TRENT UNIVERSITY
School of Computer Science

COIS 4370H – 2024WI **Computer & Info Security**

ASSIGNMENT 2
Assignment due date: Friday Mar. 8, 11:59pm

Total Marks: 150
- Written Response Questions: 60 marks
- Programming Questions" 90 marks

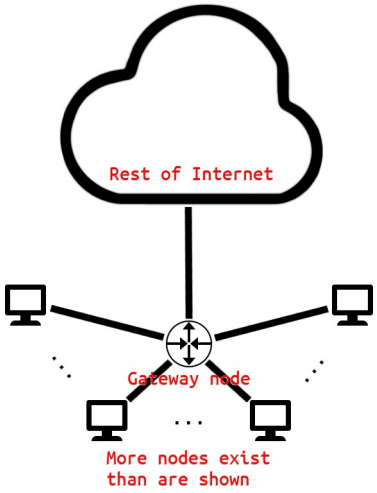
Written Response Questions (60 marks)

Note: Please ensure that written questions are answered using complete and grammatically correct sentences. You will be marked on the presentation and clarity of your answers as well as on the correctness of your answers.

By day, you, ORDINARY INDIVIDUAL, are an employee of a security consultancy firm which has just won a contract to test the security practices of a reasonably sized benevolent organization (that is, you're working as the organization's red team). By night, you are still that, but due to an insistence by the head of your firm to adopt codenames and metaphor to "keep up morale", you also have an alternate identity and role. You, PIQUANT MONGOOSE, are a high-ranking member of a secretive organization known only to outsiders as "UNSOCIETY" (actually, your firm, or even more specifically the members of your firm on the red team). Recently, you have established contact with an operative, DIFFIDENT MOLE, inside VILE CORP, a large company with dubious ethics that you want to expose and work to take down (in truth, the organization asking you to audit them). DIFFIDENT MOLE is a longtime employee who has had a change of heart (really, just their CISO). They want to walk away from the company and its actions and do something to impede it, but don't want to draw attention — legal or otherwise — to themselves. Despite the eyeroll-inducing nature of this imagining, you and your fellow employees humour the boss. It's a good gig, after all.

1. First, cast out the beam from your own eye (30 marks)

Before you can make any moves against VILE CORP, you must confirm your own resources will be secured against any unwelcome intrusion. After all, what would be more embarrassing than to be burned in the middle of your own operation? You collaborate with UNSOCIETY's head of network security (the firm's IT manager), ROBUST SPRINGBOK, to ensure your internal network is protected.



(14 marks) a. You and ROBUST SPRINGBOK decide you need to establish a firewall to protect your network from intrusion by external parties. Step-by-step, you will add rules below to meet the connectivity needs of UNSOCIETY and the least possibility connectivity beyond that. (**HINT:** CIDR Notation may be helpful for this portion of the assignment). The needs and reality of UNSOCIETY's network may be described as follows:

- UNSOCIETY controls 64 IP addresses with the prefix `72.36.115.128/26`.
- UNSOCIETY employs a star topology — all machines connect to each other, and the full internet, through one gateway node, located at `72.36.115.129`. (cf. diagram above) (This is where you will put the firewall).
- UNSOCIETY runs a server (located at `72.36.115.150`) that hosts its webpage (on the usual HTTPS port, `443`), which UNSOCIETY makes available to the full internet to proselytize its message (to advertise your firm, that is).
- ROBUST SPRINGBOK has noticed unusual activity coming out of St. Pierre & Miquelon (IP range `70.36.0.0/20`). While neither you nor ROBUST SPRINGBOK is sure, you think they may be trying to gain illicit access to the web server to shut it down.
- Secretly, UNSOCIETY receives funding by running a particularly lucrative game server for COMPETITIVE ONLINE GAME at `72.36.115.175`. For purposes of speed, COMPETITIVE ONLINE GAME uses UDP packets to communicate between servers and game clients; packets arrive and depart from port `4761` on the server, but clients may transmit from any port between `4700` and `4799`, inclusive.
- This same server secretly also hosts an IRC channel (on port `6667`). This channel is only for use by two parties — internal machines and DIFFIDENT MOLE from inside VILE CORP.
- IRC clients may use any port. IRC uses TCP connections. By default, IRC does not

use TLS or other forms of encryption for its connections.

- DIFFIDENT MOLE's machine uses the IP address `56.172.1.164`.

Below, you will add rules to accomplish UNSOCIETY's networking goals. Note that you may need more than one rule to accomplish the goal in question. Please specify rules to include the following information: DROP or ALLOW, source IP address, destination IP address, source port, destination port, TCP or UDP or BOTH. An example rule to allow members of UNSOCIETY to receive the result of DNS lookups from `1.1.1.1` might look like this (think carefully: would this rule be sufficient to make a DNS lookup to `1.1.1.1`?):

ALLOW `1.1.1.1` ==> `72.36.115.128/26` FROM PORT `53` TO `all` BY `UDP`

HINT: Ports may be specified as a range, or as sets, or as a singular value, or as '`all`'. IPs should be specified in CIDR notation for multiple, or as a singular value for one. You may assume that this firewall is stateful; it makes decisions about (TCP) connections, but once (TCP) connections are established, it does not interfere.

