Bachelor 2019

Red VS Blue, Cyber Security Simulator
User manual

Christian Bråthen Tverberg
Maarten Dijkstra
Nataniel Gåsøy

January-May 2019

Contents

1 Introduction

This document is intended to be a user manual for the real-time cyber security simulator prototype designed and implemented during our bachelor thesis.

2 Scenario creator

This section is for the scenario creator, and will cover process behind making a scenario. This includes how to add and connect components, set attributes as well as saving a scenario with the player and game statistics.

2.1 Making a scenario

In order to make a scenario, a plan must first be in place. This plan must include what the goal of the scenario will be, what resources and advantages the attacker and defender has from the beginning as well as what components will be involved.

The next step is to make the scenario. Either load an existing scenario or start a new one. Place the components desired for the scenario (from the menu on the left-hand side) by clicking the corresponding button and drag these to the desired place. Note that if an object is dropped outside of the editing field (The marked area in the center of the screen) it will be deleted.

Right-click on the components to change it's attributes (name, security level, if it is an entry point, list of vulnerabilities). From here it is also possible to delete the component, or make a connection between it and another component. In order to connect to another component, right-click a component, select "connect" and click the component you want to connect it to.

The connecting reference lines can also be attributed (firewall) or deleted by right-clicking on it.

After the topology is finished, and the attributes have been set, press save in order to save this scenario. In the save menu, you choose the name for the scenario as well as setting the attributes and resources for the attacking and defending team.

2.2 Scenario creator manual

This section will explain in more detail the different aspects of the scenario creator.

In this scenario creator screenshot (1), the menu seen on the left-hand side is a series of buttons, each representing the available system components. Pushing one of these will instantiate an object of the related system component from the folder of prefabs. This will be an empty component with only the base attributes of the corresponding system components.

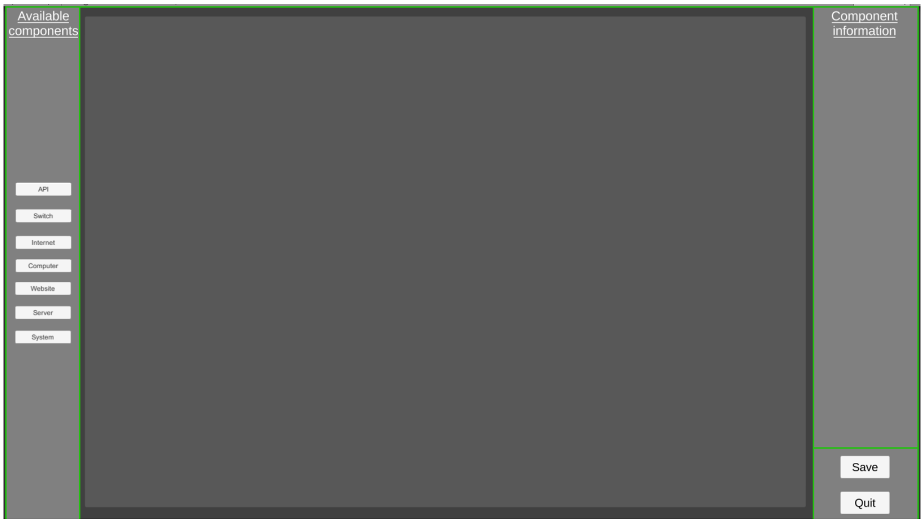
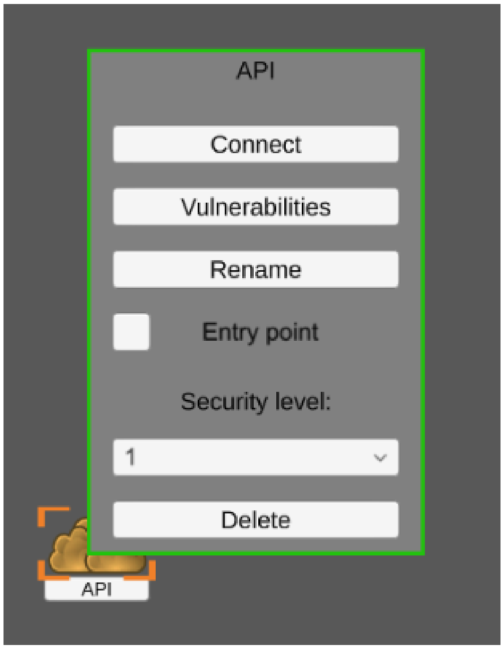


Figure 1: An empty scenario creator screen

On the right-hand side, the information of the selected system component is displayed. This information includes component type, security level, if it is an entry point and the list of vulnerabilities this component has. At the bottom of the right-hand menu, there is a button for saving the newly made scenario as well as a quit button to exit the scenario.

The next figure (2) shows the system component menu. This is accessed by right-clicking a system component within the editing field. This menu consists of the component type, connect button, vulnerabilities button, rename button, entry point toggle, security level dropdown and delete button.



□ Entry point

Security level: 1

Figure 2: A system component's right-click menu

The connect button is used to connect two system components. the vulnerabilities button will bring up the vulnerabilities menu. Here a list of vulnerabilities is read from the vulnerabilities XML file, and displayed in the menu. Selecting a vulnerability and pressing the "==¿" button will apply the selected vulnerability to the system component. The rename button opens the rename menu, which enables giving the system component a new name instead of the default name (which is the same as the type). The entry point toggle lets the user specify if this system component is an entry point or not. The security level describes how secure this particular system component is (or how vulnerable it is, depending on the angle you view it from). Finally, the delete button enables you to delete a specific system component.

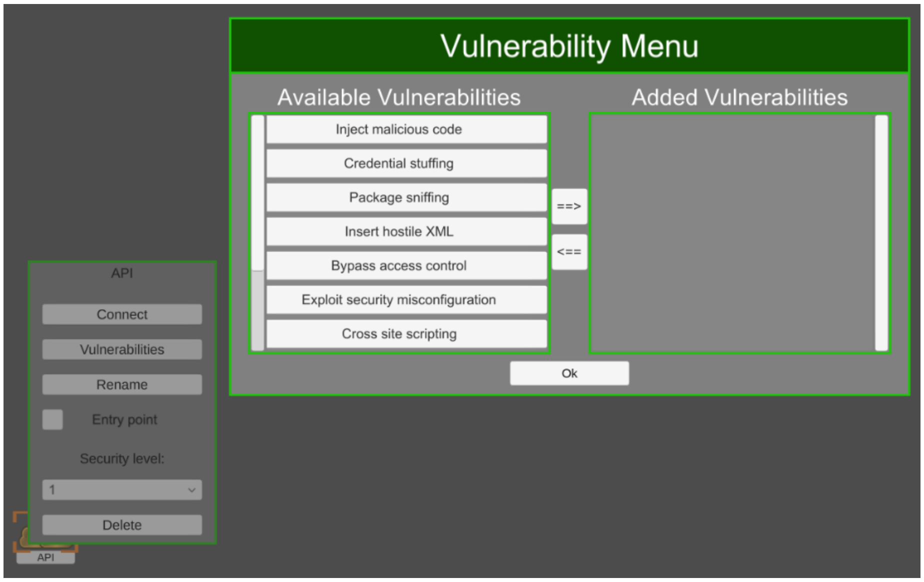


Figure 3: Vulnerability menu

In the vulnerability menu, seen in figure (3), the user can specify the vulnerabilities for the selected system component. The available vulnerabilities is read from an XML file, and displayed in a scrollable menu. From here, the user can add the desired vulnerabilities provided that they exist in the XML file, or remove a vulnerability from the list of added vulnerabilities.

