DEVSECOPS BOOTCAMP

BUILDING RUGGED SOFTWARE

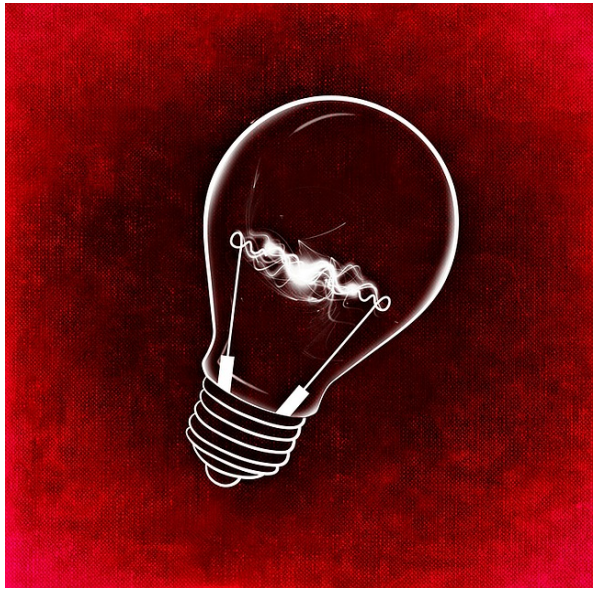
YEAR ONE / WEEK SEVEN / LESSON ONE

Agenda

- Incident Response
- Issues
- Gathering Data
- Forensics Account
- Instances
- ELBs
- Lab 1

Incident Response

- Something bad happened last week
- How do we know that the account is safe?
- How do we determine how the attacker was able to compromise the system/account?
- Don’t shut down instances
- Incident Response Role



Issues With Cloud Forensics

- No access to underlying infrastructure
- No easy way to dump system memory
- No traditional firewall logs
- No ability to perform real write blocked forensic imaging

Gathering Forensics Configuration

- Can be done using AWS CLI
- Need to enumerate all of the calls you need to make
- The more data you can gather the better
- Make sure you store the Metadata in another secure account (Forensics Account)
- Better to script it out for reproducibility

Forensics Account

- Account only used for investigation
- Best practice is to allow limited access
- Analysis should be done on copies of snapshots from the compromised account
- Get ready for some potentially large storage costs

EC2 Forensics Configuration

aws ec2 describe-instances

- You should dump **all** of the data
- Includes
  - Owner
  - ReservationID
  - Instances
  - State
  - PublicDNS
  - Lots more
- http://docs.aws.amazon.com/cli/latest/reference/ec2/describe-instances.html


```
{
    "OwnerId": "xxxxxxxxxxxx",
    "ReservationId": "r-xxxxxxxx",
    "Groups": [],
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-x-x-x-x.us-west-2.compute.amazonaws.com",
            "RootDeviceType": "ebs",
            "State": {
                "Code": 80,
                "Name": "stopped"
            },
            "EbsOptimized": false,
            "LaunchTime": "2016-06-29T17:51:57.000Z",
            "PublicIpAddress": "x.x.x.x",
            "PrivateIpAddress": "x.x.x.x",
            "ProductCodes": [],
            "VpcId": "vpc-xxxxxxxx",
            "StateTransitionReason": "User initiated (2016-07-01 04:02:35 GMT)",
            "InstanceId": "i-xxxxxxxx",
            "ImageId": "ami-xxxxxxxx",
            "PrivateDnsName": "ip-x-x-x-x.us-west-2.compute.internal",
            "KeyName": "xxxxxx",
            "SecurityGroups": [
                {
                    "GroupName": "all ports",
                    "GroupId": "sg-xxxxxxxx"
                },
                {
                    "GroupName": "jenkins",
                    "GroupId": "sg-xxxxxxxx"
                },
                {
                    "GroupName": "student1-app",
                    "GroupId": "sg-xxxxxxxx"
                }
```

ELB Forensics Configuration

aws elb describe-load-balancers

- You should dump **all** of the data
- Includes
  - Subnets
  - Listener Descriptons
  - Health Checks
  - VPC ID
  - And lots more
- http://docs.aws.amazon.com/cli/latest/reference/elb/describe-load-balancers.html


```
{
    "LoadBalancerDescriptions": [
        {
            "Subnets": [
                "subnet-xxxxxxxx"
            ],
            "CanonicalHostedZoneNameID": "xxxxxxxx",
            "CanonicalHostedZoneName": "xxxxxxxx.us-west-2.elb.amazonaws.com",
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 8080,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            "HealthCheck": {
                "HealthyThreshold": 9,
                "Interval": 30,
                "Target": "TCP:8080",
                "Timeout": 5,
                "UnhealthyThreshold": 2
            },
            "VPCId": "vpc-xxxxxxxx",
            "BackendServerDescriptions": [],
            "Instances": [
                {
                    "InstanceId": "i-xxxxxxxx"
                }
            ],
            "DNSName": "xxxxxxxx.elb.amazonaws.com",
            "SecurityGroups": [
                "sg-xxxxxxxx",
                "sg-xxxxxxxx"
            ],
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": []
            },
            "LoadBalancerName": "xxxxxxxx",
            "CreatedTime": "2016-06-24T17:34:54.670Z",
            "AvailabilityZones": [
                "us-west-2b"
            ],
```

Lab 1 Gathering Data by Hand

- https://github.com/devsecops/bootcamp/blob/master/Week-7/labs/LAB-1.md