Appendix A

Creation and Deployment of Azure Virtual Machine with T-Pot

Figure A-1. Select Create Resource in Microsoft Azure

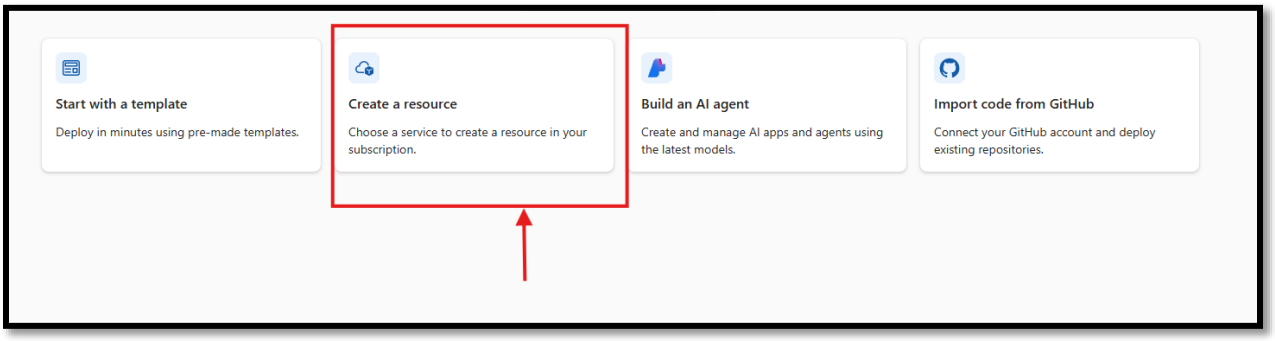


Figure A-2. Select Create Virtual Machine

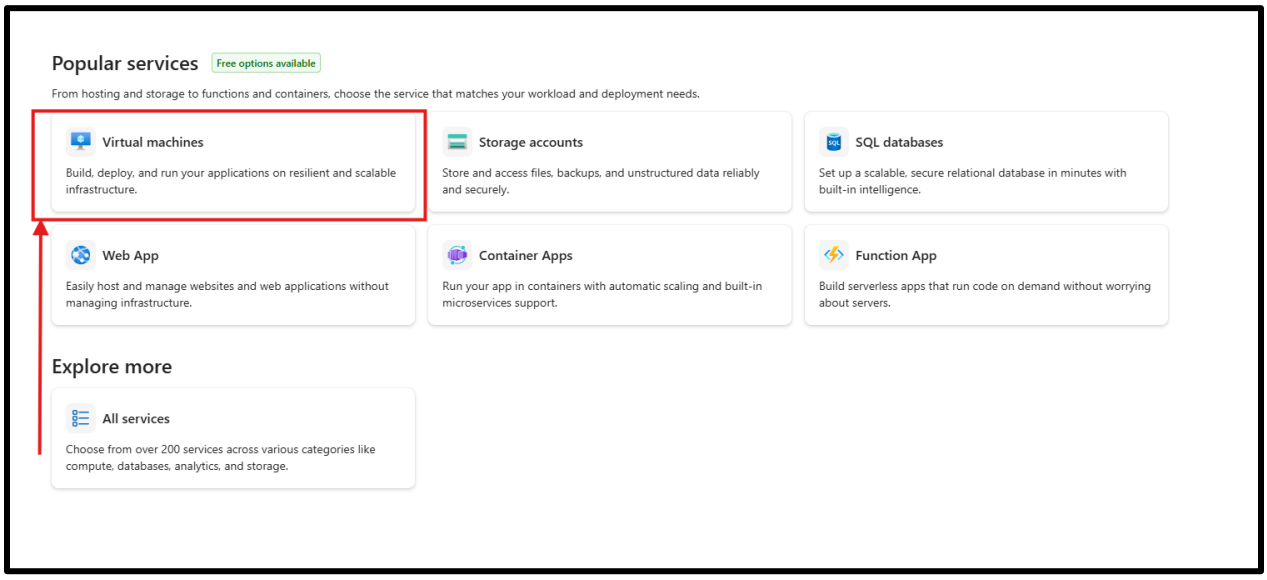


Figure A-3. Configure subscription, resource group, VM name, region, and Debian 12 x64 image

