Mick O'Hanlon
Week 9 Homework Report
mjo4rk

Milestone 1: Create MHN Admin VM

- Created firewall to allow ingress traffic on ports 3000 and 10000

```
Your active configuration is: [default]
Micks-Air:~ mickohanlon$ gcloud beta compute firewall-rules create mhn-allow-adm
in --direction=INGRESS --priority=1000 --network=default --action=ALLOW --rules=
tcp:3000,tcp:10000 --source-ranges=0.0.0.0/0 --target-tags=mhn-admin
You do not currently have this command group installed.  Using it
requires the installation of components: [beta]


Your current Cloud SDK version is: 224.0.0
Installing components from version: 224.0.0

These components will be installed.
```

Name	Version	Size
gcloud Beta Commands	2018.07.16	< 1 MiB

- Internal and external IP:

```
NAME       ZONE           MACHINE_TYPE  PREEMPTIBLE  INTERNAL_IP  EXTERNAL_IP     STATUS
mhn-admin  us-central1-c  f1-micro                   10.128.0.2   35.232.251.199  RUNNING
Micks-Air:~ mickohanlon$
```

- Establish SSH Access:

```
SHA256:aRq26ihoo5rEodDLcGgnMCbf21eJLZ+sdl49c
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|                 |
|+.               |
|+= .     + .     |
|+++.. o S +      |
|=++. + =.= . .   |
|ooo . + .o+ . o  |
|++ . . ...++ . . |
|B.o.o  .o**oE    |
+----[SHA256]-----+
Updating project ssh metadata...⠛
```

Milestone 2: Install the MHN Admin Application

- Update apt

```
Get:23 http://us-central1.gce.archive.ubuntu.com trusty-backports/main Translation-en [
Get:24 http://us-central1.gce.archive.ubuntu.com trusty-backports/multiverse Translatio
Get:25 http://us-central1.gce.archive.ubuntu.com trusty-backports/restricted Translatio
Get:26 http://us-central1.gce.archive.ubuntu.com trusty-backports/universe Translation-
Get:27 http://us-central1.gce.archive.ubuntu.com trusty/main Sources [1,064 kB]
Get:28 http://us-central1.gce.archive.ubuntu.com trusty/restricted Sources [5,433 B]
Get:29 http://us-central1.gce.archive.ubuntu.com trusty/universe Sources [6,399 kB]
Get:30 http://archive.canonical.com trusty Release.gpg [916 B]
Get:31 http://archive.canonical.com trusty Release [9,359 B]
Get:32 http://us-central1.gce.archive.ubuntu.com trusty/multiverse Sources [174 kB]
Get:33 http://archive.canonical.com trusty/partner amd64 Packages [5,349 B]
Hit http://us-central1.gce.archive.ubuntu.com trusty/main amd64 Packages
Hit http://us-central1.gce.archive.ubuntu.com trusty/restricted amd64 Packages
Hit http://us-central1.gce.archive.ubuntu.com trusty/universe amd64 Packages
Hit http://us-central1.gce.archive.ubuntu.com trusty/multiverse amd64 Packages
Hit http://us-central1.gce.archive.ubuntu.com trusty/main Translation-en
Hit http://us-central1.gce.archive.ubuntu.com trusty/multiverse Translation-en
Hit http://us-central1.gce.archive.ubuntu.com trusty/restricted Translation-en
Get:34 http://security.ubuntu.com trusty-security InRelease [65.9 kB]
Hit http://us-central1.gce.archive.ubuntu.com trusty/universe Translation-en
Get:35 http://archive.canonical.com trusty/partner Translation-en [4,207 B]
Ign http://us-central1.gce.archive.ubuntu.com trusty/main Translation-en_US
Ign http://us-central1.gce.archive.ubuntu.com trusty/multiverse Translation-en_US
Ign http://us-central1.gce.archive.ubuntu.com trusty/restricted Translation-en_US
Ign http://us-central1.gce.archive.ubuntu.com trusty/universe Translation-en_US
Get:36 http://security.ubuntu.com trusty-security/main Sources [166 kB]
Get:37 http://security.ubuntu.com trusty-security/universe Sources [92.7 kB]
```

- Install get

```
Get:1 http://us-central1.gce.archive.ubuntu.co
Get:2 http://us-central1.gce.archive.ubuntu.co
Get:3 http://us-central1.gce.archive.ubuntu.co
Fetched 3,054 kB in 0s (41.2 MB/s)
Selecting previously unselected package liberr
(Reading database ... 42034 files and director
Preparing to unpack .../liberror-perl_0.17-1.1
Unpacking liberror-perl (0.17-1.1) ...
Selecting previously unselected package git-ma
Preparing to unpack .../git-man_1%3a1.9.1-1ubu
Unpacking git-man (1:1.9.1-1ubuntu0.9) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a1.9.1-1ubuntu0
Unpacking git (1:1.9.1-1ubuntu0.9) ...
Processing triggers for man-db (2.6.7.1-1ubunt
Setting up liberror-perl (0.17-1.1) ...
Setting up git-man (1:1.9.1-1ubuntu0.9) ...
Setting up git (1:1.9.1-1ubuntu0.9) ...
```