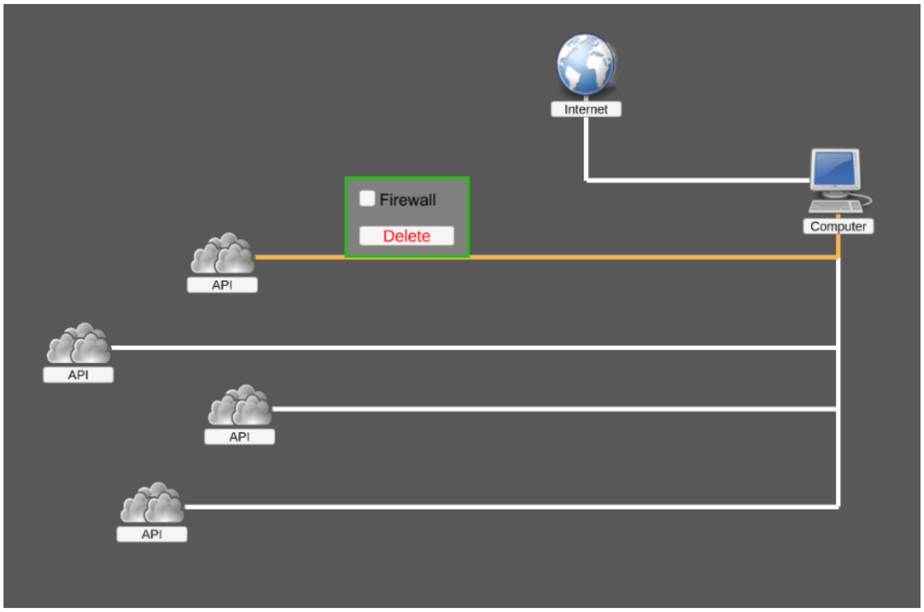
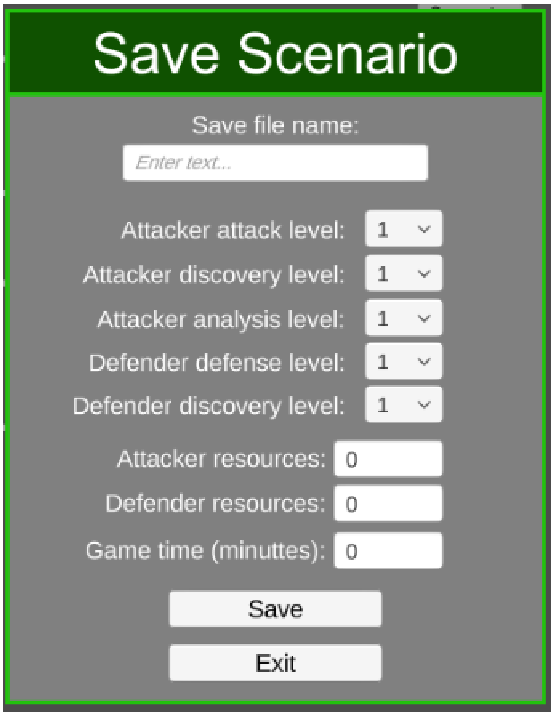


Figure 4: Connections and connection line menu

Right-clicking the connections, as seen in figure (4), brings up the menu for reference connections. Here the user can choose if the connection has a firewall or not, as well as delete the connection.



Save file name: Enter text...

Attacker attack level: 1

Attacker discovery level: 1

Attacker analysis level: 1

Defender defense level: 1

Defender discovery level: 1

Attacker resources: 0

Defender resources: 0

Game time (minuttes): 0

Figure 5: Save menu

Figure (5) shows the save menu. Here the user chooses a name for the new scenario created. If a file with that already exists, the user is asked if they want to overwrite this file or not. The statistics for attacker and defender, as well as their available resources and the duration of the scenario, is also set here for the scenario.

3 Gameplay

3.1 Setting up and connecting to a game

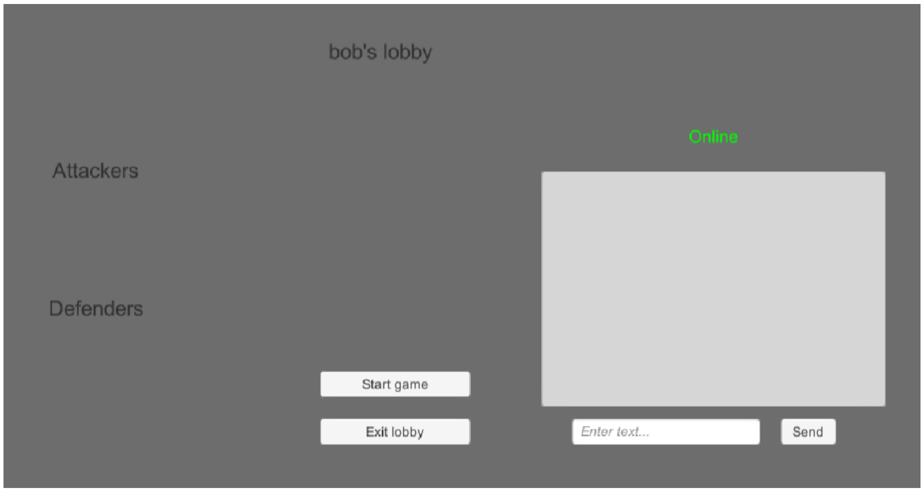


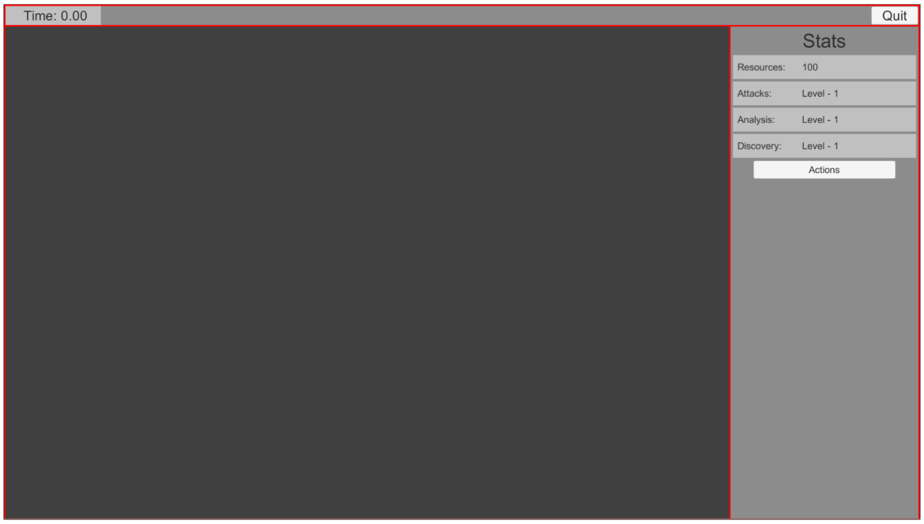
Figure 6: View of an empty lobby from host’s perspective.