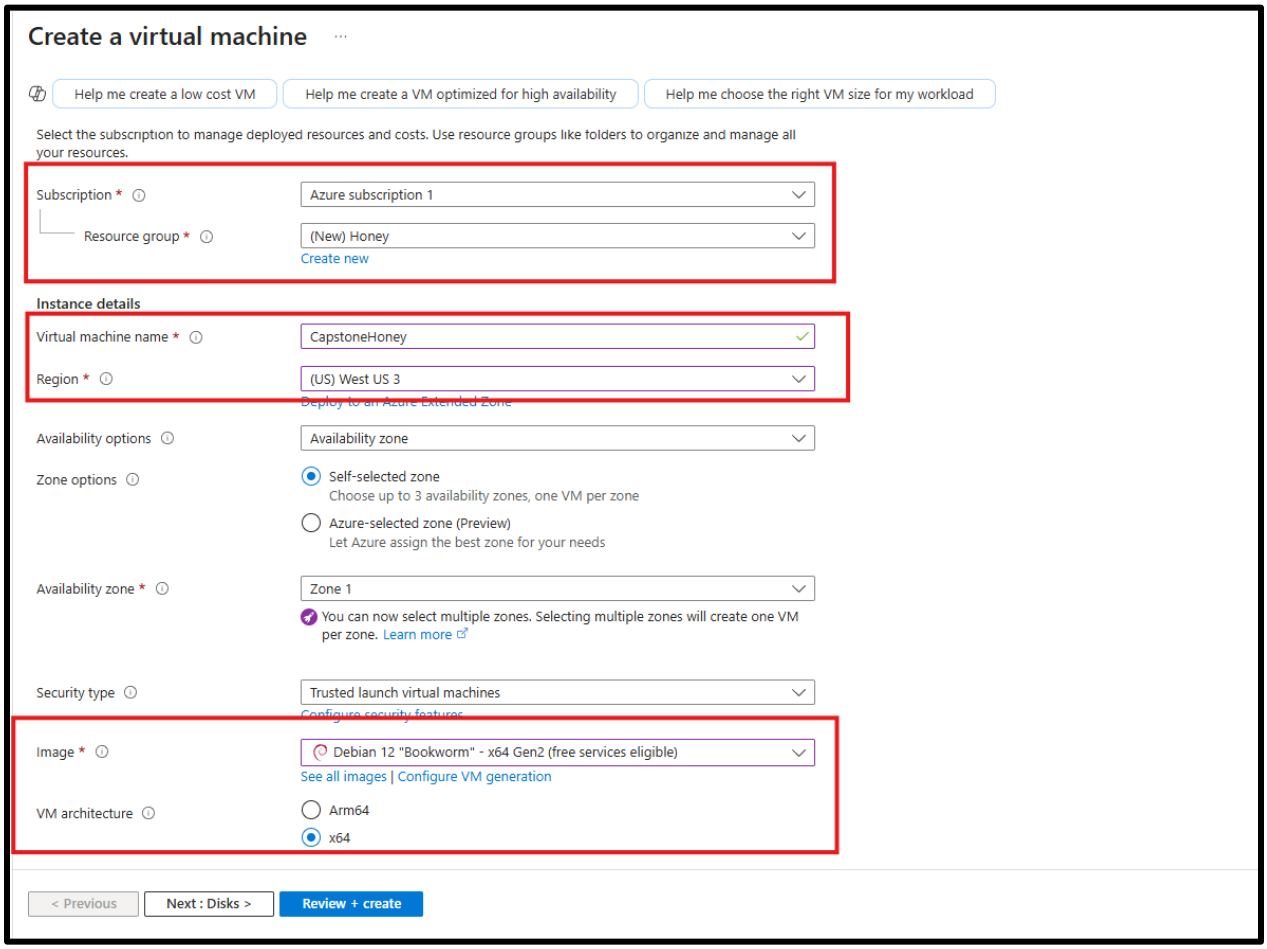


Figure A-4. Set OS disk size to 128 GiB

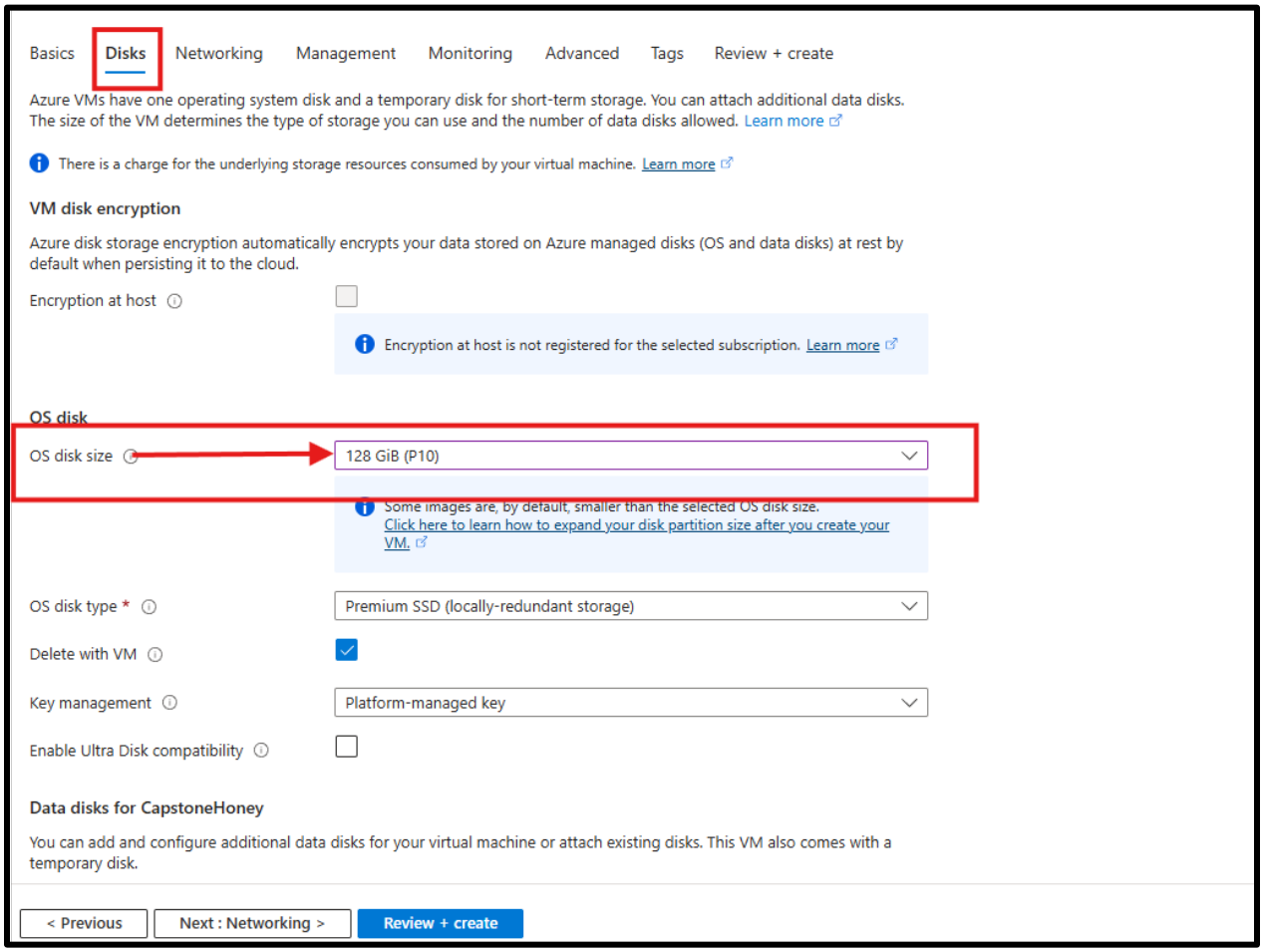


Figure A-5. Ensure Auto-shutdown is unchecked

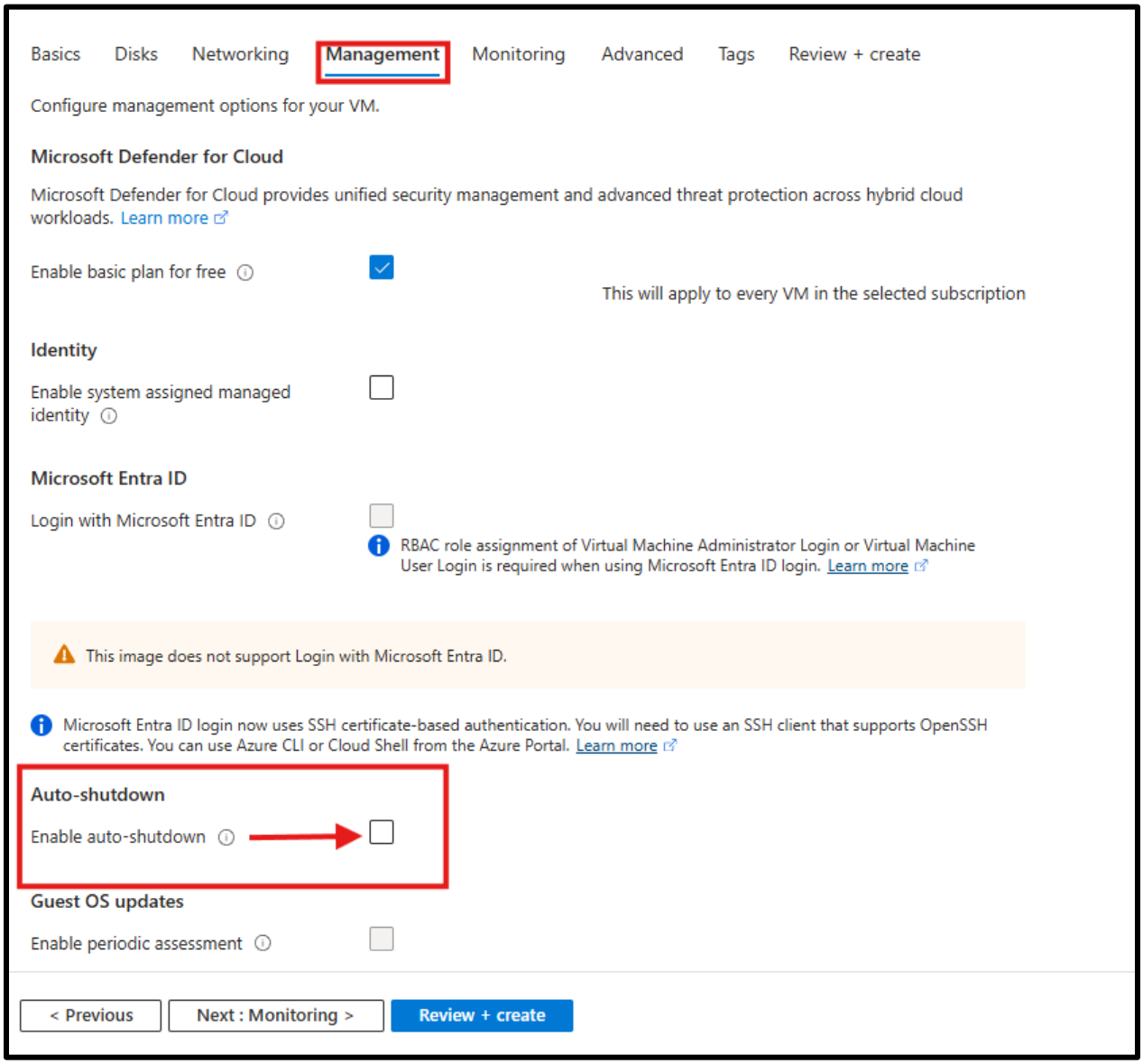


Figure A-6. Review and create virtual machine

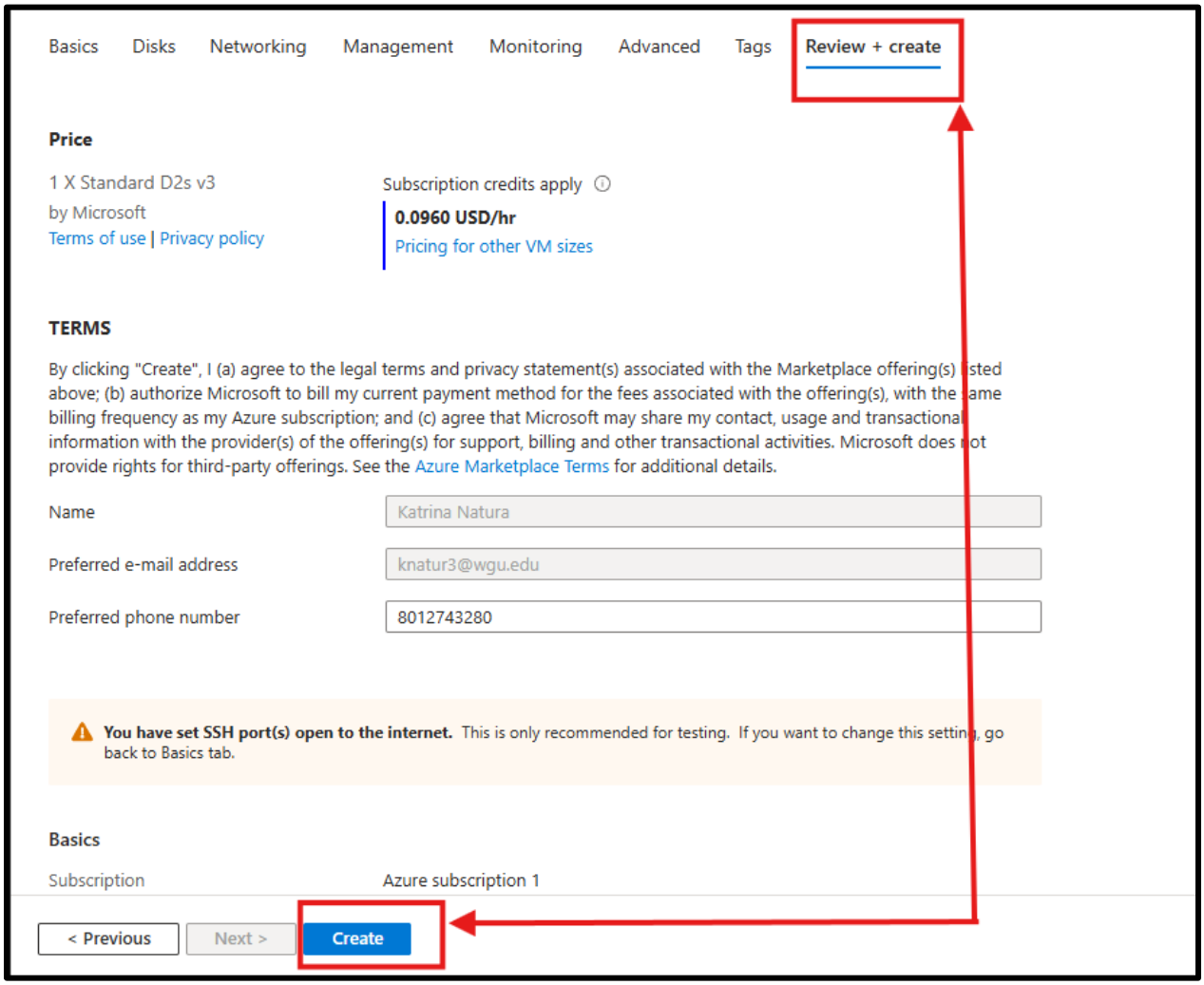


Figure A-7. Download and create private SSH keys

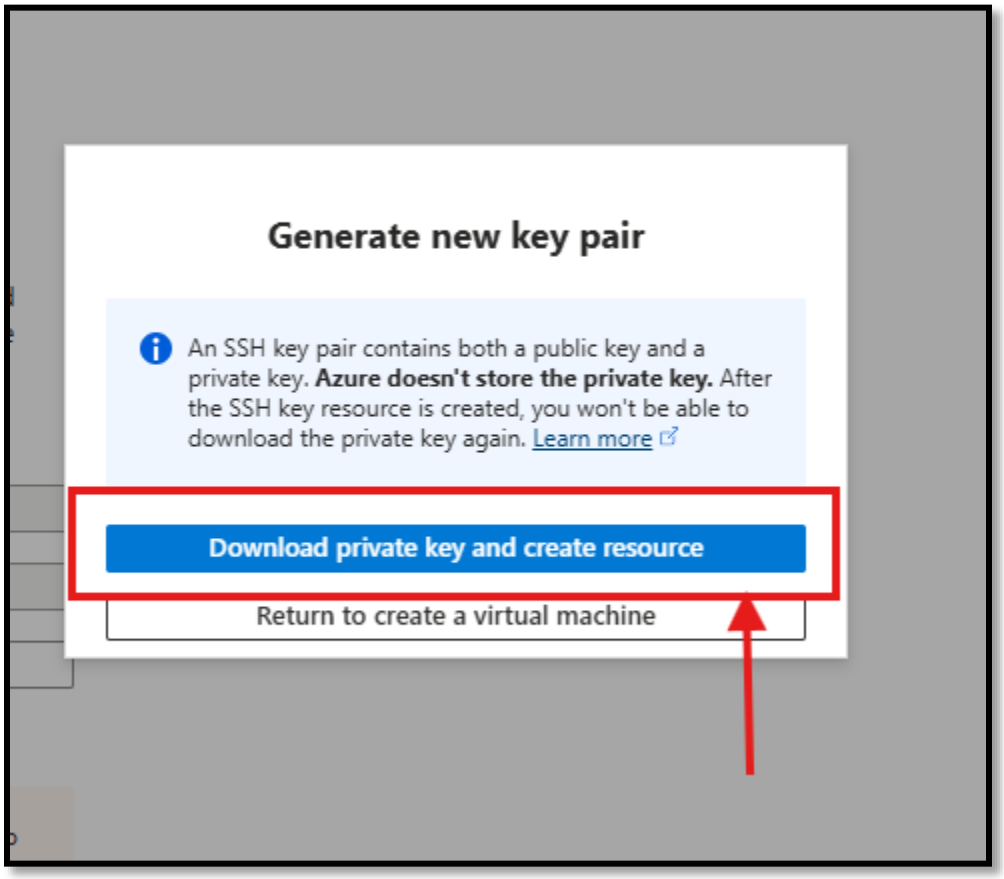