- Start script running

```
Ign http://us-central1.gce.archive.ubuntu.com trusty/multiverse Translation
Ign http://us-central1.gce.archive.ubuntu.com trusty/restricted Translation
Ign http://us-central1.gce.archive.ubuntu.com trusty/universe Translation-e
Hit http://security.ubuntu.com trusty-security/universe Sources
Hit http://archive.canonical.com trusty/partner amd64 Packages
Hit http://security.ubuntu.com trusty-security/main amd64 Packages
Hit http://archive.canonical.com trusty/partner Translation-en
Hit http://security.ubuntu.com trusty-security/universe amd64 Packages
Hit http://security.ubuntu.com trusty-security/main Translation-en
Hit http://security.ubuntu.com trusty-security/universe Translation-en
```

- Error with logging into Github on the terminal.

```
remote: Repository not found.
fatal: repository 'https://github.com/HurricaneLabs/pyev.git/' not found
Command "git clone -q https://github.com/HurricaneLabs/pyev.git /opt/hpfeeds/env/src/pyev" failed with error code 128 in None
mickohanlon@mhn-admin:/opt/mhn$
```

Milestone 3: Create a MHN Honeypot VM

- Create firewall rule

```
mickohanlon@mhn-admin:/opt/mhn$ gcloud beta compute firewall-rules create mhn-allow-honeypot --direction=INGRESS --priority=1000 --network=d
efault --action=ALLOW --rules=all --source-ranges=0.0.0.0/0 --target-tags=mhn-honeypot
Creating firewall...
.....
```

Create VM for honeypot:

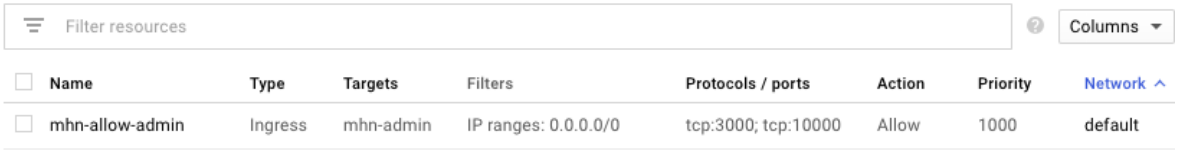
```
mickohanlon@mhn-admin:/opt/mhn$ gcloud compute instances create "mhn-honeypot-1" --machine-type "f1-micro" --subnet "default" --maintenance-
policy "MIGRATE"  --scopes "https://www.googleapis.com/auth/devstorage.read_only","https://www.googleapis.com/auth/logging.write","https://w
ww.googleapis.com/auth/monitoring.write","https://www.googleapis.com/auth/servicecontrol","https://www.googleapis.com/auth/service.managemen
t.readonly","https://www.googleapis.com/auth/trace.append" --tags "mhn-honeypot","http-server" --image "ubuntu-1404-trusty-v20171010" --imag
e-project "ubuntu-os-cloud" --boot-disk-size "10" --boot-disk-type "pd-standard" --boot-disk-device-name "mhn-honeypot-1"
```

SSH to VM:

```
mickohanlon@mhn-admin:/opt/mhn$ gcloud compute ssh mhn-honeypot-1
WARNING: The public SSH key file for gcloud does not exist.
WARNING: The private SSH key file for gcloud does not exist.
WARNING: You do not have an SSH key for gcloud.
WARNING: SSH keygen will be executed to generate a key.
Generating public/private rsa key pair.
Your identification has been saved in /home/mickohanlon/.ssh/google_compute_engine.
Your public key has been saved in /home/mickohanlon/.ssh/google_compute_engine.pub.
The key fingerprint is:
68:91:e6:ac:65:da:c9:ab:70:c6:a9:2e:6e:30:52:22 mickohanlon@mhn-admin
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|       .         |
|      +          |
|E .  + o         |
|.o    B S        |
|+  . X .         |
|o.. B +          |
|.. =   .         |
|o+o ...          |
+-----------------+
```

Milestone 4: Install the Honeypot Application

- Firewall is set up:



- Deployed script

- New honeypot under sensors tab

Milestone 5: Attack!

- Ran into a problem installing nmap

References