployment confirmation

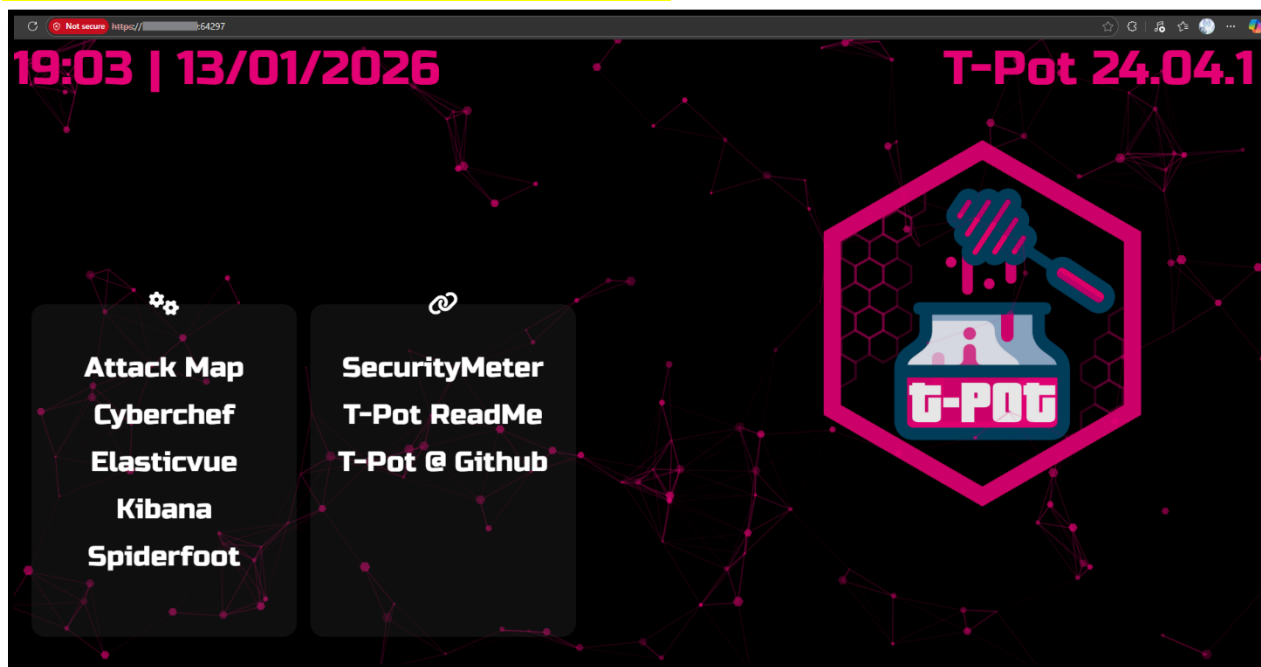


Figure A-16. Inbound Security Rules for Honeypot Management and Exposure

Network security group: **CapstoneHoney-nsg** attached to networkInterface: capstonehoney532\_z1  
Impacts 0 subnets, 1 network interfaces

+ Create port rule

Priority	Name	Port	Protocol	Source	Destination	Action
100	Admin_Access_Only	64295,64297	TCP		Any	Allow
110	Block_Admin_Public	64295,64297	Any	Any	Any	Deny
120	AllowAll_HoneyPot	Any	Any	Any	Any	Allow
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound port rules (3)

## Appendix B

### T-Pot Attack Analysis and Data Visualization

Figure B-1. T-Pot integrated attack map with live feed indicating real-time attacks against the honeypot