Figure A-8. Virtual machine successfully deployed and active

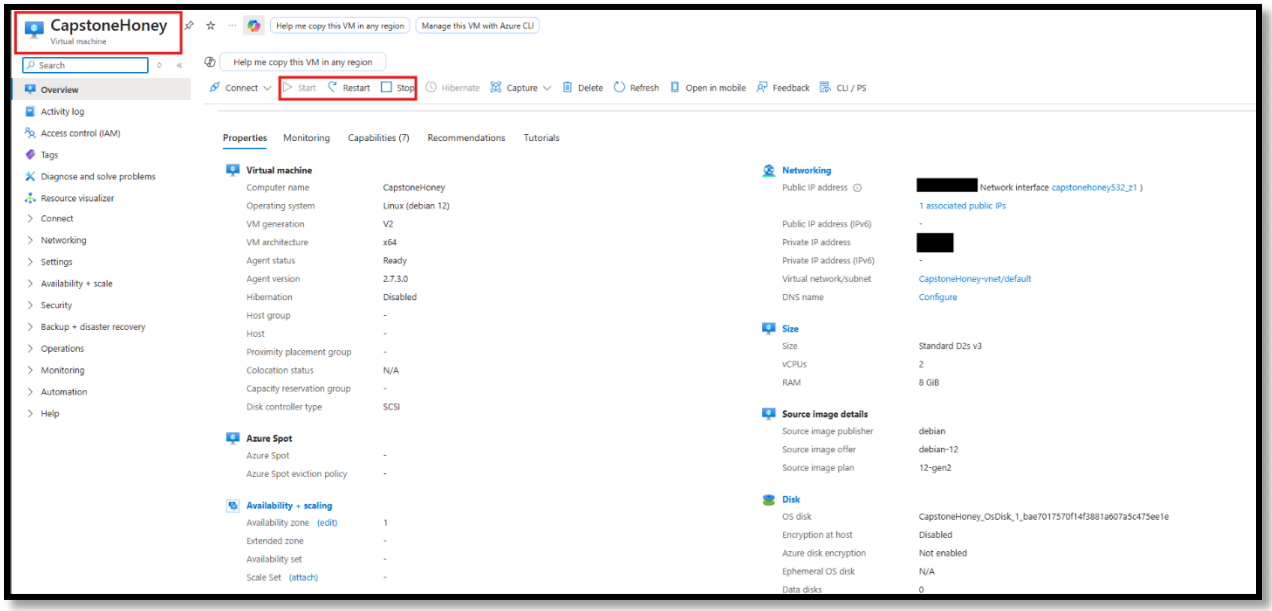


Figure A-9. Successful SSH connection to VM from local machine

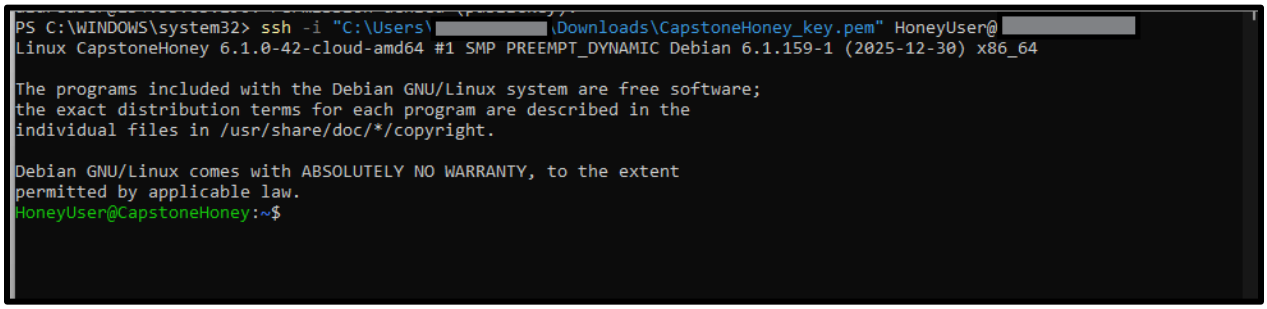


Figure A-10. System maintenance command prior to installing T-Pot

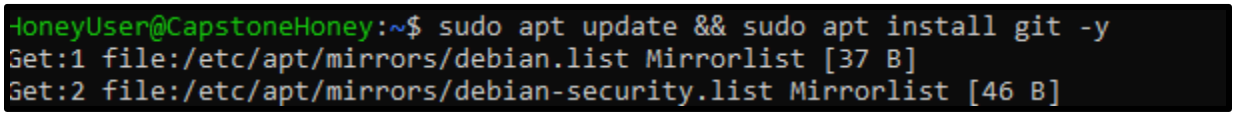


Figure A-11. Downloading T-Pot from the GitHub repository

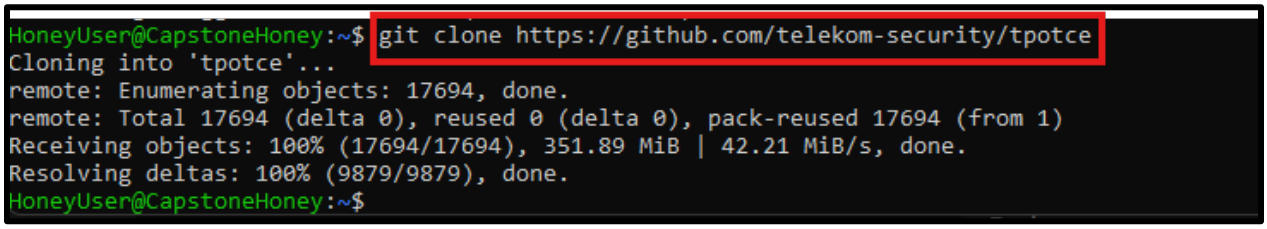