To play the game you would need to either host a lobby and play as an observer, or join a lobby as a client and play as either attacker or defender. As a host you have the button for starting the game which you can do when each team has a player connected. As a client that joins a game you will get a list of available lobbies in the local network(if there are anyone hosting at the moment). If you are sure that a host is hosting yet you can’t find that lobby you would need to follow a few steps outside the game. Firstly open the command prompt window, then use the command ”$ping < IP >$”, where ”¡IP¿” is the hosts IP. You can find this IP by using either the command ”$ipconfig$” and use the value next to ”$IPv4$” or ”$arp - a$” and use the value next to ”interface” in a command prompt window on the hosts pc. This will fix the problem.

Before the game starts you have the option to swap between playing as defender/attacker by clicking on the other player, the swap will go through if the other player choose to accept. When there is a player on both teams(attacker/defender) the host can start the game and everyone will go into their own view according to their mode(attacker/defender/observer).

3.2 Game screen

3.2.1 Attacker POV


Time: 0.00

Stats

Resources: 100

Attacks: Level - 1

Analysis: Level - 1

Discovery: Level - 1

Figure 7: Attacker's initial view

Upon starting a session the Attacker (red team) will be met by a blank screen with no nodes (Figure 7). The right side panel is used for showing either user information, showing initial actions the attacker can take, information about a selected node, or different attacks to send to a node. The first entry here is the amount of resources the attacker has to spend on different actions. The second entry shows the attacker's attack level. The third entry is the attackers analysis level. The fourth entry is the attackers discovery level. Increasing a level in one of these will increase it's success chance. Hovering over any of these fields will display a small tooltip explaining what the entries mean. The final entry is a button which will lead to an actions menu.

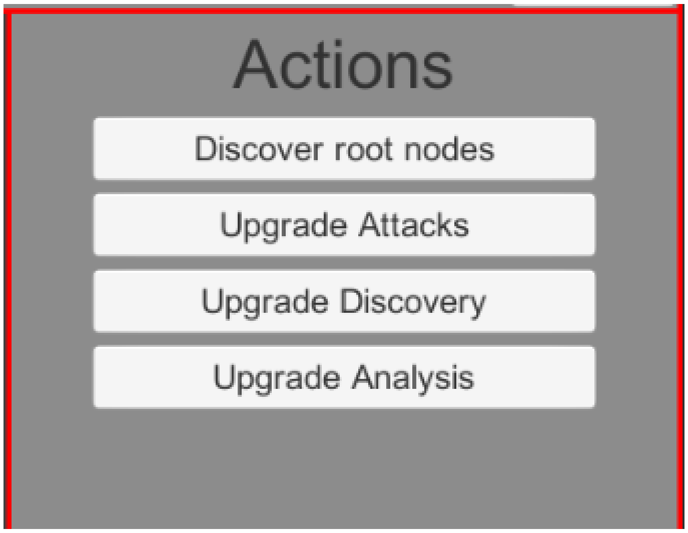
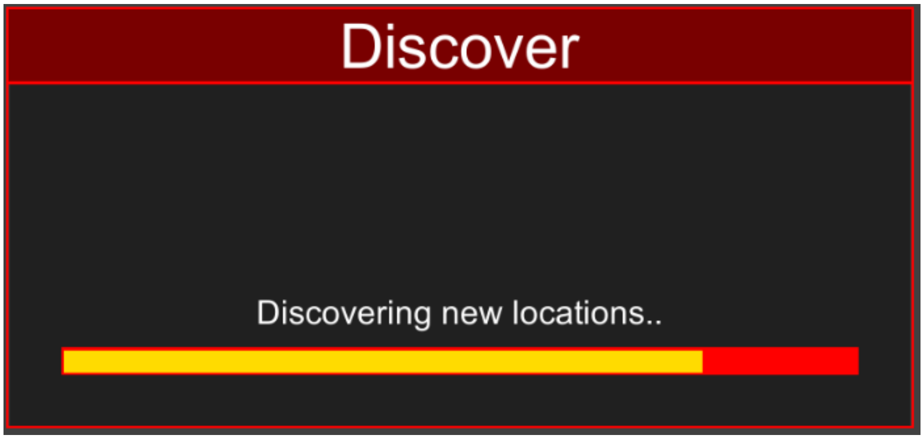


Figure 8: Attacker's actions menu

Clicking on the actions button will change the right panel into showing the different actions the attacker can do (Figure 8). Discovering root nodes does what it sounds it does. It tries to find an access point to the network in the scenario. Discovering an entry point will always succeed, but delving deeper into the network might not. The other three buttons are for upgrading their respective actions. Each upgrade level costs more and takes longer than the previous, but will increase the chance of success doing any of those actions. Currently, the success chance increases linear, and the max level on any action is level three.

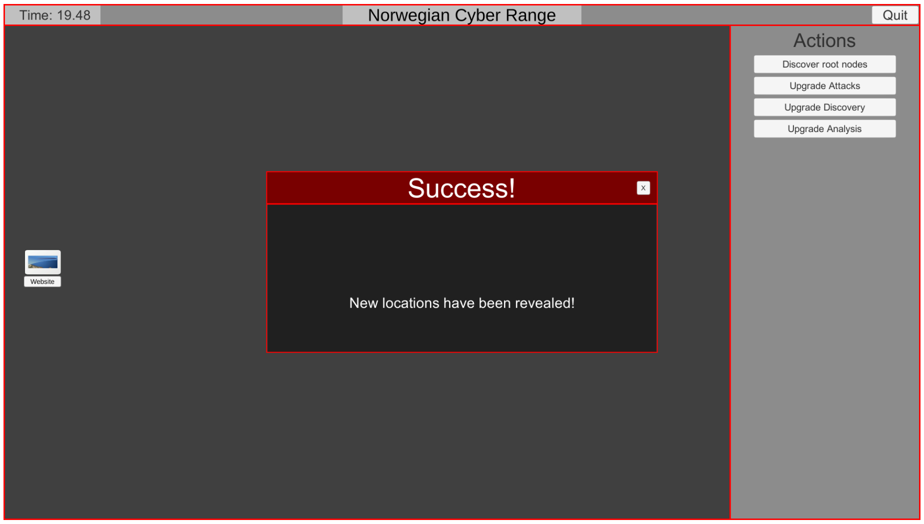


Discover

Discovering new locations..