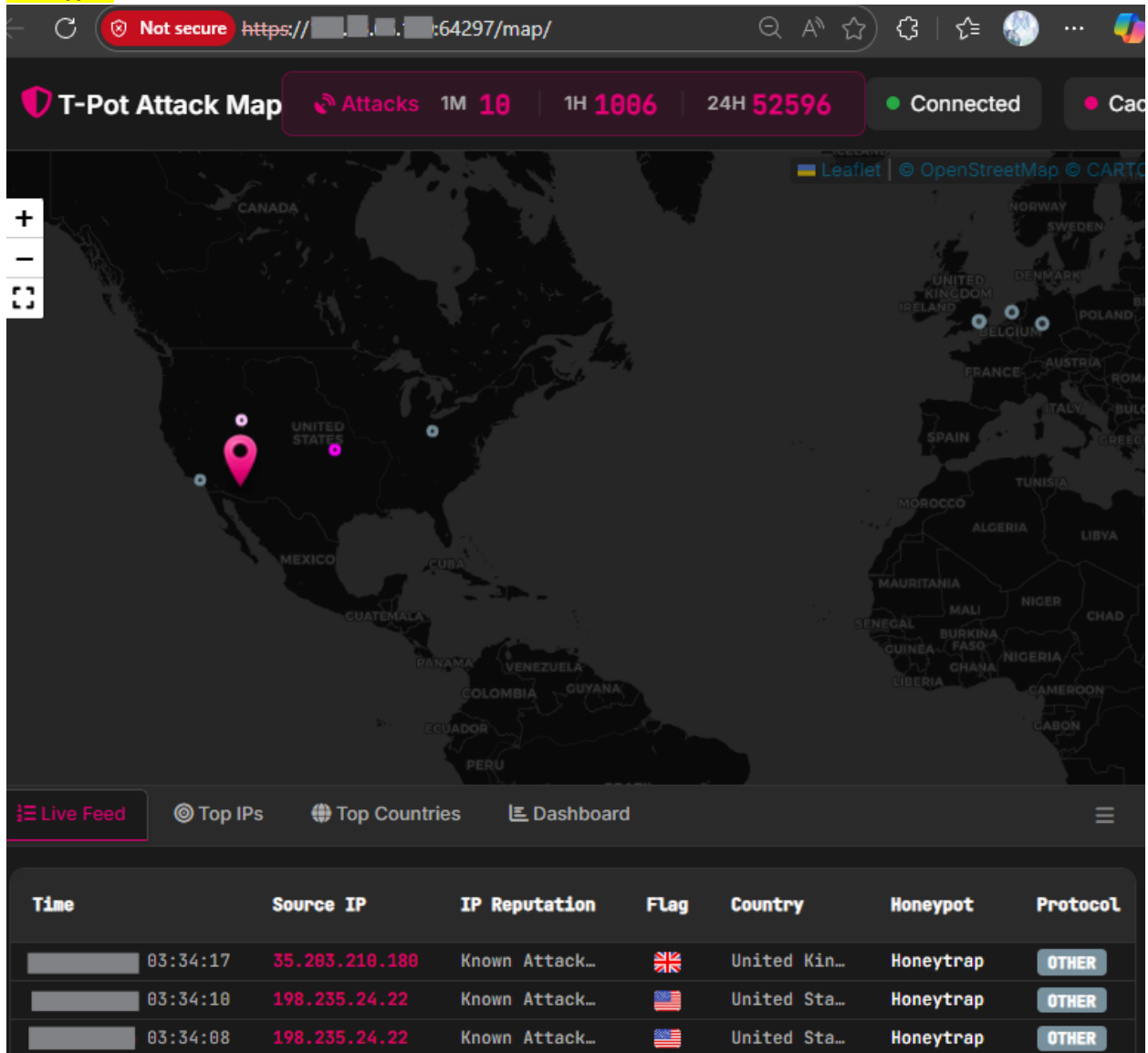


Figure B-2. Kibana dashboard displaying attack data collected over the last seven days, showing 478,000 established connections, including histograms of most targeted destination ports and top source countries