Figure A-12. Running the T-Pot installer from the tpotce directory

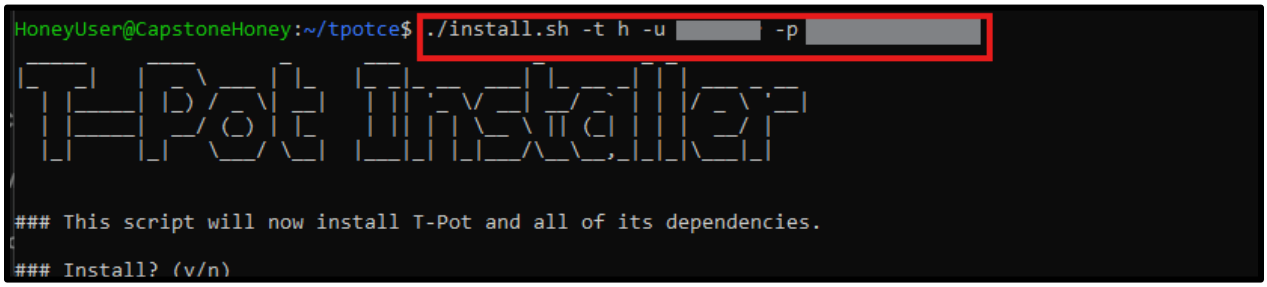


Figure A-13. Accessing the T-Pot web interface via <IP address>:64297

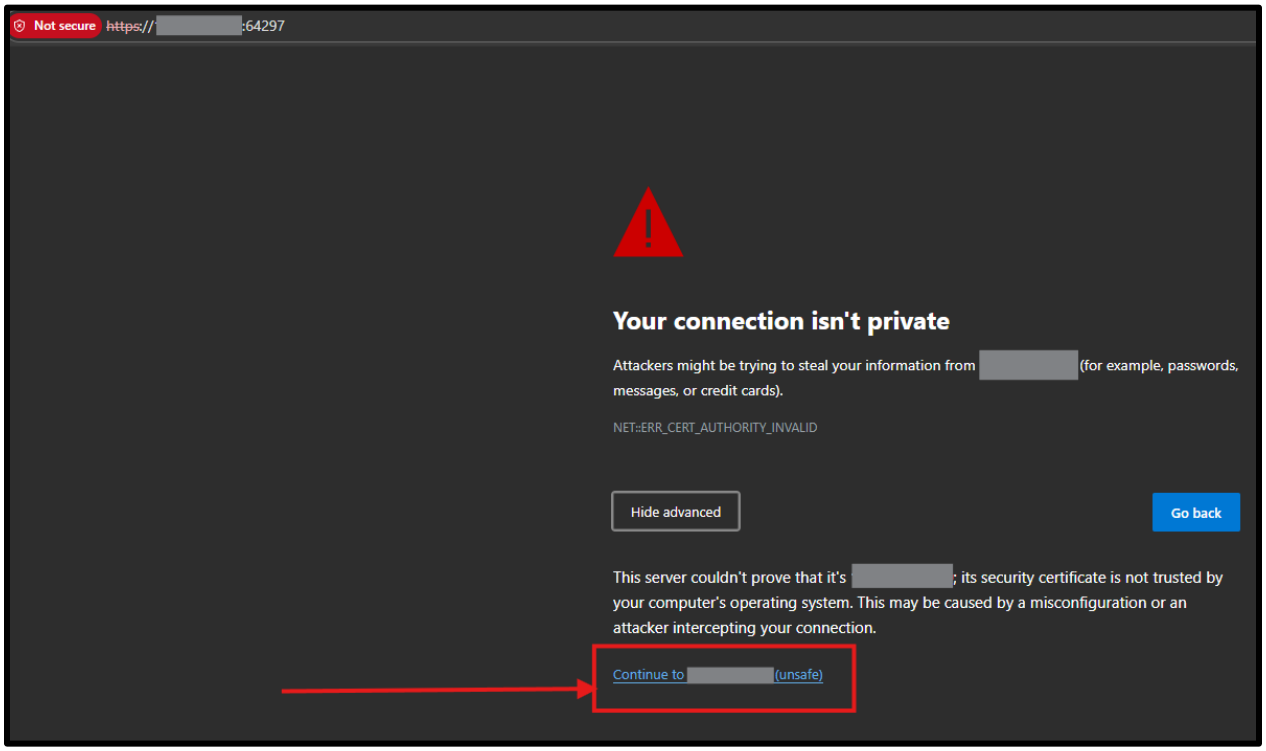


Figure A-14. T-Pot authentication using configured credentials

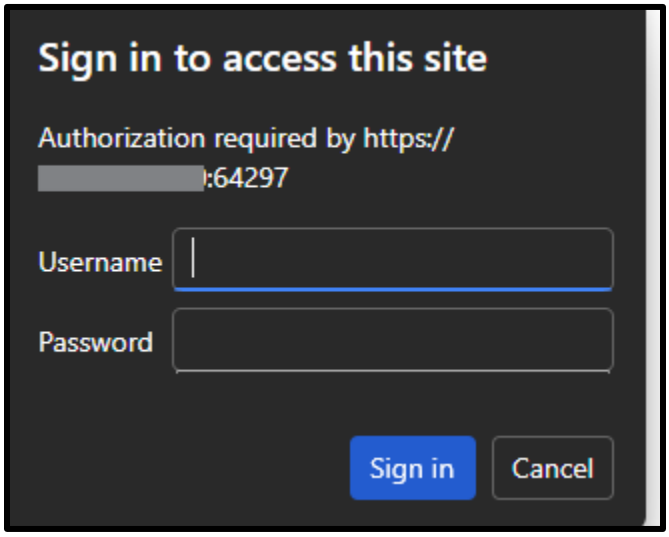


Figure A-15. Successful T-Pot deployment confirmation

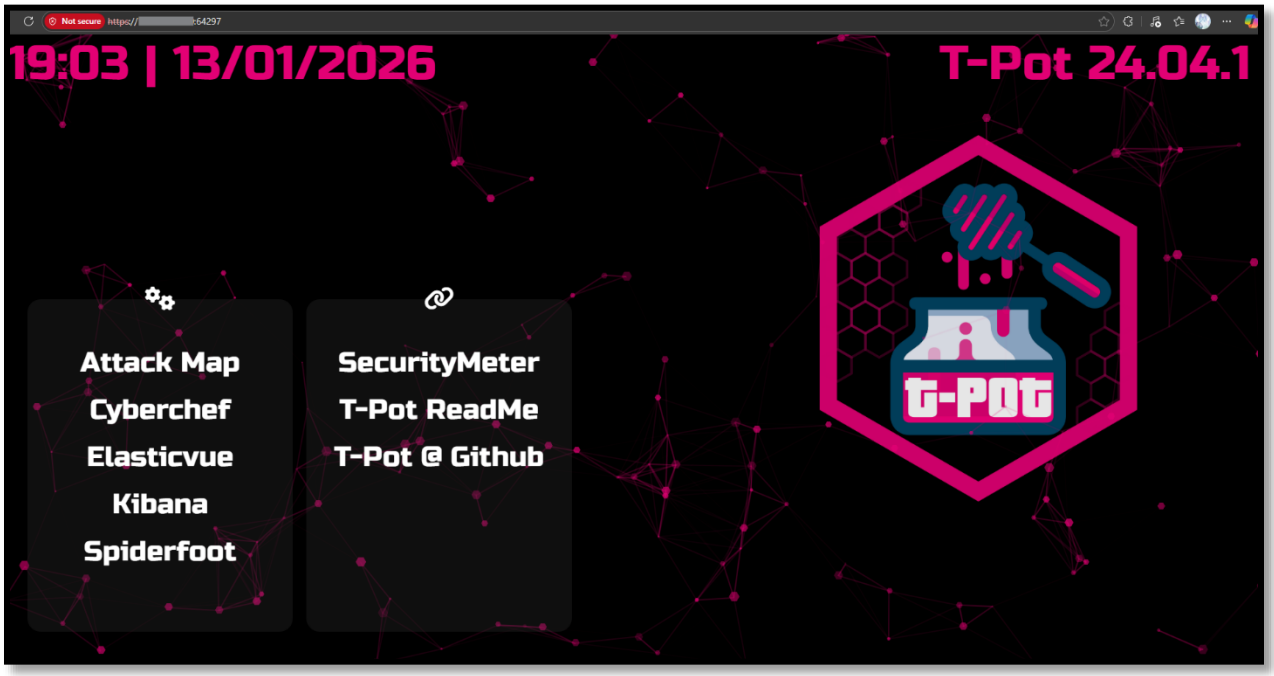
