

Intro to HoneyPot

What is a honeypot?

 A cyber trap or decoy designed to look like a legitimate part of a system, network, or other digital environment

How do they operate?

- Research vs Production
- Use security vulnerabilities to lure in attackers

Benefits of using a honeypot

- Detection of malicious activity
- Diversion of malicious traffic
- Data collection



Deployment to Azure

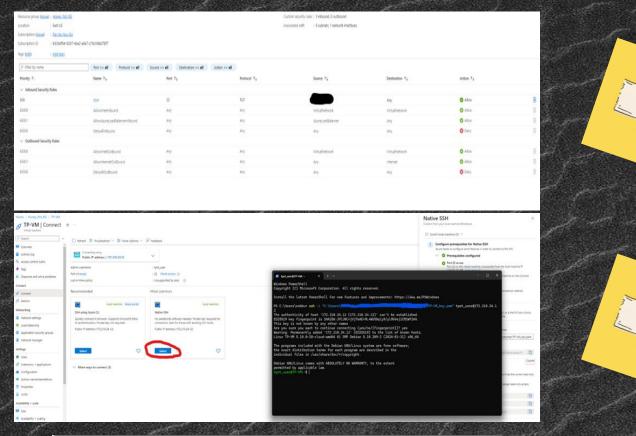
	rirtual mad	ey_Pot_RG > Mar chine ···				
Basics Disks	Networking	Management	Monitoring	Advanced	Tags	Review + create
image. Complete		n Review + create to				or use your own customized t parameters or review each tal
Project details						
Select the subscri your resources.	iption to manage o	leployed resources	and costs. Use resc	ource groups	like folde	ers to organize and manage all
Subscription * ()	Pay-As-You-Go				
Resource group * ①		the state of the s	Honey_Pot_RG			ं
Instance details		Create new	2			
Virtual machine name * ③		16-AW	IP-VM			
Region * ①		(US) East	(US) East US			
Availability options ①		Availabilit	Availability zone			
Availability zone * ①		Zones 1				
			now select multip e. Learn more of	le zones. Sele	ecting mu	Itiple zones will create one VM
Security type ①		Standard	Standard			
Image * ①		O Debian 11 "Bullseye" - x64 Gen2				
		See all ima	ges Configure VM	generation		

VM architecture ①	O Arm64				
	● x64				
	Arm64 is not supported with the selected image.				
Run with Azure Spot discount 💿					
Size * ①	Standard_B4ms - 4 vcpus, 16 Gi8 memory (\$121.18/month)	~			
	See all sizes				
Enable Hibernation (preview) 🛈					
	Hibernate is not supported by the size that you have selected. Choose a compatible with Hibernate to enable this feature. <u>learn more</u> of	size that is			
Administrator account					
Authentication type ①	 SSH public key 				
	Password				
	 Azure now automatically generates an SSH key pair for you and allow store it for future use. It is a fast, simple, and secure way to connect to virtual machine. 				
Username * ③	tpot_user	-			
	Figure 1 and	~			
SSH public key source	Generate new key pair				
	Generate new key pair TP-VM_key	7			
Key pair name *	Secretario de la constitución de	V			
Key pair name * Inbound port rules Select which virtual machine netwo	TP-VM_key rk ports are accessible from the public internet. You can specify more limited or	granular			
Key pair name * Inbound port rules Select which virtual machine network access on the Networking	TP-VM_key rk ports are accessible from the public internet. You can specify more limited or	granular			
Key pair name * Inbound port rules Select which virtual machine network access on the Networking	TP-VM_key rk ports are accessible from the public internet. You can specify more limited or tab.	granular			
SSH public key source Key pair name * Inbound port rules Select which virtual machine netwo network access on the Networking Public inbound ports * Select inbound ports *	TP-VM_key rik ports are accessible from the public internet. You can specify more limited or tab. None	granular			

