BsidesBHAM

Honey Dripping from the Cloud

Attacking and Defending Cloud Infrastructure

Hrushikesh Kakade | Kumar **Ashwin**

About Us

Hrushikesh Kakade (Security Engineer @ MPL)

- Cloud & Cloud Native Security
- Application Security
- DevSecOps
- Twitter Handle: @hkh4cks

Kumar **Ashwin** (Security Consultant @ Payatu)

- Cloud Security
- Web Security
- DevSecOps
- Twitter Handle: @0xCardinal

What are we going to cover?

- ➔ Common Misconfigurations In Cloud
- ➔ Defensive Techniques To Secure Cloud Infrastructure
- ➔ What Are “Honeypots”?
- ➔ How HoneyPots Can Be Helpful?
- ➔ Different Implementation Techniques
- ➔ Demo
- ➔ QnA?

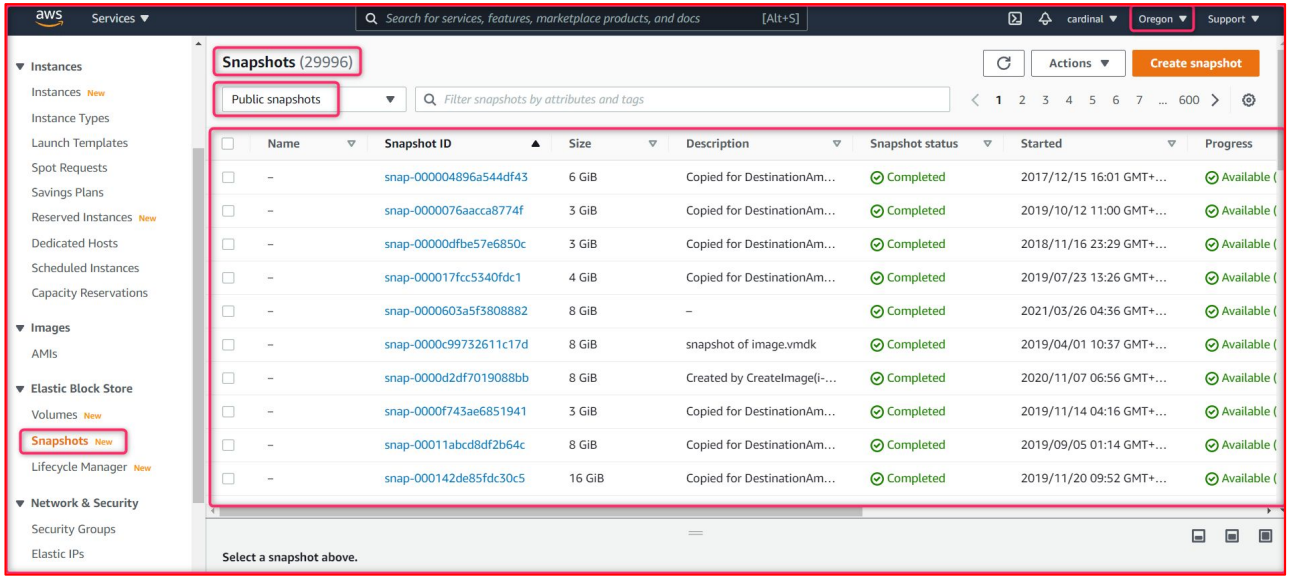
Common Misconfigurations In Cloud

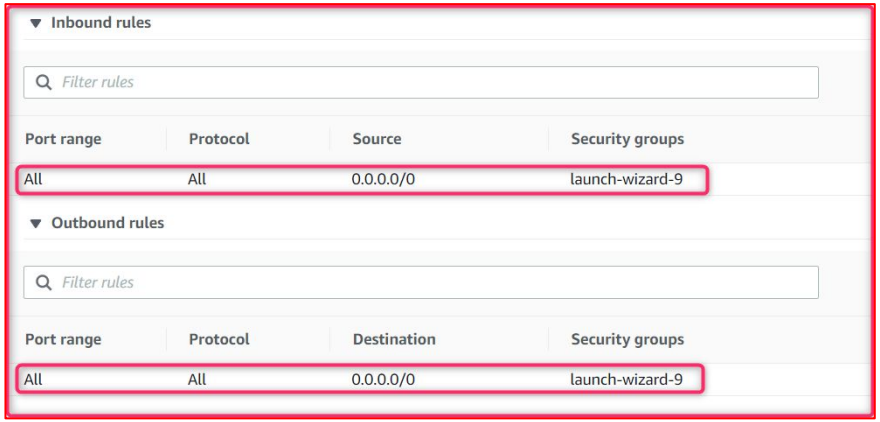
- ➔ EC2 Instance Misconfiguration
- ➔ S3 Misconfiguration
- ➔ Misconfigured Security Groups
- ➔ Bad AWS IAM Policies