Figure 9: Progress window

Doing any action requires time, and starting one will pop up a progress window showing what you do and the current progress on the task (Figure 9). Here we are almost done with a discovery action. Different actions take a different amount of time to complete, and since you are only one attacker, you can only do one thing at a time.

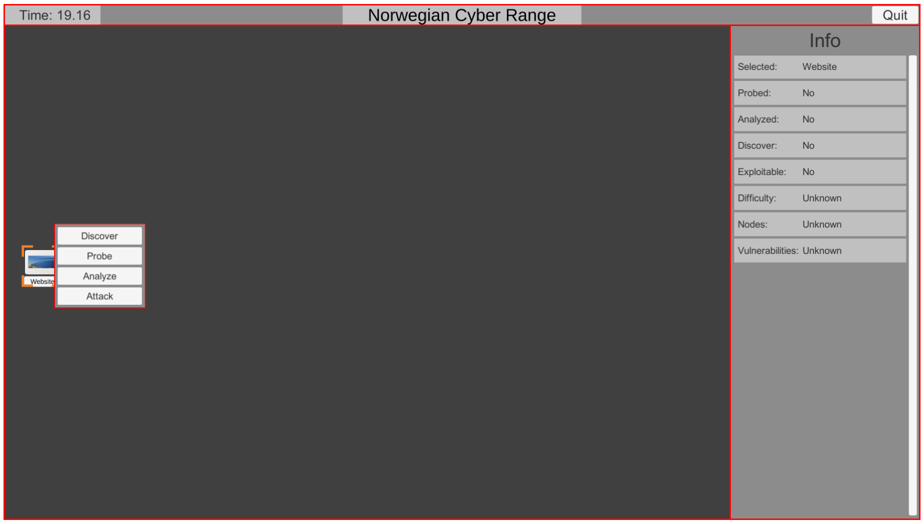


Success!

New locations have been revealed!

Figure 10: Discovery success!

Once an action has been completed either a success or failure message will pop up, and here we succeeded in finding a root node (Figure 10). There will always be at least one entry point to network, and here we found a node called ’Website’.

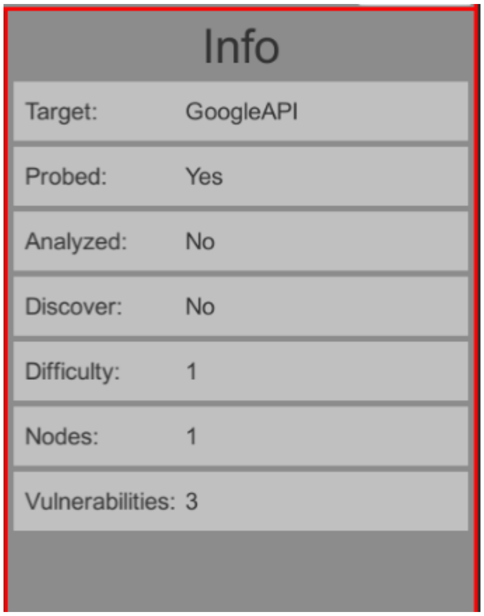


Time: 19.16

Selected: Website
Probed: No
Analyzed: No
Discover: No
Exploitable: No
Difficulty: Unknown
Nodes: Unknown
Vulnerabilities: Unknown

Figure 11: Node view

When we click on a node (here ’Website’) the right panel with be filled with the info we have on it. With a right-click on a selected node a menu will popup next to the node (Figure 11). The info panel will show you the information you currently have available on the node. Each entry has a tooltip explaining the entry. The popup menu has four available actions you can take on the node. Discover will try and find any node that is connected to the selected one. Probe will get you surface level information of the node (Difficulty, number of connected nodes and number of vulnerabilities). Analyze will let you find the specific vulnerabilities on that node. Attack will let you choose which attack you want to send to the node. Every action except Probe has a chance for failure, or a partial success. Probe will always succeed.

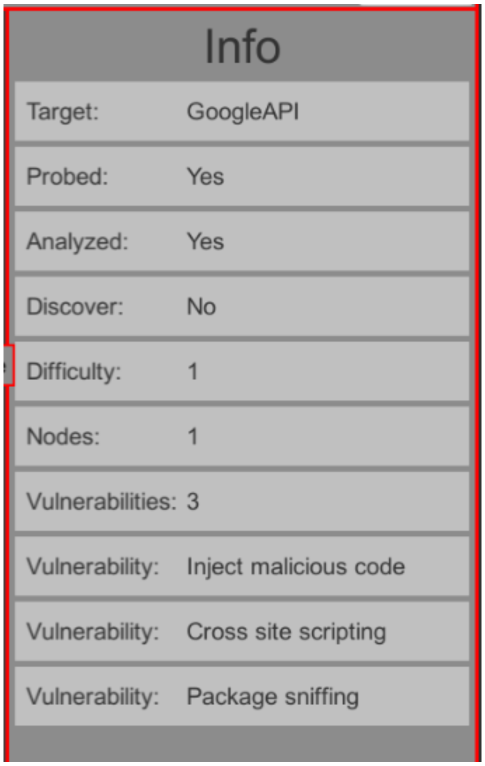


Info

Target:	GoogleAPI
Probed:	Yes
Analyzed:	No
Discover:	No
Difficulty:	1
Nodes:	1
Vulnerabilities:	3

Figure 12: Info panel detailed after probing

Here we see the information available for the 'GoogleAPI' node after probing (Figure 12). The difficulty is one, there is one connected node, and there are three vulnerabilities on this node.



Info

Target:	GoogleAPI
Probed:	Yes
Analyzed:	Yes
Discover:	No
Difficulty:	1
Nodes:	1
Vulnerabilities:	3
Vulnerability:	Inject malicious code
Vulnerability:	Cross site scripting
Vulnerability:	Package sniffing

Figure 13: Info panel detailed after analysis

Here we see the information available for the 'GoogleAPI' node after analyzing it (Figure 13). We were lucky and found all three vulnerabilities. This information might get outdated as the game progresses as the defender might add defenses to the node, in which case you have to probe and analyze again to get the new information.