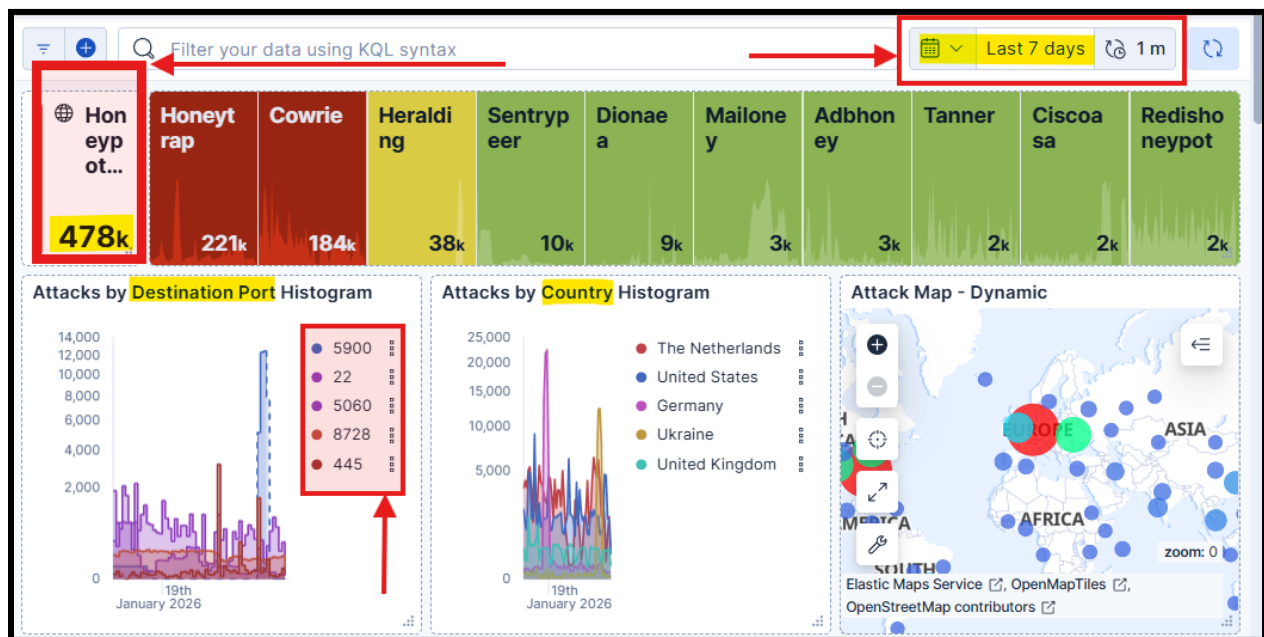


Figure B-3. Kibana filter configured using IP reputation data associated with known attackers, displaying the most frequently targeted ports by identified malicious sources over the last seven days