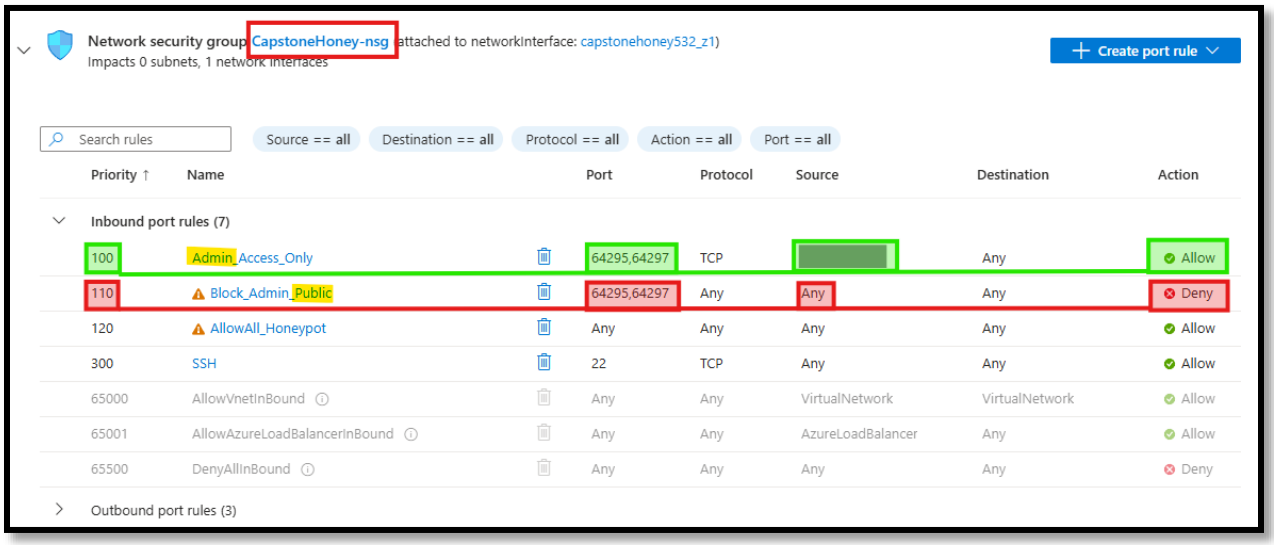


Figure A-16. Inbound Security Rules for Honeypot Management and Exposure



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

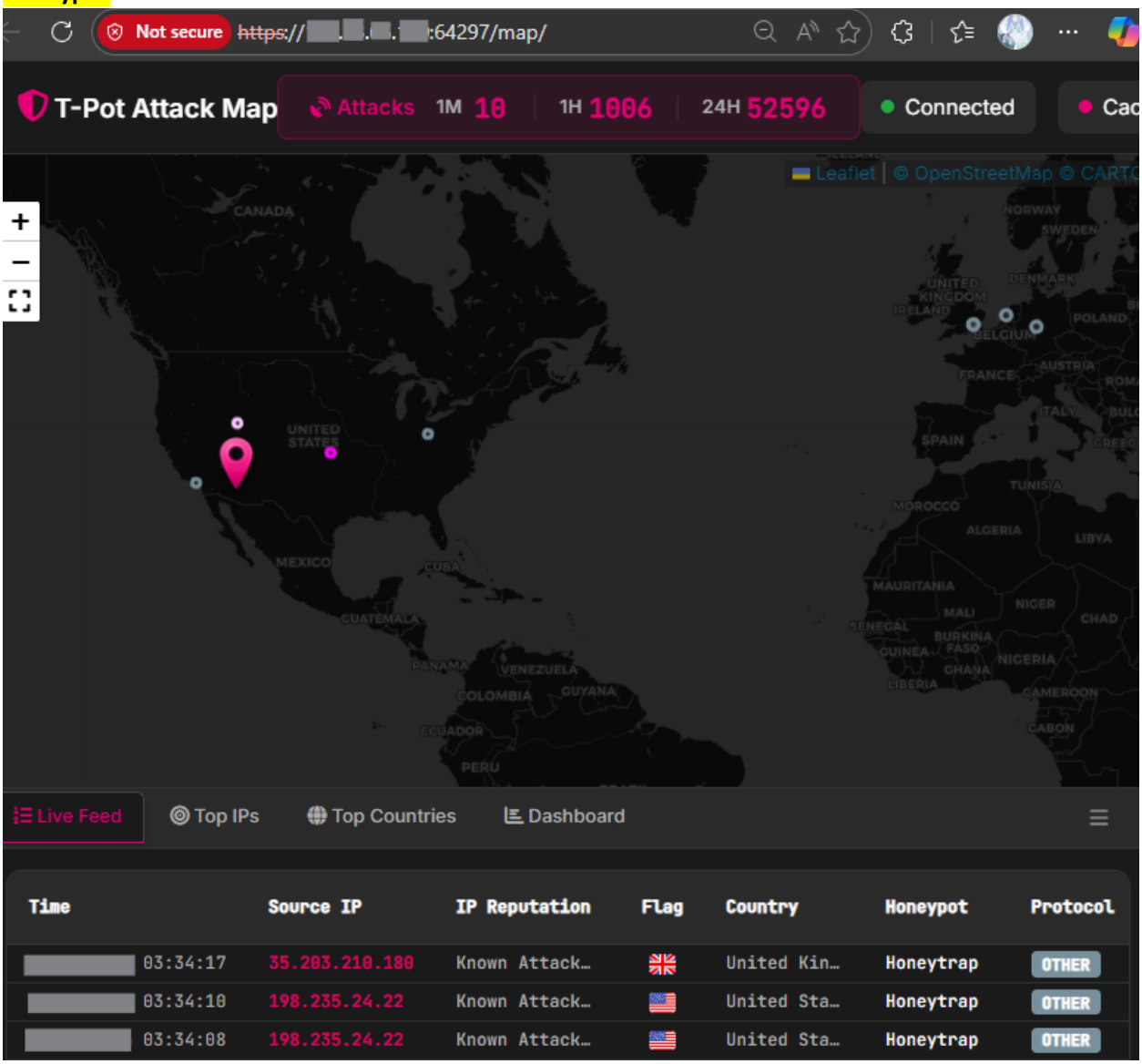


Figure B-2. Kibana dashboard displaying attack data collected over the last seven days, showing 478,000 established connections, including histograms of most targeted destination ports and top source countries