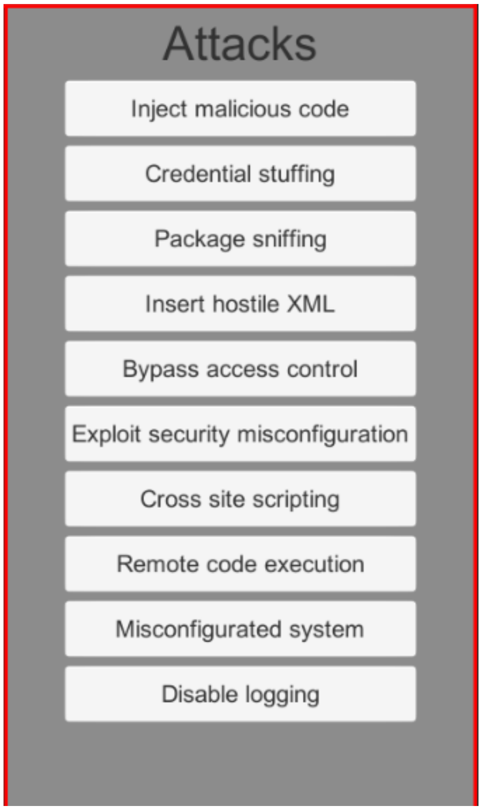
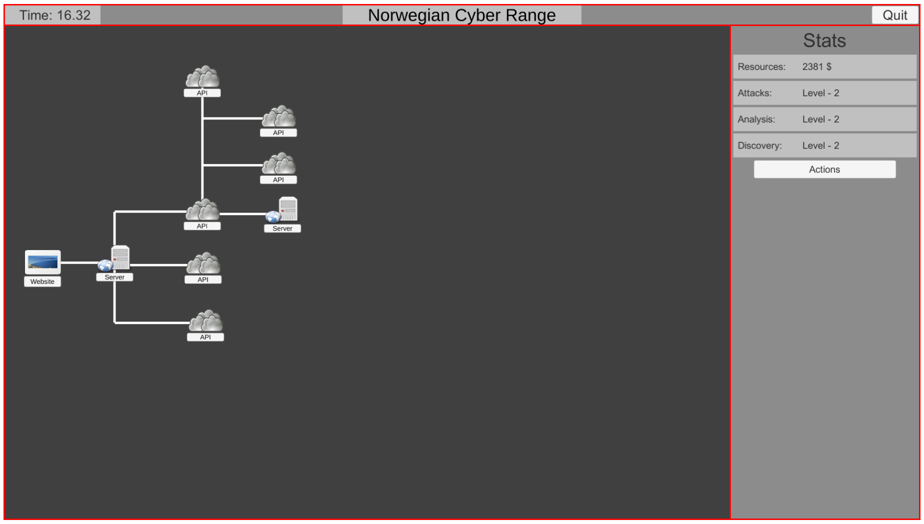


Figure 14: Attack options

When clicking on the Attack button from the popup menu (Figure 11), the right panel will be populated with the different attack options available to you (Figure 14). The best way of attacking is knowing which vulnerabilities the node has. Attacking blindly might succeed if you are lucky, but more often than not you will fail.


Time: 16.32

Norwegian Cyber Range

Stats

Resources: 2381 $

Attacks: Level - 2

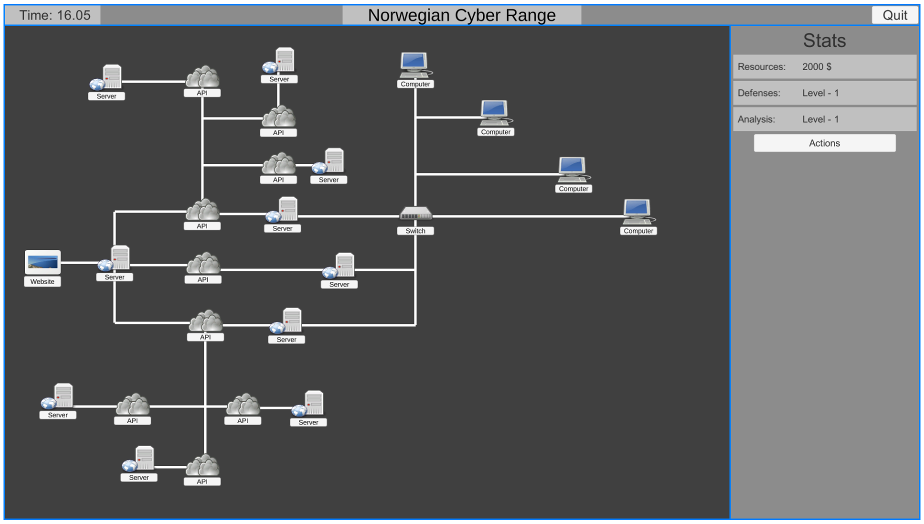
Analysis: Level - 2

Discovery: Level - 2

Figure 15: Progress

This is an example of what your game screen might eventually look like. We have several different nodes with individual icons, and lines connecting them.

3.2.2 Defender POV


Time: 16.05

Norwegian Cyber Range

Stats

Resources: 2000 $

Defenses: Level - 1

Analysis: Level - 1

Figure 16: Defender's initial view

Upon starting a session the Defender (blue team) will be met by all the nodes in the network (Figure 16). The right side panel is used for showing either user information, showing initial actions the defender can take, information about a selected node, or different defenses to implement in a node. The first entry here is the amount of resources the defender has to spend on different actions. The second entry shows the defender's defense level. The third entry is the defenders analysis level. Increasing a level in one of these will increase it's success chance. Hovering over any of these fields will display a small tooltip explaining what the entries mean. The final entry is a button which will lead to an actions menu.

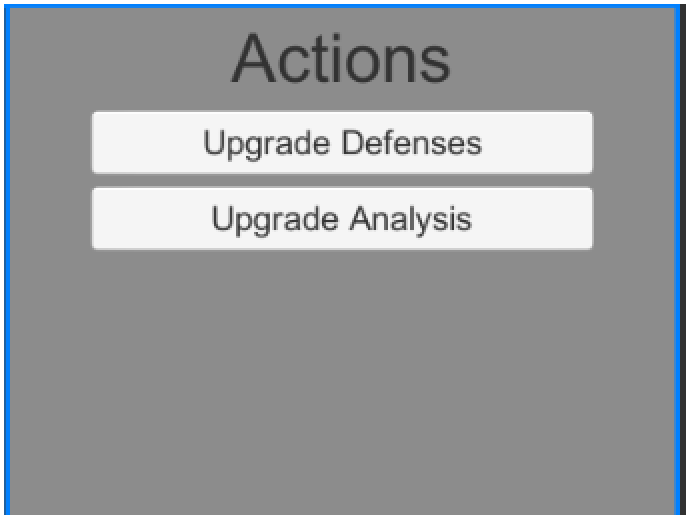
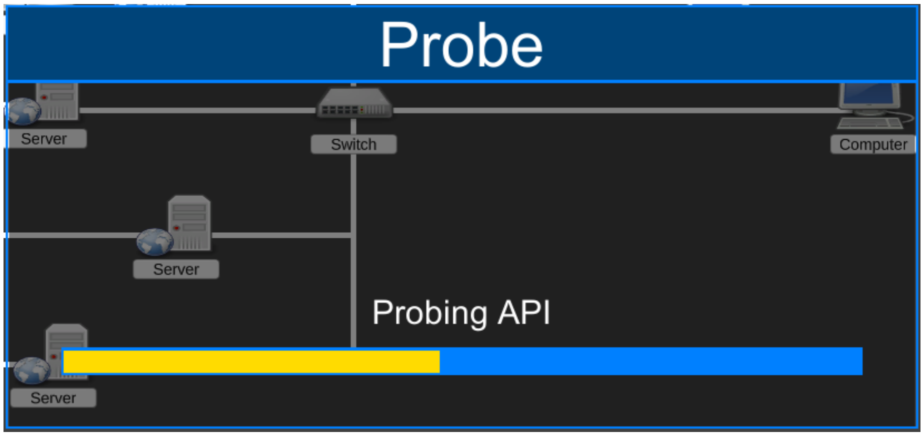