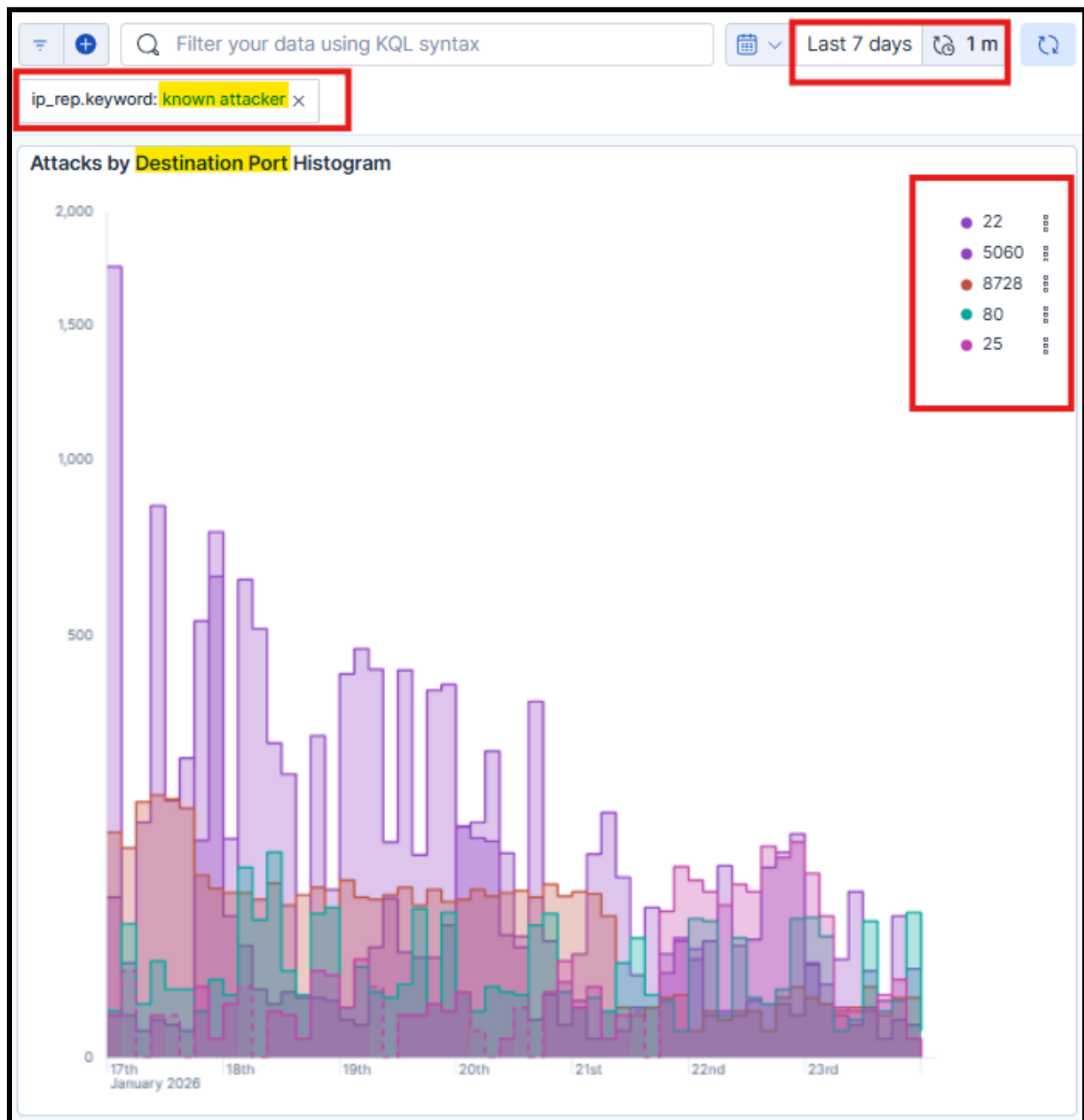


Figure B-4. Suricata alert signature analysis showing one of the top ten signatures related to the user-agent 'python-requests', accounting for 8,776 detected events

Suricata Alert Signature - Top 10		
ID	Description	Count
2100560	GPL INFO VNC server response	254,422
2002920	ET INFO VNC Authentication Failure	36,845
2002923	ET EXPLOIT VNC Server Not Requiring Authentication (case 2)	36,845
2100384	GPL ICMP PING	11,933
2017515	ET INFO User-Agent (python-requests) Inbound to Webserver	8,776
2006408	ET INFO HTTP Request on Unusual Port Possibly Hostile	2,862
2402000	ET DROP Dshield Block Listed Source group 1	2,850
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	2,795
2009582	ET SCAN NMAP -sS window 1024	947
2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port	775

Figure B-5. Visualization of the most common attacker source IP addresses observed targeting the honeypot

Attacker Source IP - Top 10	
Source IP	Count
45.95.147.22	20,080
187.108.1.13	12,632
204.76.203.1	3,504
129.212.176.	3,197
129.212.187.	3,188
91.224.92.15	2,621
78.128.112.7	2,082
194.50.16.13	1,755
129.212.183.	1,638
206.189.102.	1,498
Rows per page: 10	
< 1 >	







## Appendix C

### Secured Virtual Machine Hardening and Compliance Validation

**Figure C-1. Configuration overview of the Secured-VM, including assigned IP address, virtual machine size, and operating system image**