Disk and Networking

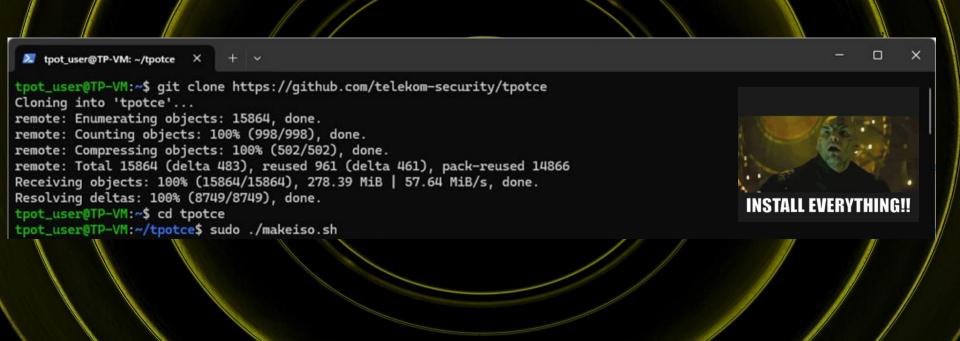
Basics Disks Networking I	Management Monitoring Advanced Tags Review + create	Basics Disks Networking	Management Monitoring Advanced Tags Review + create		
▲ The desired performance might no machine size supports up to 37 M	ot be reached due to the maximum virtual machine disk performance cap. The current virtual Bps. The total for disks attached to "TP-VM" is 100 MBps. <u>Learn more</u> of		virtual machine by configuring network interface card (NIC) settings. You can control ports, with security group rules, or place behind an existing load balancing solution.		
		Network interface			
	disk and a temporary disk for short-term storage. You can attach additional data disks. e of storage you can use and the number of data disks allowed. Learn more of	When creating a virtual machine, a ne	etwork interface will be created for you.		
VM disk encryption		Virtual network * ⊙	(new) TP-VM-vnet		
Azure disk storage encryption automat default when persisting it to the cloud.	ically encrypts your data stored on Azure managed disks (OS and data disks) at rest by	Subnet * ⊙	Create new (new) default (10.1.0.0/24)		
Encryption at host ⊙		Public IP ①	(new) TP-VM-ip		
Encryption at host (c)		Public IP ()	Create new		
	 Encryption at host is not registered for the selected subscription. Learn more about enabling this feature (5° 	NIC network security group ①	None		
	SACTION SHOCK STREET GUILLE SACKS	The factority group (Basic		
2200			O Advanced		
OS disk			None		
OS disk size ③	128 GiB (P10)	Public inbound ports * ①	Allow selected ports		
	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 YM. of	Select inbound ports *	This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules I limit inbound traffic to known IP addresses.		
OS disk type * ①	Premium SSD (locally-redundant storage)		Create rates to minist inducated trains, to known in adultesses.		
Delete with VM ()		Delete public IP and NIC when VM is deleted ①			
Key management ①	Platform-managed key	Enable accelerated networking ①			
Enable Ultra Disk compatibility ①		2	The selected VM size does not support accelerated networking.		
		Load balancing			
Data disks for TP-VM		You can place this virtual machine in t	the backend pool of an existing Azure load balancing solution. Learn more ೆ		
You can add and configure additional of temporary disk.	data disks for your virtual machine or attach existing disks. This VM also comes with a	Load balancing options ①	None		
LUN Name	Size (GiB) Disk type Host caching Delete with VM ①		 Azure load balancer Supports all TCP/UDP network traffic, port-forwarding, and outbound flows. 		
Create and attach a new disk Attac	th an existing disk		 Application gateway Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall. 		

Net_Sec Group and Preparing for Install









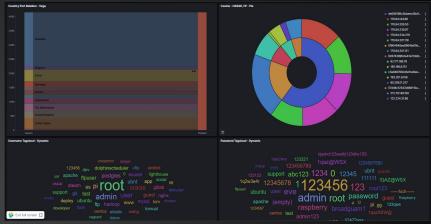
User Install Method

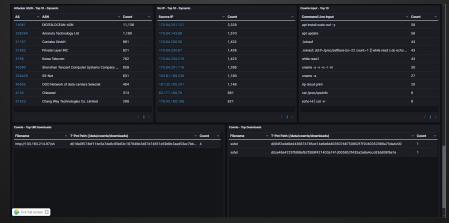


(If you have Debian already Installed)

Elasticvue/Kibana







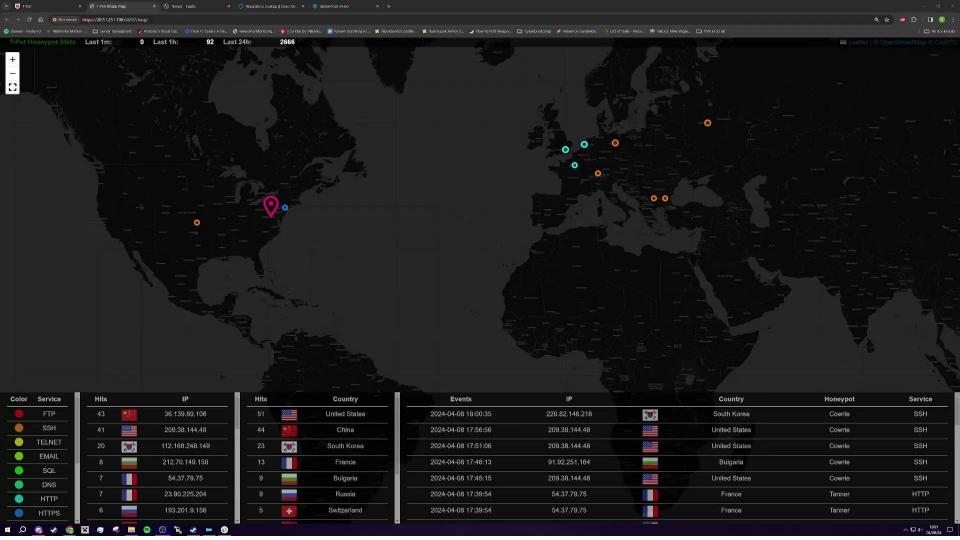
Honeypot Demonstration: Cowrie Vulnerability: Ports 22 and 23 Mike Staples



Honeypot Demonstration: Tanner

Vulnerability: HTTP

Nathan Almeida



Legal/Ethical Implications

Entrapment

- Despite the controversy, Honeypots are not a form of entrapment
- Honeypots don't induce anyone

Privacy

- Federal Wiretap Act
- Exemption under Service Provider Protection

Liability

- Liability implies you could be sued if your honeypot is used to harm others.
- Civil issue

Resources

T-Pot/tpotce

https://github.com/telekom-security/tpotce?tab=readme-ov-file#ssh-and-cockpit