Figure 17: Defender's initial actions

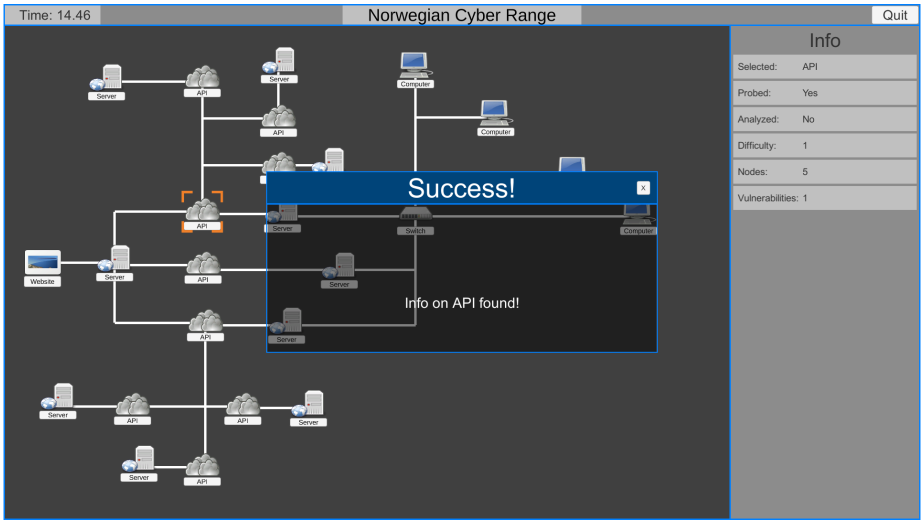
Clicking on the actions button will change the right panel into showing the different actions the defender can do (Figure 8). Unlike the attacker, the defender always see all nodes, so there is no need to discover. The two buttons are for upgrading their respective actions. Each upgrade level costs more and takes longer than the previous, but will increase the chance of success doing any of those actions. Currently, the success chance increases linear, and the max level on any action is level three.


Probe

Probing API

Figure 18: Progress window

Doing any action requires time, and starting one will pop up a progress window showing what you do and the current progress on the task (Figure 18). Here we are almost done with a probe action. Different actions take a different amount of time to complete, and since you are only one defender, you can only do one thing at a time.


Time: 14.46

Norwegian Cyber Range

Info

Selected: API

Probed: Yes

Analyzed: No

Difficulty: 1

Nodes: 5

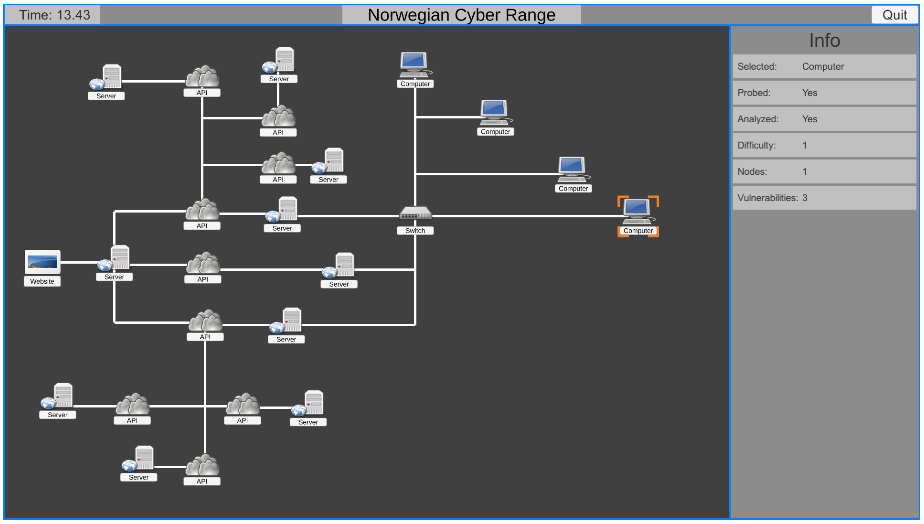
Vulnerabilities: 1

Success!

Info on API found!

Figure 19: Probe success!

Once an action has been completed either a success or failure message will pop up, and here we succeeded in probing an API (Figure 19).



Time: 13.43

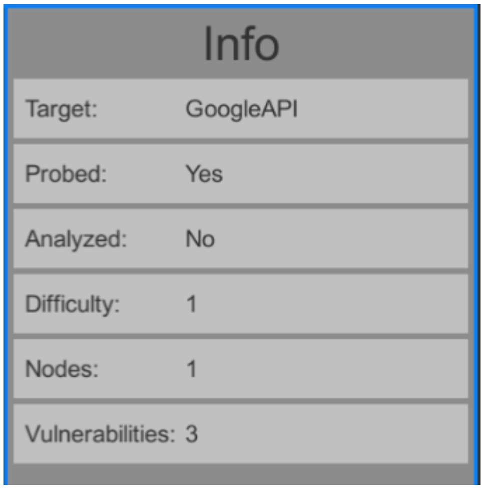
Norwegian Cyber Range

Info

Selected:	Computer
Probed:	Yes
Analyzed:	Yes
Difficulty:	1
Nodes:	1
Vulnerabilities:	3

Figure 20: Node view

When we click on a node (here 'Computer') the right panel with be filled with the info we have on it. With a right-click on a selected node a menu will popup next to the node (Figure 20). The info panel will show you the information you currently have available on the node. Each entry has a tooltip explaining the entry. The popup menu has three available actions you can take on the node. Probe will get you surface level information of the node (Difficulty, number of connected nodes and number of vulnerabilities). Analyze will let you find the specific vulnerabilities on that node. Defend will let you choose which defense you want to implement on the node. Every action except Probe has a chance for failure, or a partial success. Probe will always succeed.