1. Agents trying to browse the web from the internal network may do so.
2. The full internet may access the UNSOCIETY webpage.
3. The full internet may access the COMPETITIVE ONLINE GAME server.
4. Agents trying to connect to the IRC channel may do so.
5. DIFFIDENT MOLE may connect to the IRC channel.
6. ROBUST SPRINGBOK would like to set up a honeypot on the web server to gain more information about the potential St. Pierre & Miquelon spies. After backing up the server onto another machine, another operative (OBSEQUIOUS AARDWOLF) has designed a program that looks like SSH, and which has designed vulnerabilities that potential spies could interact with and believe they have infiltrated the server. Only these potential spies should be able to see it, however. (The server otherwise has no SSH capabilities).
7. Handle traffic not specifically allowed by other rules.

(4 marks) b. You have reason to suspect one of your newer agents, GROUCHY PUMA (IP address `72.36.115.191`), may be compromised. You are concerned they may attempt to exfiltrate data on UNSOCIETY's operations; with the firewall configuration you created above, would it be possible for them to? Why or why not? If it is possible for them to exfiltrate data, design a rule to prevent them from doing so, and state where in the order of the rules above it should go.

(4 marks) c. Is a firewall sufficient to keep the IRC communication secret? Why or why not? If so, what, if any, additional configuration would be required to keep that communication secret? If not, what additional measures could you take?

(2 marks) d. You think back to your time and remember black hole attacks can be a threat to availability of web services. You want your website (and especially, your game server) to be available no matter what — does your firewall protect you from a black hole attack? Why or why not?

(2 marks) e. While black hole attacks are self-evidently a problem when a malicious entity drops

packets, is there any advantage gained by an adversary who uses the same technique to redirect packets through its network, but still otherwise routes them properly? Explain.

(4 marks) f. Name one advantage of the star topology network that UNSOCIETY uses. Name one disadvantage/potential improvement.

With your firewall in place, and a backchannel secured to communicate regularly with DIFFIDENT MOLE, you begin to reconnoiter VILE CORP.

2. She will win who, prepared herself, waits to take the enemy unprepared. (20 marks)

DIFFIDENT MOLE reports that VILE CORP uses the Bell-LaPadula Confidentiality Model in order to secure its documents. Their intel indicates that VILE CORP uses the following sensitivity/clearance levels:

$$\text{Executive} >_c \text{Management} >_c \text{Developer} >_c \text{Customer Support} >_c \text{Public}$$

Additionally, VILE CORP uses compartments for access control; compartments are characterized with Greek characters. For this part of the audit, DIFFIDENT MOLE instructs a lower-ranking member of the company (OBEISANT QUOKKA, your boss is quick to name them) to cooperate fully with your instructions, to test the resiliancy of their system against an insider threat. OBEISANT QUOKKA reveals that they hold (Management, $\{\varphi, \upsilon, \rho, \eta\}$) clearance.

(8 marks) a. For each of the following documents, report whether OBEISANT QUOKKA has read access, write access, both, or neither for that document in the Bell-LaPadula Confidentiality Model.

(i) D926: (Developer, $\{\varphi, \upsilon, \rho, \eta\}$)

(ii) D269: (Management, $\{\upsilon, \rho\}$)

(iii) D621: (Executive, $\{\varphi, \eta\}$)

(iv) D513: (Management, $\{\varphi, \upsilon, \rho, \eta\}$)

(v) D200: (Public, $\{e\}$)

(vi) D634: (Executive, $\{\varphi, \lambda, \upsilon, \rho, \eta, \psi\}$)

(vii) D364: (Customer Support, $\{\varphi, \rho\}$)

(viii) D818: (Developer, $\{\varphi, \eta, x\}$)

(12 marks b.) DIFFIDENT MOLE knows of a file that contains information they believe will be very valuable to UNSOCIETY's goals, D413 (Edited 2018-10-08) (~~Director~~ Executive, $\{\varphi, \upsilon, \rho, x\}$). DIFFIDENT MOLE reports that the file is protected under a dynamic Biba model that makes use of the low watermark property for both subject and object.

You want D413. You are going to try and reduce D413's integrity level so that OBEISANT

QUOKKA can give you the file without triggering alerts from a firewall or an intrusion detection system. There could be less contrived ways of getting the information in the file, but, admittedly, OBEISANT QUOKKA is not a technical-minded person — they're just an HR manager — and you want the exact file itself. Before starting, DIFFIDENT MOLE warns you of the following:

(i) The intrusion detection system will trigger an alert if a document loses more than one clearance level per action (for example, an action that drops a file from Management level to Unclassified level will trigger an alert).