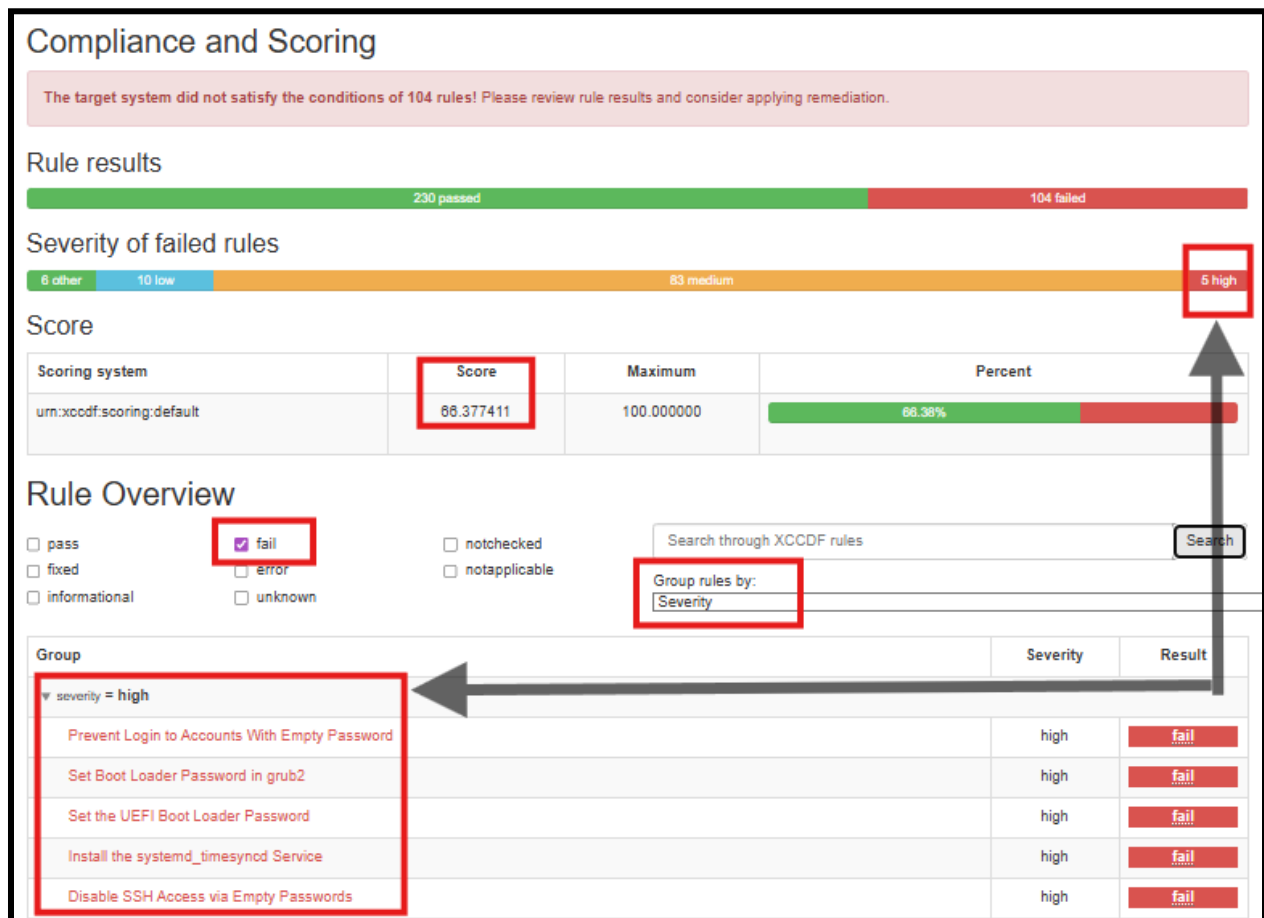
 <b>Networking</b>	
Public IP address ⓘ	134.33.97.29 Network interface secured-vm879_z1 ) 1 associated public IPs
Public IP address (IPv6)	-
Private IP address	
Private IP address (IPv6)	-
Virtual network/subnet	vnet-westus3-1/snet-westus3-1
DNS name	Configure
 <b>Size</b>	
Size	Standard B2as v2
vCPUs	2
RAM	8 GiB
 <b>Source image details</b>	
Source image publisher	canonical
Source image offer	0001-com-ubuntu-server-jammy
Source image plan	22_04-lts-gen2

Figure C-2. Web application hosted on the Secured-VM, accessed directly via the virtual machine's public IP address (134.33.97.29)



**Figure C-3. Initial OpenSCAP CIS benchmark audit results for the Secured-VM using default Azure-recommended settings, showing a compliance score of 66.377% with five high-severity findings**



**Figure C-4. Modification of the /etc/ssh/sshd\_config file on the Secured-VM via Azure Serial Console, showing the PermitRootLogin directive set to "no"**

```
GNU nano 6.2 /etc/ssh/sshd_config
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
```

Figure C-5. Modification of the /etc/ssh/sshd\_config file on the Secured-VM via Azure Serial Console, showing the PermitEmptyPasswords directive set to “no”