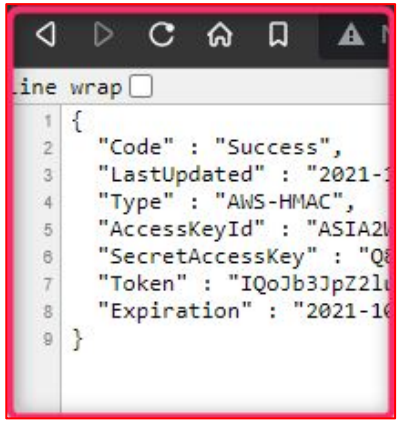
EC2 Instance Misconfiguration

- ➔ Public Snapshots
- ➔ Vulnerable Web Apps Hosted on EC2 leading to SSRF
- ➔ Firewall Misconfiguration

Examples


Services
Search for services, features, marketplace products, and docs [Alt+S]
cardinal
Oregon
Support
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Images
AMIs
Elastic Block Store
Volumes New
Snapshots New
Lifecycle Manager New
Network & Security
Security Groups
Elastic IPs
Snapshots (29996)
Actions
Create snapshot
Public snapshots
Filter snapshots by attributes and tags
1 2 3 4 5 6 7 ... 600
Name
Snapshot ID
Size
Description
Snapshot status
Started
Progress
snap-000004896a544df43 6 GiB Copied for DestinationAm... Completed 2017/12/15 16:01 GMT+... Available
snap-0000076aacca8774f 3 GiB Copied for DestinationAm... Completed 2019/10/12 11:00 GMT+... Available
snap-00000dfbe57e6850c 3 GiB Copied for DestinationAm... Completed 2018/11/16 23:29 GMT+... Available
snap-000017fcc5340fdc1 4 GiB Copied for DestinationAm... Completed 2019/07/23 13:26 GMT+... Available
snap-0000603a5f3808882 8 GiB – Completed 2021/03/26 04:36 GMT+... Available
snap-0000c99732611c17d 8 GiB snapshot of image.vmdk Completed 2019/04/01 10:37 GMT+... Available
snap-0000d2df7019088bb 8 GiB Created by CreateImage(i-... Completed 2020/11/07 06:56 GMT+... Available
snap-0000f743ae6851941 3 GiB Copied for DestinationAm... Completed 2019/11/14 04:16 GMT+... Available
snap-00011abcd8df2b64c 8 GiB Copied for DestinationAm... Completed 2019/09/05 01:14 GMT+... Available
snap-000142de85fdc30c5 16 GiB Copied for DestinationAm... Completed 2019/11/20 09:52 GMT+... Available
Select a snapshot above.


Inbound rules
Filter rules
Port range
Protocol
Source
Security groups
All
All
0.0.0.0/0
launch-wizard-9
Outbound rules
Filter rules
Port range
Protocol
Destination
Security groups
All
All
0.0.0.0/0
launch-wizard-9


ine wrap
{
"Code" : "Success",
"LastUpdated" : "2021-
"Type" : "AWS-HMAC",
"AccessKeyId" : "ASIA2
"SecretAccessKey" : "Q
"Token" : "IQoJb3JpZ2l
"Expiration" : "2021-1
}

S3 Misconfiguration

- ➔ Defining “Full Control” access to Authenticated AWS Users.
- ➔ Enabling “write” access to “Everyone” group.
- ➔ Misconfiguring object and bucket ACLs.
- ➔ And many more...

https://hackerone.com/reports/998981
https://hackerone.com/reports/764243
https://blog.detectify.com/2017/07/13/aws-s3-misconfiguration-explained-fix/
https://labs.detectify.com/2017/07/13/a-deep-dive-into-aws-s3-access-controls-taking-full-control-over-your-assets/

Misconfigured Security Groups

➔ Security Groups are the virtual firewall for your AWS resources. It defines what comes in and what goes out.

➔ Over-exposure of your AWS resources.
➔ Exposing to all interfaces.
➔ If it works, don’t touch it.

