In-class Practice 2: Detecting SQLMAP Scanning with SNORT

Description

In this practice, you are going to run sqlmap on the Kali VM to scan SQL Injection vulnerabilities in the WebGoat web server. Then you will need to create a snort rule to run in the web server to detect the scanning behavior.

Part 1: Configure and start the networks as required by the pre-class practice

Details omitted

Part 2: Monitor traffic to the web server on the router VM

Run the following commands in the terminal of the router VM:

```
tcpdump -s 0 -A -vvvv -n 'port 8000'  | grep -i password
```

Why we do this: by doing so, we can monitor the POST requests sent from Kali to the web server, so that we can learn what sqlmap attempts to do

Part 3: Run sqlmap on the Kali VM to scan SQL Injection vulnerabilities

Make sure your WebGoat web server is running and can be accessed from the Kali VM

Then run the following command on the terminal of Kali VM:

```
sqlmap -u http://10.0.2.4:8000/WebGoat/login --data "username=admin&password=admin"  --method POST
```

Give the following answers to the prompted questions:

N
N
N
…

Check the traffic captured at Part 2 (on the router VM) and pay attention to the values in the fields of "username" and "password"

Part 4: Run SNORT on the webserver to detect sqlmap scanning actions

- Step 1: Install snort on the WebGoat VM by running the following:

  ```
  sudo apt update [ignore the errors if you see any]
  sudo apt-get install snort
  ```

- Step 2: When you are asked for network interfaces, input: `enp0s3`

- Step 3: Stop snort and switch to root:

  ```
  sudo systemctl stop snort
  sudo su -
  ```

- **Step 4: Design your snort rules based on observations on the values set by sqlmap for "username" and "password" [sorry, no guidance here]**

- Step 5: Add your snort rules to the configuration file:

  ```
  cd /etc/snort/rules
  ```

  Open "local.rules", do some editing …. close the file

- Step 6: Disable the default snort rules:

  ```
  cd /etc/snort
  ```

  Open "snort.conf" [needs to be "root"]

  Find the line "include $RULE_PATH/local.rules", comment out all the follow-up "include" statements except for the last one (i.e., do not comment out "include threshold.conf" at the end of the file)

Close the file

- Step 7: Start snort:

```
snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i enp0s3
```

- Step 8: Run sqlmap on Kali again

Submission:

Prepare a PDF document to include:

- The snort rules you created for this practice
- Screenshots of the snort output when you launch sqlmap scanning
- Upload your PDF to Gradescope