CYBR371: System and Network Security
2024– T1

Arman Khouzani, Mohammad Nekooei

Lab 5: Intrusion Detection Systems (4%)

Submission Deadline: ***23:59:00 (NZST) on Sunday, 26 May 2024***

Question:	1	2	3	4	5	6	Total
Points:	6	4	6	12	8	4	40
Score:							

1 IDS alerts

Complete the following labs on **`netlab`** (access them through **`Nuku`**, under **`modules`**) and answer the questions accordingly:

- **Identifying and Analyzing NHIDS Alerts**

Q.1. [6 points] Describe the columns in the **`Sguil`**. Do this by choosing one event log (of your choice), i.e., one row, explain the information in each column, along with the value for that example event.

Q.2. [4 points] In **`Sguil`**, choose one event of your choice, find out the rule responsible for creating that alert, then explain why that rule was triggered for that event.

Q.3. [6 points] (a) Repeat the first question now with **`Squert`**.

(b) Compare and contrast the kind of information that **`Squert`** provides versus **`Sguil`**. In particular, is there any information that one provides and not the other?

— Once you complete the labs, please free up the Netlab pod by ending the reservation.

2 IDS evasion

Complete the following labs on **`netlab`** (access them through **`Nuku`**, under **`modules`**) and answer the questions accordingly:

- **Evading IDS**

Q.4. There are 3 IDS evasion techniques presented in this lab:

- Low MTU Scan
- Decoy Scan
- Spoofed MAC scan

(a) [4 points] Provide the **`nmap`** command that corresponds to the first technique (Low MTU scan – hint: remember what happens to packets that are bigger in size than the MTU! – Describe the command in simple words (what does it do). Finally, explain in simple terms how this achieves the IDS evasion.

(b) [4 points] Evaluate the success of the "Low MTU scan" (in the previous part) in evading the NIDSs by comparing its effect on the NIDS logs compared with a simple **`nmap`** scan.

(c) [4 points] Describe the **`nmap`** command that was used for the "Decoy scan" method in simple words, i.e., explain what the command does in simple English.

3 Tripwire HIDS

Complete the following labs on **`netlab`** (access them through **`Nuku`**, under **`modules`**) and answer the questions accordingly:

- **Tripwire Host Based Intrusion Detection System**

Q.5. (a) [4 points] Create a directory **`/opt/cybr371`**. Then add a rule to the tripwire's policy file that watches the integrity of this directory, i.e., generates an alert if something is changed in that directory. Provide the rule here.

(b) [4 points] Violate the integrity of the directory by creating a sub-directory inside it. Did tripwire produce an alert? If so provide the report here. If not, explain why it was not generated.

Q.6. [4 points] Can tripwire be used to create alerts when a file or directory is only accessed (is read) but not modified? If the answer is affirmative, provide an example rule, if the answer is negative, discuss an alternative.