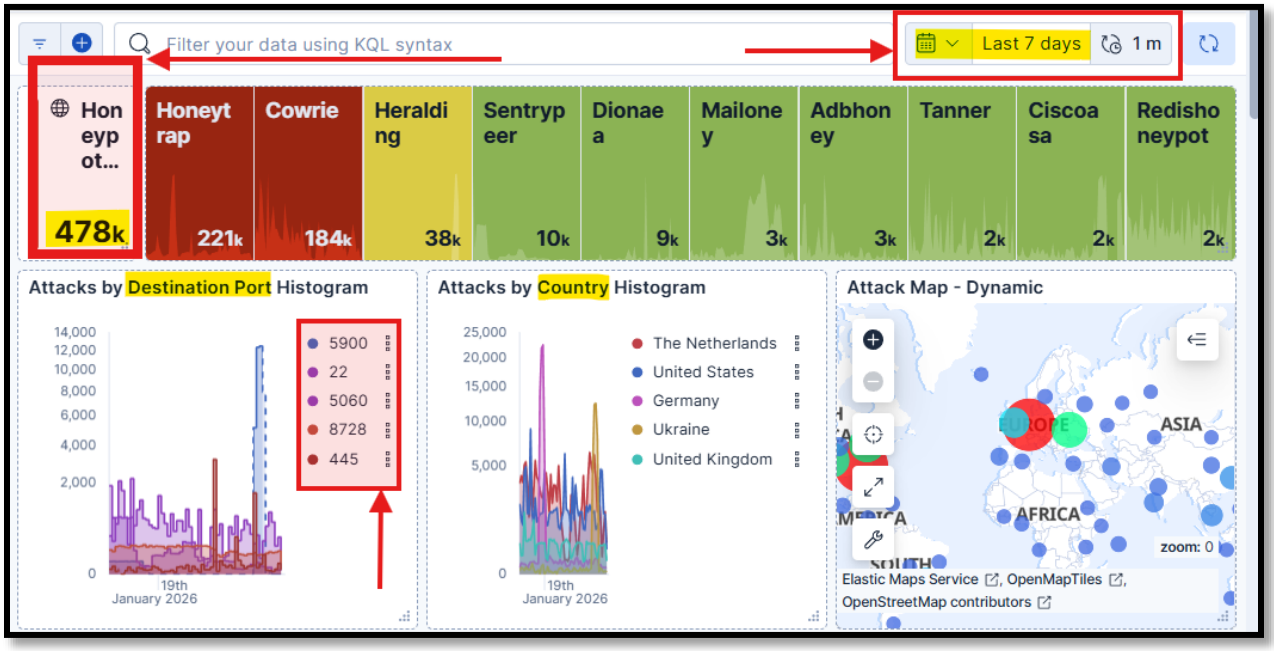


Figure B-3. Kibana filter configured using IP reputation data associated with known attackers, displaying the most frequently targeted ports by identified malicious sources over the last seven days

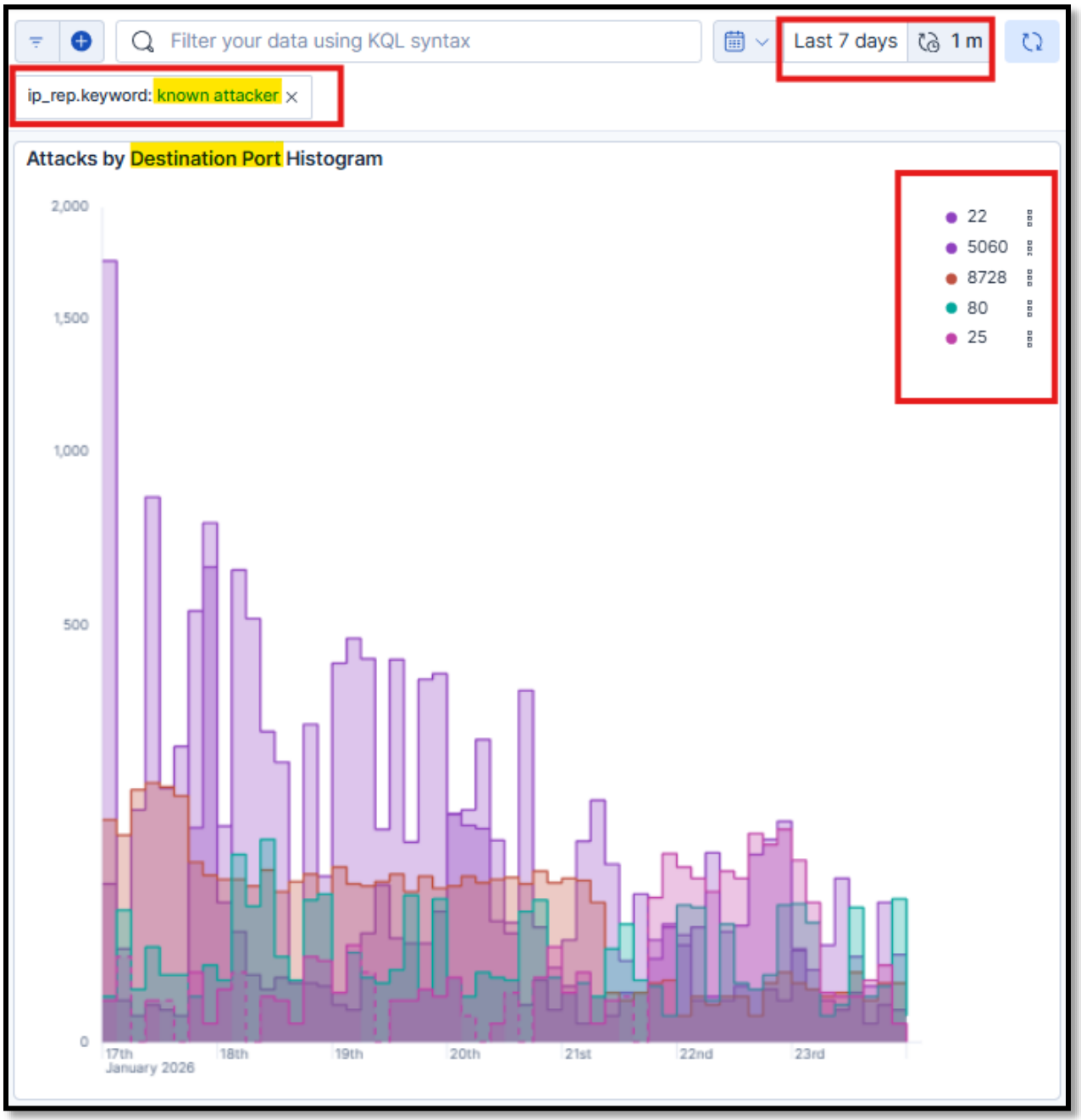
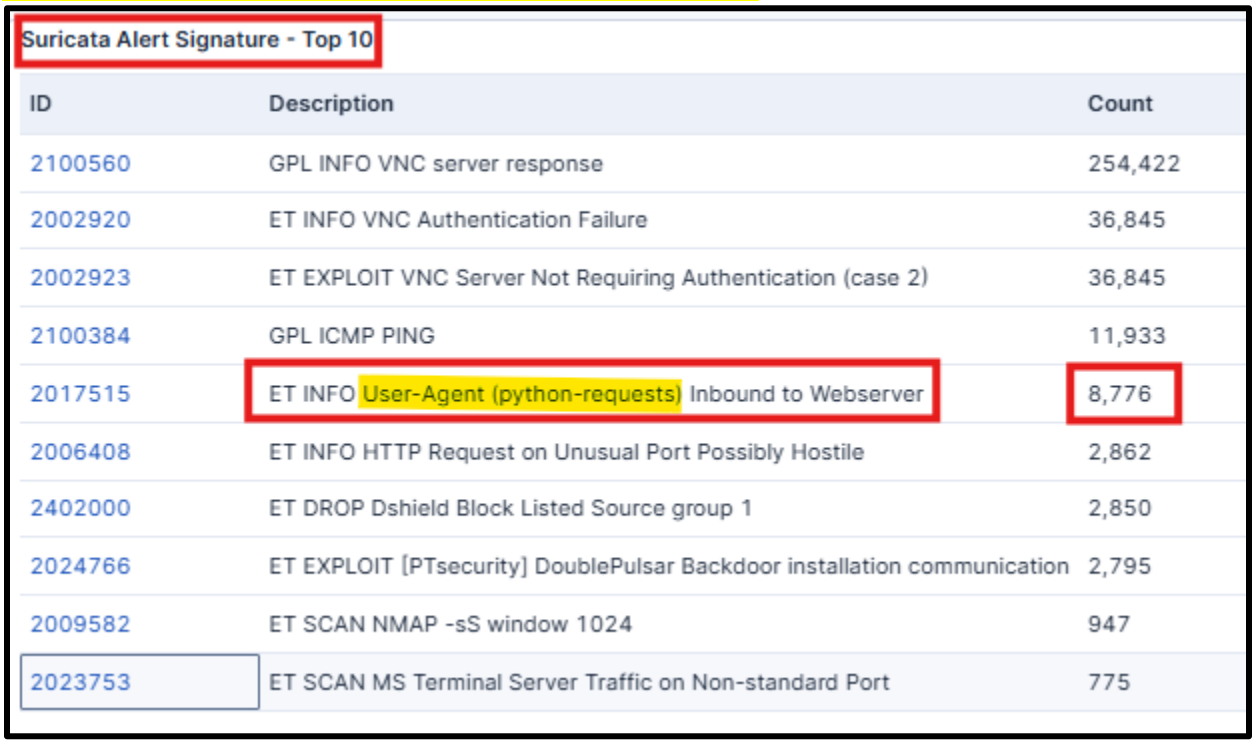