Source: Google

Bad IAM Policies

➔ IAM policies are the objects when associated with the object, defines their permissions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

https://kloudle.com/blog/iam-bad-privilege-escalation-using-misconfigured-policies-in-aws-iam-webinar

Defence Against

Common Misconfigurations In Cloud

Responsibility Matrix

Responsibilities	On-prem	IaaS	CaaS	PaaS	FaaS	SaaS
All Things Client Side	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Data (Transit and Cloud)	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Identity & Access Management	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Functional Logic	Tenant	Tenant	Tenant	Tenant	Tenant	Provider
Applications	Tenant	Tenant	Tenant	Tenant	Provider	Provider
Runtime	Tenant	Tenant	Tenant	Provider	Provider	Provider
Middleware	Tenant	Tenant	Provider	Provider	Provider	Provider
OS	Tenant	Tenant	Provider	Provider	Provider	Provider
Virtualization	Tenant	Provider	Provider	Provider	Provider	Provider
Load Balancing	Tenant	Provider	Provider	Provider	Provider	Provider
Networking	Tenant	Provider	Provider	Provider	Provider	Provider
Servers	Tenant	Provider	Provider	Provider	Provider	Provider
Physical Security	Tenant	Provider	Provider	Provider	Provider	Provider

Source: NotSoSecure

EC2 Instance Misconfiguration

- ➔ Keep a close look on the resources you own and what you make public
- ➔ Use IDMSv2 or Deny access to Metadata service
- ➔ Only allow the least that is required

https://blog.appsecco.com/server-side-request-forgery-ssrf-and-aws-ec2-instances-after-instance-meta-data-service-version-38fc1ba1a28a
https://summitroute.com/blog/2017/08/13/defensive_options_when_using_aws_iam_roles/

S3 Misconfiguration

- ➔ Define the least privileged access to the bucket and review those permissions on a regular basis across all buckets.
- ➔ Enable Encryption
- ➔ Enable Bucket Versioning
- ➔ Enable “Block Public Access” for buckets that should never be public
- ➔ Ensure the logging access is enabled to track access requests

https://medium.com/geekculture/defending-in-depth-s3-buckets-66883620ea4c

Misconfigured Security Groups

- ➔ Limit the ingress and egress rules
- ➔ Remove unused security groups

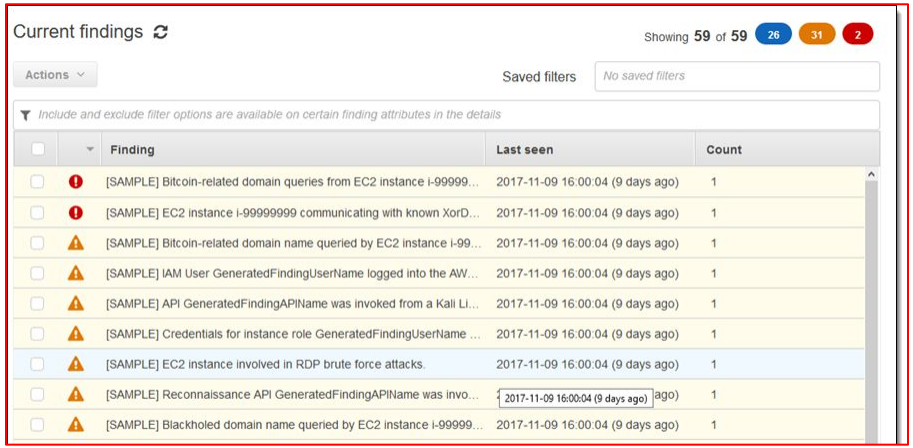
Bad IAM Policies

- ➔ Restrict access based on Condition Keys like SourceIp, SourceVpc, etc.
- ➔ Limit the AWS privileges granted

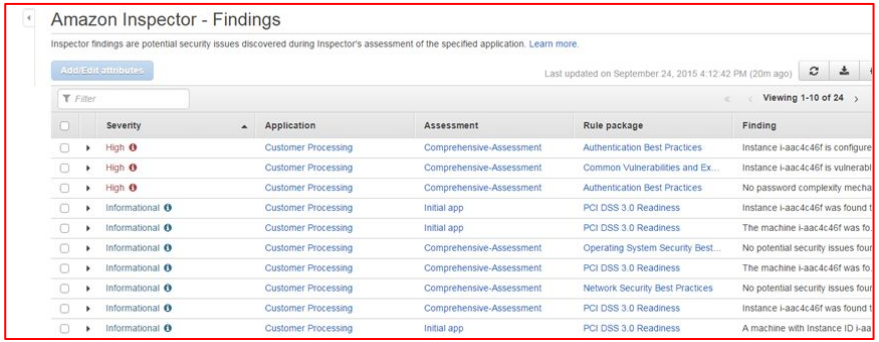
https://summitroute.com/blog/2017/08/13/defensive_options_when_using_aws_iam_roles/

AWS Services for Security

- ➔ GuardDuty
- ➔ Inspector
- ➔ Macie



GuardDuty



Inspector

Out Of The Box Security Strategies

Before getting into that - let’s understand **what are HoneyPots?**

What are HoneyPots?

“

Honeypots are decoy systems or servers deployed alongside production systems within your network. When deployed as enticing targets for attackers, honeypots can add security monitoring opportunities for blue teams and misdirect the adversary from their true target.