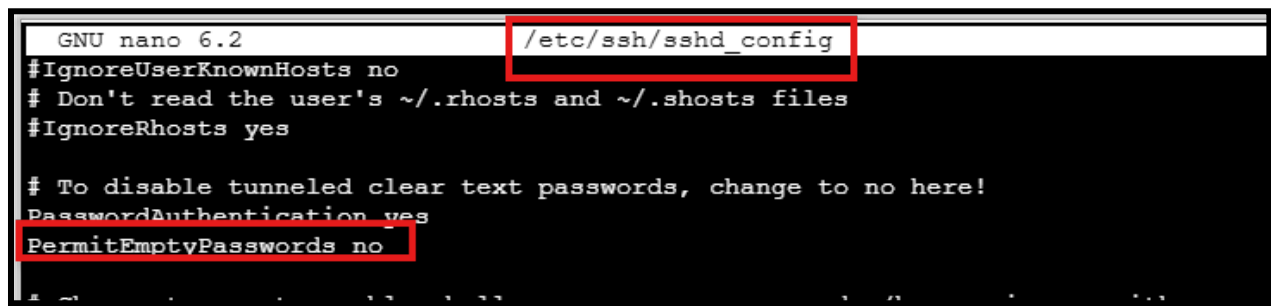


Figure C-6. Follow-up OpenSCAP scan results indicating a reduction to three high-severity findings and an improved compliance score of 68.23% after SSH hardening

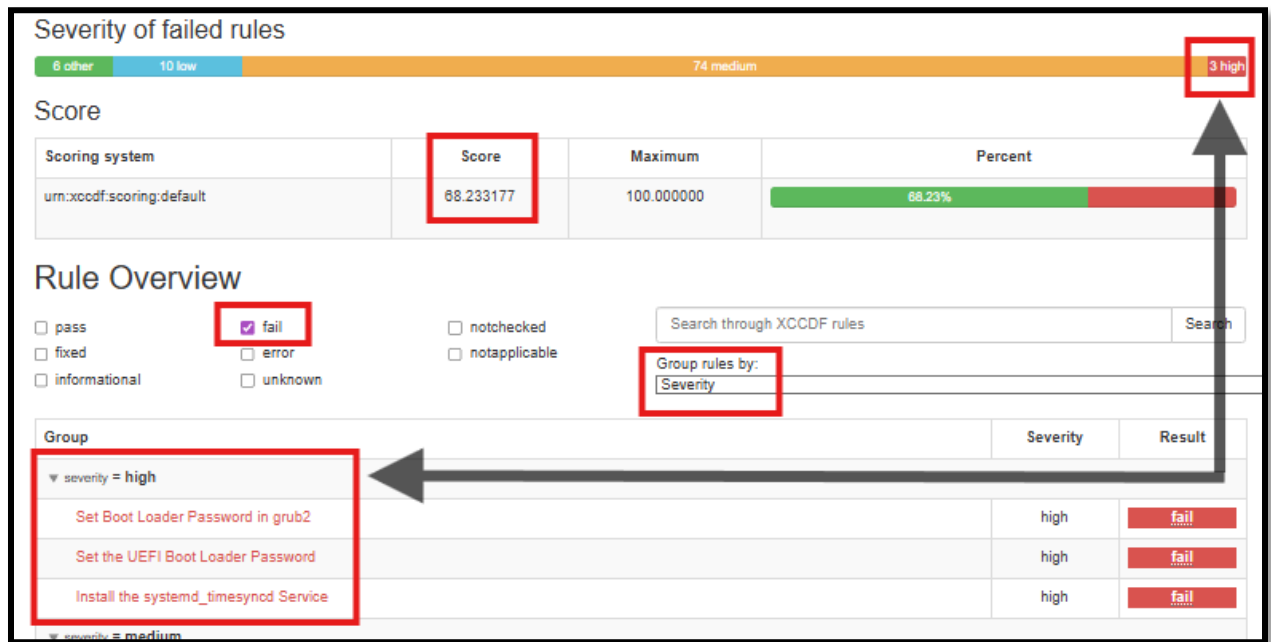


Figure C-7. Implementation of an inbound Azure Network Security Group (NSG) rule on the Secured-VM to block top attacker source IP addresses identified through threat analysis (Figure B-5)

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
100	Deny_Top_Attacker_IPs	Any	Any	45.95.147.22,187.108.1....	Any	Deny

Figure C-8. Implementation of an outbound Azure Network Security Group (NSG) rule on the Secured-VM to restrict suspicious Python-based callback traffic observed during attack analysis

Prio...	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
Outbound port rules (4)						
100	Anti_callback_rule	80,443	TCP	Any	Internet	Deny

Figure C-9. Final OpenSCAP scan results after applying threat-informed security controls, showing no additional improvement in compliance score, indicating that network-level controls do not directly impact CIS benchmark scoring