Figure B-4. Suricata alert signature analysis showing one of the top ten signatures related to the user-agent 'python-requests', accounting for 8,776 detected events

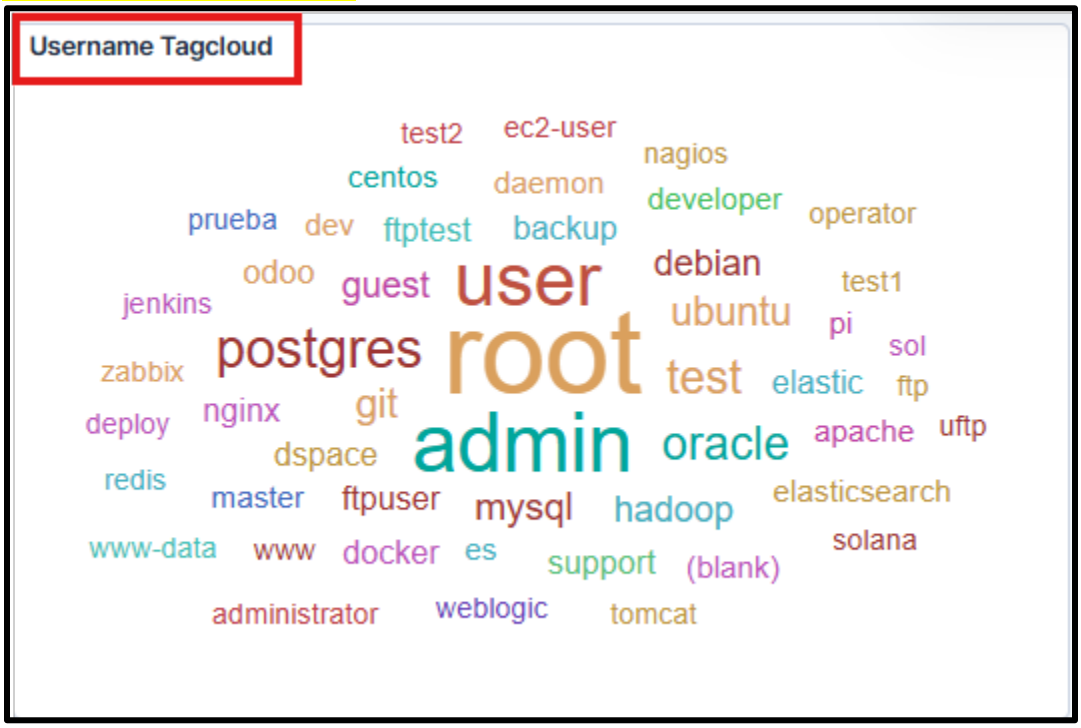


Suricata Alert Signature - Top 10

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

Figure B-6. Visualization of the most commonly used usernames observed in authentication-based attacks against the honeypot



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

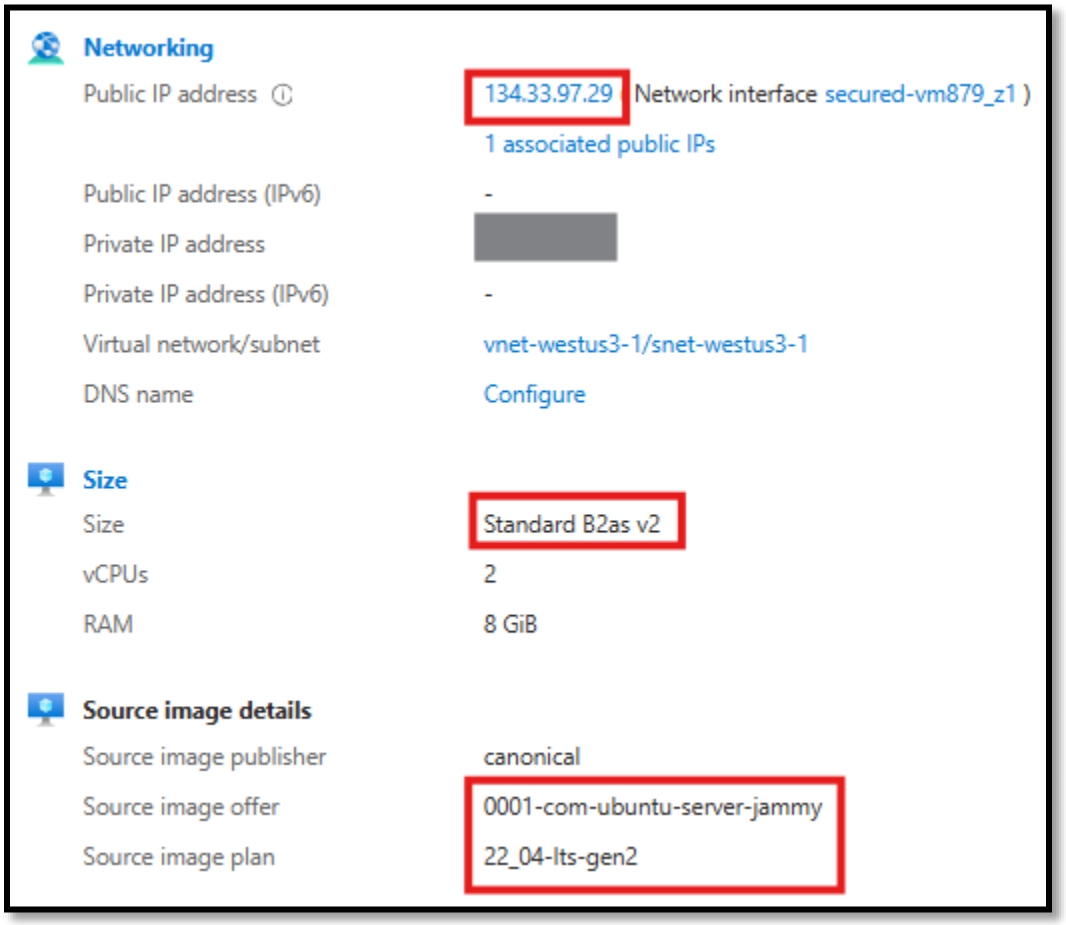


Figure C-2. Web application hosted on the Secured-VM, accessed directly via the virtual machine's public IP address (134.33.97.29)