Info

Target: GoogleAPI

Probed: Yes

Analyzed: No

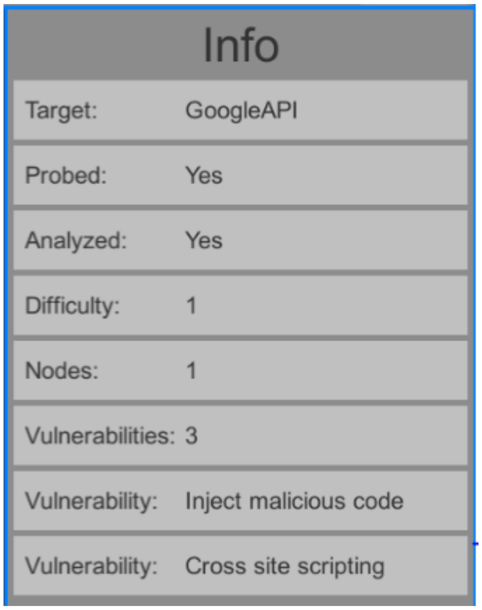
Difficulty: 1

Nodes: 1

Vulnerabilities: 3

Figure 21: Info panel detailed after probing

Here we see the information available for a 'GoogleAPI' node after probing (Figure 21). The difficulty is one, there is one connected node, and there are three vulnerabilities on this node.



Info

Target: GoogleAPI

Probed: Yes

Analyzed: Yes

Difficulty: 1

Nodes: 1

Vulnerabilities: 3

Vulnerability: Inject malicious code

Vulnerability: Cross site scripting

Figure 22: Info panel detailed after analyzing

Here we see the information available for a 'GoogleAPI' node after analyzing it (Figure 22). We weren't lucky and only found two of three vulnerabilities This information might get outdated as the game progresses as you might add defenses to the node, in which case you have to probe and analyze again to get the new information.

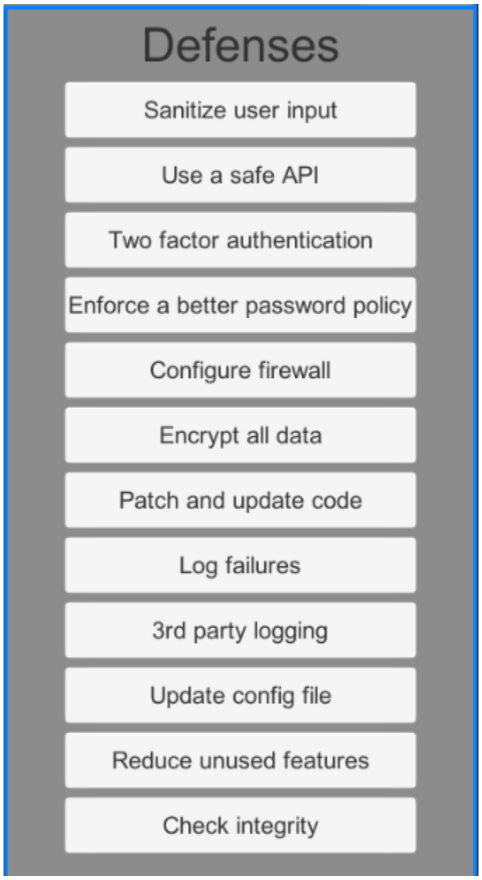


Figure 23: Defense options

When clicking on the Defense button from the popup menu (Figure 20), the right panel will be populated with the different defense options available to you (Figure 23). The best way of defending is knowing which vulnerabilities the node has. Defending blindly might succeed if you are lucky, but more often than not you will fail.

3.2.3 Observer POV

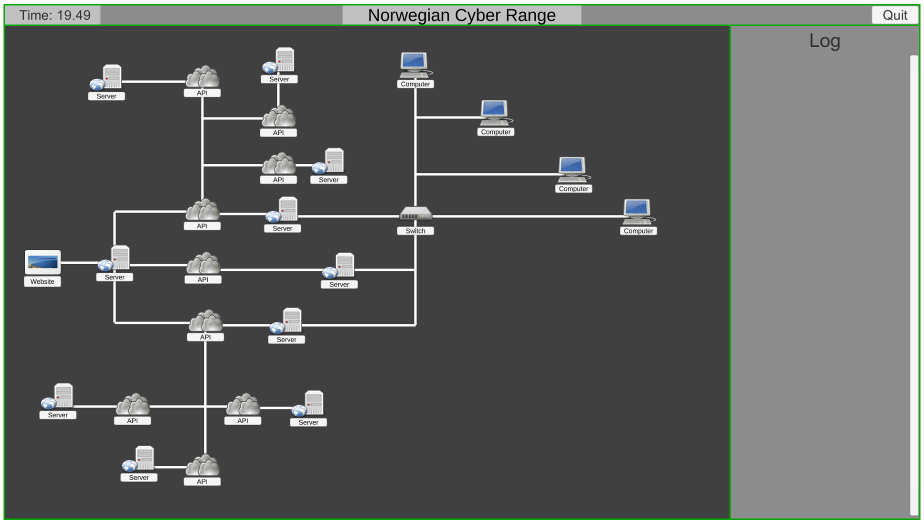
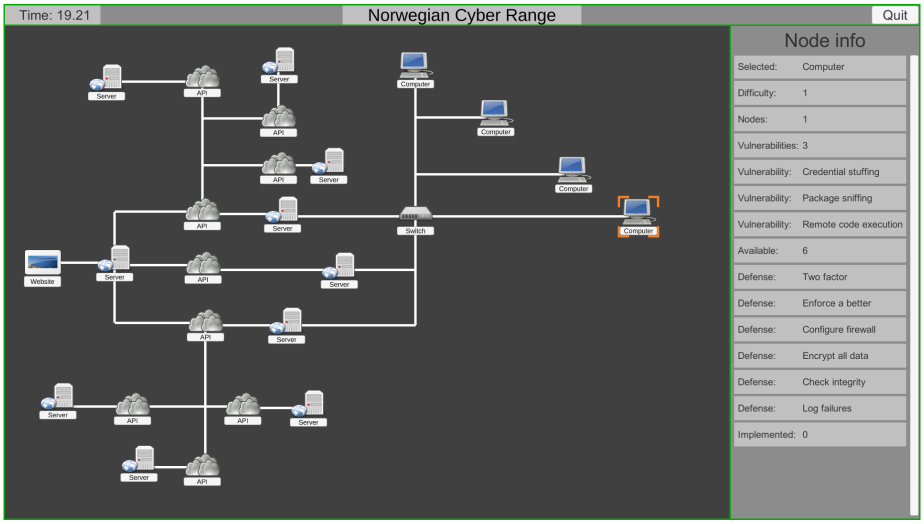


Figure 24: Observer's initial view

Upon starting a session the Observer will be met by all the nodes in the network (Figure 24). The right side panel is used for showing either the log of events, or information about a selected node. The log will automatically scroll to the bottom to display the newest events during gameplay. Most events will also be saved to log files, divided between attacker and defender, to be able to be reviewed at a later point.