Source: Rapid7

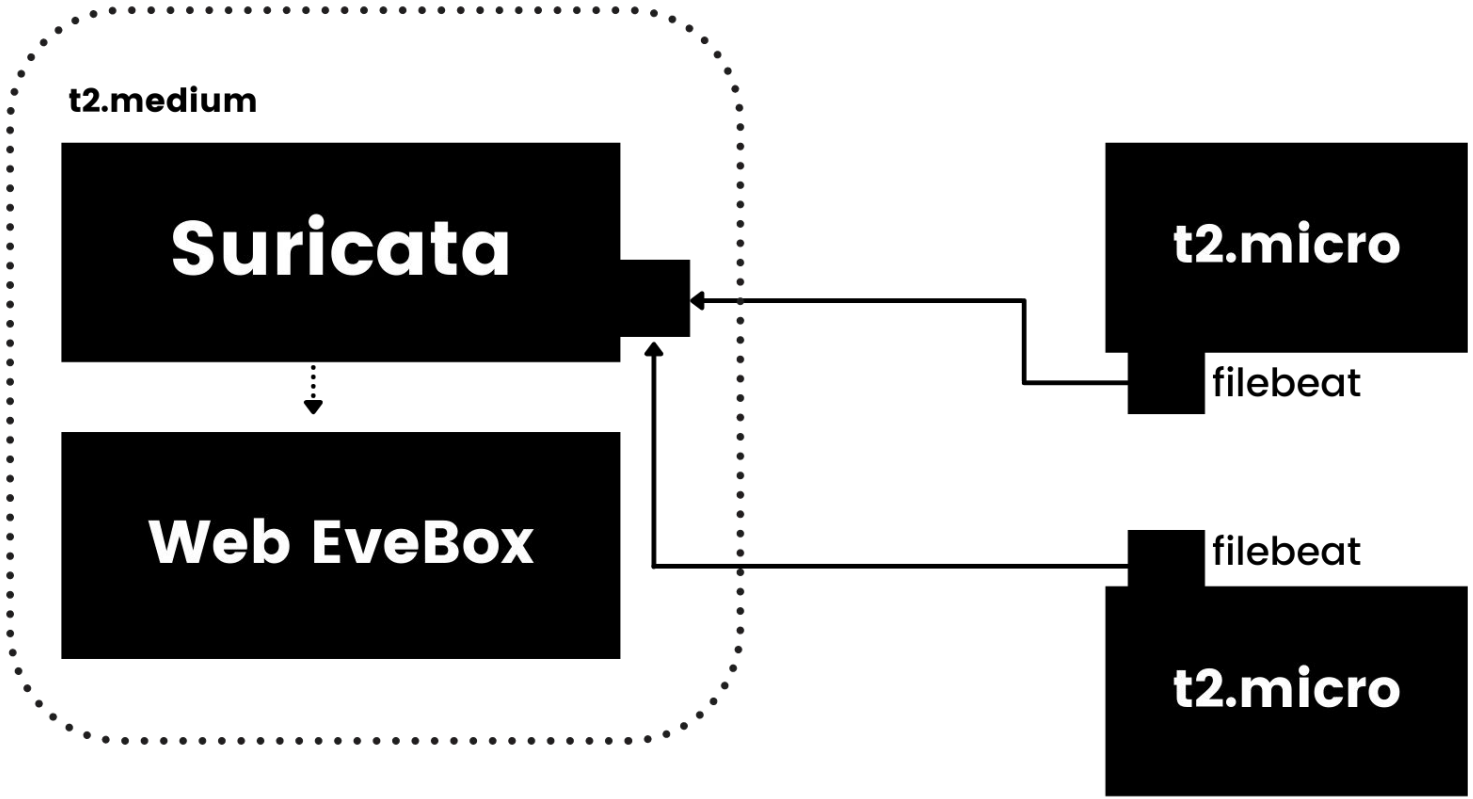
How can HoneyPots be helpful?

- ➔ They break the attacker kill chain and slow attackers down.
- ➔ They are straightforward and low-maintenance
- ➔ They help you test your incident response processes

Out Of The Box Security Strategies

- ➔ HoneyPots have been seen to have high benefits in the on-prem infrastructure, so why not implement those on the cloud.
- ➔ Fo doing so, we have different strategies that we can implement.
- ➔ Deployment of honeypots is highly based on creativity and requirement.
- ➔ But more than that it is based on constant logging and monitoring.

Demo


t2.medium
Suricata
Web EveBox
t2.micro
filebeat
filebeat
t2.micro

Questions?

Thanks BsidesBHAM! :)

0xCardinal - Kumar **Ashwin** | hkh4cks - **Hrushikesh** Kakade