(ii) Both objects and subjects with Management and with Customer Support level integrity must have an even number of compartments.

In a sequence of steps, direct OBEISANT QUOKKA to read or write D413, some of the eight documents listed earlier, or some of the below documents to step by step bring down D413's integrity level to (Public, $\emptyset$). Note that writing an empty string to a file will still trigger integrity level changes without changing the file itself (you may find this useful). At each step, describe the changes, if any, in both D413's integrity level and OBEISANT QUOKKA's clearance level. Be careful to heed DIFFIDENT MOLE's warnings, lest you trigger alerts and be penalized for your carelessness.

- D437: (Public, $\{\upsilon, \rho, x\}$)
- D759: (Developer, $\{\rho\}$)
- D866: (Management, $\{\varphi, \psi\}$)
- D553: (Customer Support, $\{\varphi, \eta\}$)
- D480: (Public, $\{\varphi, \upsilon\}$)
- D649: (Management, $\{\rho, x\}$)
- D500: (Management, $\{\varphi, \rho\}$)
- D342: (Customer Support, $\{\upsilon, \rho, \eta, x\}$)

OBEISANT QUOKKA manages to make D413 an unclassified file, copies it to a thumb drive and leaves it for you at a dead drop (hands it to you after they finish). DIFFIDENT MOLE is upset; for one, because OBEISANT QUOKKA was able to actually get the file free, and this means they have to rethink their model. For another, though, OBEISANT QUOKKA really messed up their clearance level, and now DIFFIDENT MOLE has to fix it by hand so they can go back to their normal work. The sacrifice was worth it, though... D413 contains hashes for passwords.

3. The sash wringing... the trash thinging... mash flinging... the flash springing, bringing the crash thinging, the... (10 marks)

The following is a hash from D413

```
$1$$353881A96DE856756C3FA8C1DD24A40C
```

(**HINT:** Knowing a little about how `/etc/shadow` files are formatted may be helpful here; however, note that we are not storing the hash itself in Base64, which is atypical for an `/etc/shadow` file. This fact should not impact your answers to any question below.)

(1 mark) a. What hash function produced this hash?

(2 marks) b. Is this an appropriate choice for a hashing function? If it is, describe what makes this choice more secure than other choices for password hashes. If it is not, describe a vulnerability this choice has that makes it a poor choice.

(2 marks) c. Does this hash reveal any weaknesses (aside from, potentially, choice of hashing function) the organization has with their passwords? Explain.

(1 mark) d. What is the password that created this hash? (**HINT:** There is no need to write code/run a password cracker to find this answer. Instead, searching the correct query on Google or other search engines will reveal it. Think carefully: what query could that be?)

(2 marks) e. Regardless of any weaknesses revealed by this hash, name something the organization can do to improve the confidence they have in authenticating users.

(2 marks) f. In the wake of OBEISANT QUOKKA's success in exfiltrating this file, DIFFIDENT MOLE is investigating implementing implicit authentication (through biometrics like typing patterns or other factors specific to how users interact with their machines). Suppose that 1 in 5,000 users of a VILE CORP machine are attempting to do something which VILE CORP would like to shut down. If the implicit authentication scheme always correctly identifies an illicit user when they act on a machine, and correctly identifies that the intended user is the one actually using a machine 99% of the time, is it a good decision for DIFFIDENT MOLE to adopt this system? Why or why not? What percentage of alerts will be false positives?

A rose by any other name would smell as sweet

DIFFIDENT MOLE is satisfied with your audit, and your boss begrudgingly drops the codenames until the next audit contract comes up. You go back to being ORDINARY INDIVIDUAL. Somehow, it feels like something is missing.

Programming Response Questions [90 marks]

You are assigned the task of understanding, setting up, and programming labs on a topic related to **Web Security** or **Network Security** from the open source seed (https://seedsecuritylabs.org/) lab projects. You are required to fully implement two topics and have a thorough understanding of the concepts involved. You can choose any one topic from the Web Security Labs, and choose any one topic from the Network Security Labs.

You are expected to explain how you did these two labs in-person or online to the TA for marking during the office hours on Thursdays. You will not get marks if you do not explain your work to our TA.

Web Security Labs topics: (choose one topic) [45 marks]

- Cross-site Scripting Attack Lab
- Cross-site Request Forgery Attack Lab
- SQL Injection Attack Lab
- Clickjacking Attack Lab (Cupcakes)
- Shellshock Vulnerability Lab

Network Security Labs topics: (choose one topic) [45 marks]

- Packet Sniffing and Spoofing Lab
- ARP Cache Poisoning Attack Lab
- ICMP Redirect Attack Lab
- TCP Attacks Lab
- The Mitnick Attack Lab
- Firewall Exploration Lab
- Firewall Evasion Lab

- VPN Tunneling Lab
- Virtual Private Network (VPN) Lab
- BGP Exploration and Attack Lab
- Morris Worm Attack Lab
- Heartbleed Attack Lab (Ubuntu 12.04 VM only)