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

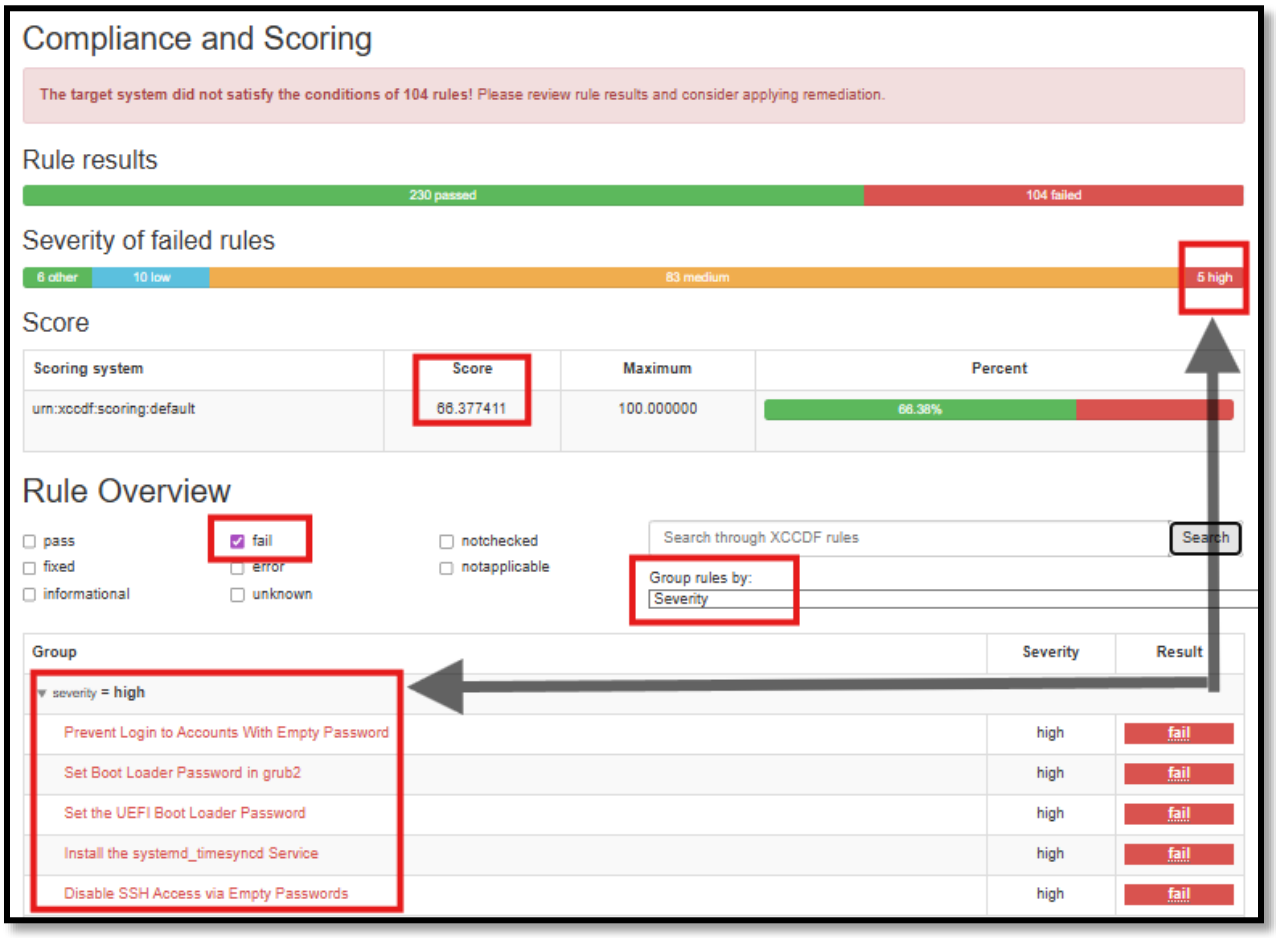


Figure C-4. Modification of the /etc/ssh/sshd_config file on the Secured-VM via Azure Serial Console, showing the PermitRootLogin directive set to "no"

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"

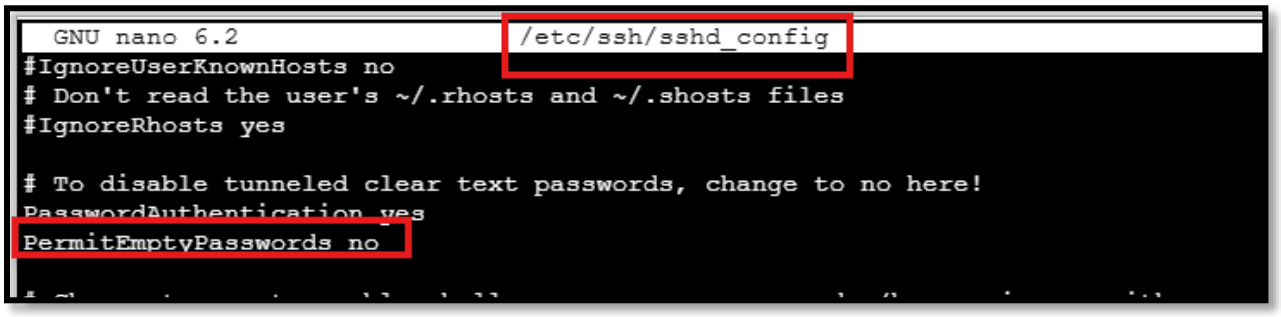


Figure C-6. Follow-up OpenSCAP scan results indicating a reduction to three high-severity findings and an improved compliance score of 68.23% after SSH hardening

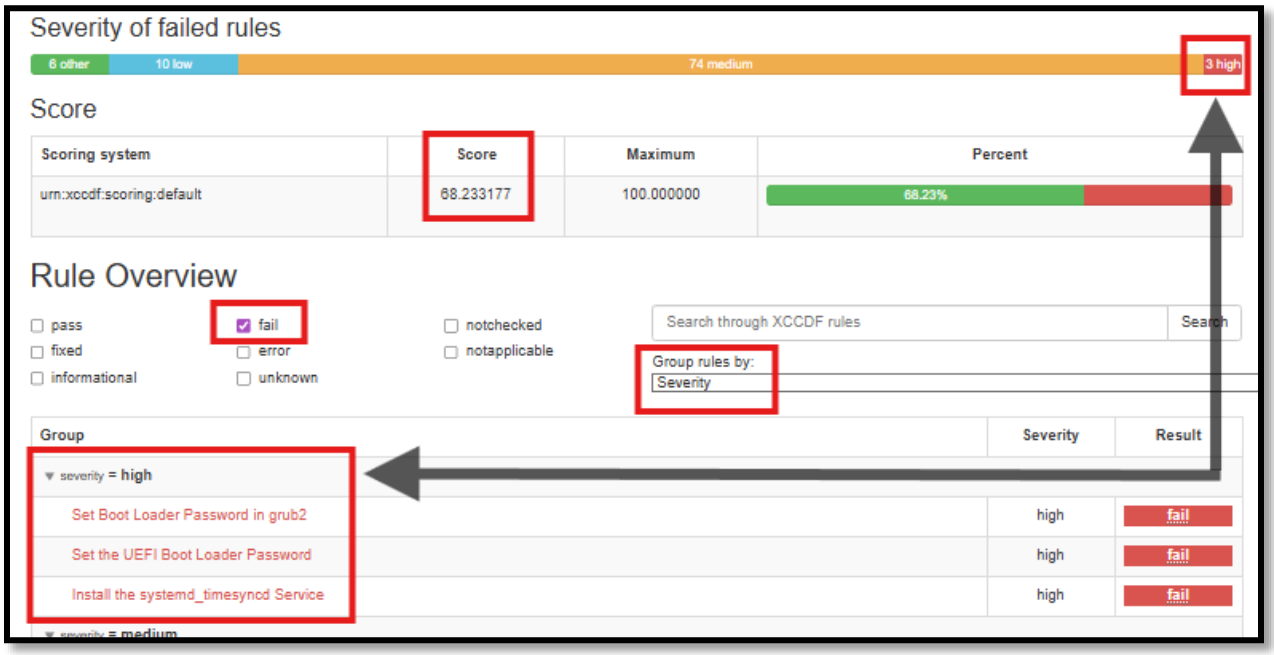


Figure C-7. Implementation of an inbound Azure Network Security Group (NSG) rule on the Secured-VM to block top attacker source IP addresses identified through threat analysis (Figure B-5)

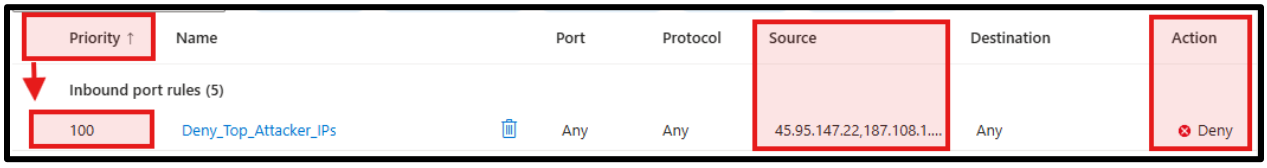


Figure C-8. Implementation of an outbound Azure Network Security Group (NSG) rule on the Secured-VM to restrict suspicious Python-based callback traffic observed during attack analysis

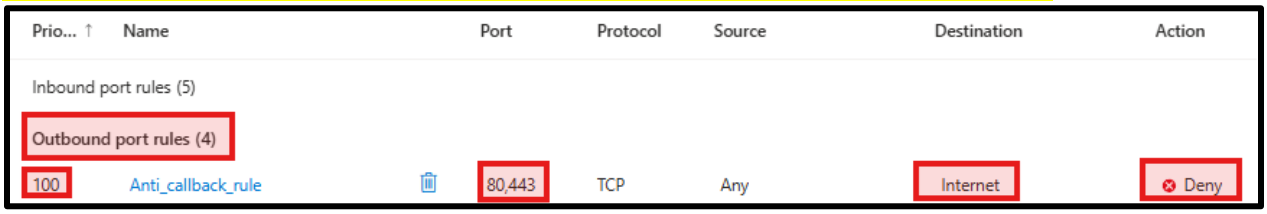


Figure C-9. Final OpenSCAP scan results after applying threat-informed security controls, showing no additional improvement in compliance score, indicating that network-level controls do not directly impact CIS benchmark scoring