```
export PATH=$PATH:/usr/local/bin:/usr/sbin:/root/.local/
bin
sudo yum update -y
sudo yum install nmap git python3 -y
sudo yum install gcc -y
sudo yum install glib2-devel -y
sudo yum install bind-utils wget unzip -y
sudo yum install cmake openssl-devel -y
sudo yum install cmake libX11-devel -y
sudo yum install cmake libXtst-devel -y
sudo yum install cmake libXinerama-devel -y
sudo yum install cmake libusb-static -y
sudo yum install cmake libusbmuxd-devel -y
sudo yum install cmake libusbx-devel -y
sudo yum install cmake libusb-devel -y
sudo yum update && sudo yum install python3-pip
sudo yum install doxygen -y
sudo yum install gcc-c++ -y
pip3 install paramiko

TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/
token" -H "X-aws-ec2-metadata-token-ttl-seconds:
21600"`
export privateIP=`curl -H "X-aws-ec2-metadata-token:
$TOKEN" -v http://169.254.169.254/latest/meta-data/
local-ipv4`
curl -L https://raw.githubusercontent.com/awslabs/
amazon-guardduty-tester/master/guardduty_tester.sh > /
home/ec2-user/guardduty_tester.sh

mkdir /home/ec2-user/compromised_keys
mkdir /home/ec2-user/domains
```

```
mkdir /home/ec2-user/passwords

curl -L https://raw.githubusercontent.com/awslabs/
amazon-guardduty-tester/master/artifacts/queries.txt > /
home/ec2-user/domains/queries.txt
curl -L https://raw.githubusercontent.com/awslabs/
amazon-guardduty-tester/master/artifacts/
password_list.txt > /home/ec2-user/passwords/
password_list.txt
curl -L https://raw.githubusercontent.com/awslabs/
amazon-guardduty-tester/master/artifacts/
never_used_sample_key.foo > /home/ec2-user/
compromised_keys/compromised.pem

FILE="/home/ec2-user/compromised_keys/
compromised.pem"

for FILE in {1..20}; do cp /home/ec2-user/
compromised_keys/compromised.pem /home/ec2-user/
compromised_keys/compromised$FILE.pem; done

curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://
169.254.169.254/latest/meta-data/instance-id  >> /
home/ec2-user/localIps.sh
curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://
169.254.169.254/latest/meta-data/local-ipv4 >> /home/
ec2-user/localIps.sh

pip3 install cmake
wget https://github.com/vanhauser-thc/thc-hydra/
archive/refs/tags/v9.4.zip -P /home/ec2-user
wget -q -O /home/ec2-user/libssh.tar.xz https://
```

```
www.libssh.org/files/0.9/libssh-0.9.4.tar.xz
tar -xvf /home/ec2-user/libssh.tar.xz

cd /home/ec2-user/libssh-0.9.4
mkdir build
cd build

cmake -DUNIT_TESTING=OFF
-DCMAKE_INSTALL_PREFIX=/usr
-DCMAKE_BUILD_TYPE=Release ..

sudo make && sudo make install

cd /home/ec2-user
unzip v9.4.zip
cd /home/ec2-user/thc-hydra-9.4
/home/ec2-user/thc-hydra-9.4/configure

sudo make

sudo make install

git clone https://github.com/galkan/crowbar /home/ec2-
user/crowbar

sudo chown -R ec2-user: /home/ec2-user
sudo chmod +x /home/ec2-user/guardduty_tester.sh
sudo chmod +x /home/ec2-user/crowbar/crowbar.py

cd /home/ec2-user

wget https://secure.eicar.org/eicar.com
```

```
wget https://secure.eicar.org/eicar.com.txt
wget https://secure.eicar.org/eicar_com.zip
wget https://secure.eicar.org/eicarcom2.zip



sudo curl -s http://pool.minergate.com/
dkjdjkjdlsajdkljalsskajdksakjdksajkllalkdjsalkjdsalkjdlkasj
> /dev/null &
sudo curl -s http://xmr.pool.minergate.com/
dhdhjkhdjkhdjkhajkhdjskahhjkhjkahdsjkakjasdhkjahdjk
> /dev/null &
sudo dig -f ./domains/queries.txt > /dev/null &
sudo dig GuardDutyC2ActivityB.com any
```