Time: 19.21

Norwegian Cyber Range

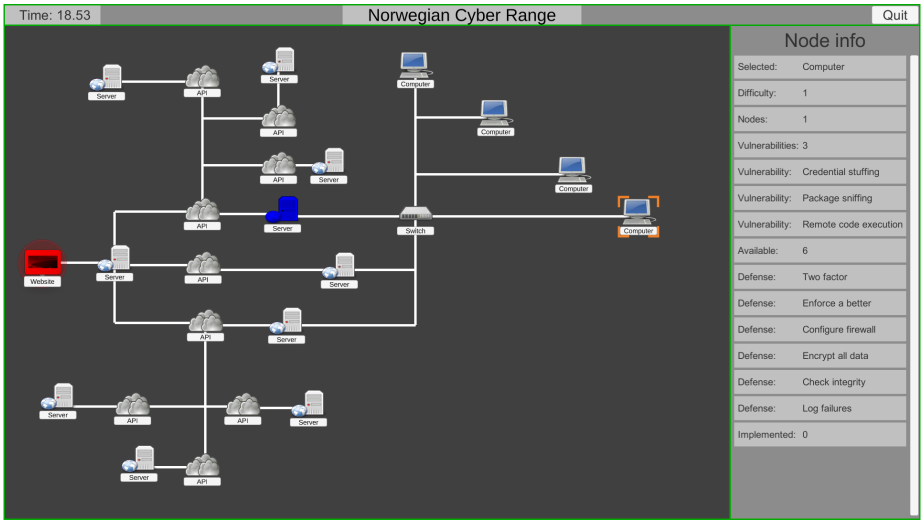
Quit

Node info

Selected:	Computer
Difficulty:	1
Nodes:	1
Vulnerabilities:	3
Vulnerability:	Credential stuffing
Vulnerability:	Package sniffing
Vulnerability:	Remote code execution
Available:	6
Defense:	Two factor
Defense:	Enforce a better
Defense:	Configure firewall
Defense:	Encrypt all data
Defense:	Check integrity
Defense:	Log failures
Implemented:	0

Figure 25: Node info

When we click on a node (here 'Computer') the right panel with be filled with all the info on it (Figure 25). Each entry has a tooltip explaining the entry. This info will automatically be updated as the game progresses.



Time: 18.53

Norwegian Cyber Range

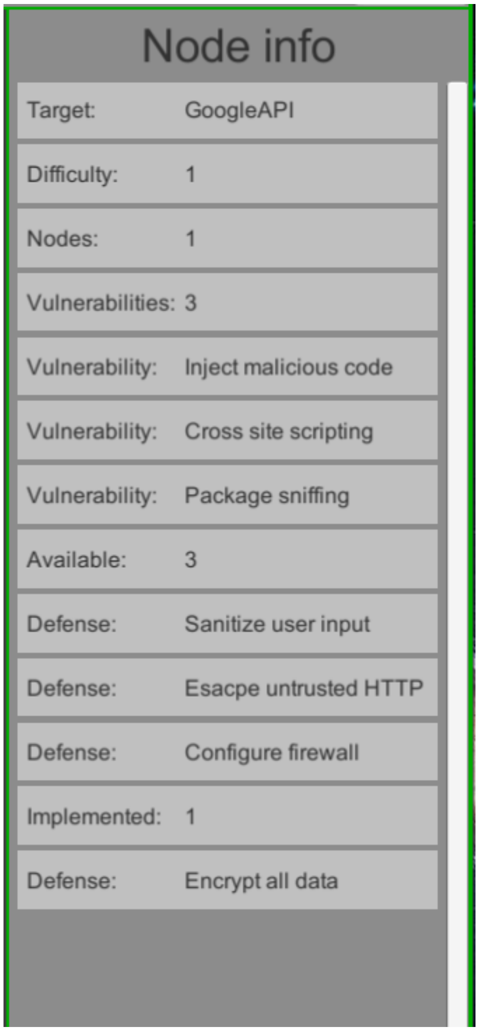
Quit

Node info

Selected:	Computer
Difficulty:	1
Nodes:	1
Vulnerabilities:	3
Vulnerability:	Credential stuffing
Vulnerability:	Package sniffing
Vulnerability:	Remote code execution
Available:	6
Defense:	Two factor
Defense:	Enforce a better
Defense:	Configure firewall
Defense:	Encrypt all data
Defense:	Check integrity
Defense:	Log failures
Implemented:	0

Figure 26: Attacker and Defender targeting

During gameplay, when either the attacker or defender is targeting a node, the nodes color will change depending on who is targeting it (Figure 26). If they target the same node, the most recent targeting will display, but if the last one deselects or targets another node, the color will be changed back to the previous color.

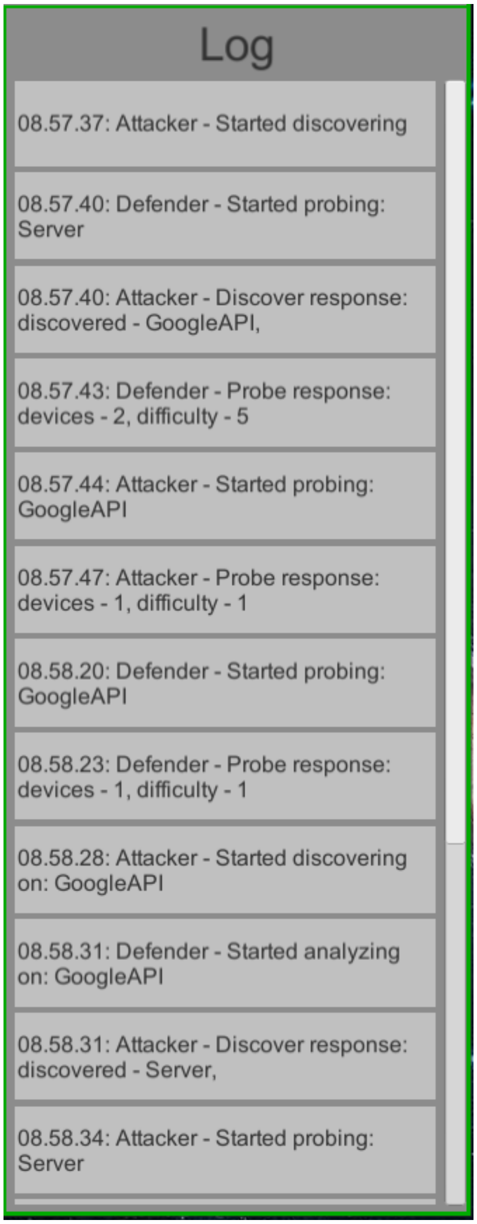


Node info

Target:	GoogleAPI
Difficulty:	1
Nodes:	1
Vulnerabilities:	3
Vulnerability:	Inject malicious code
Vulnerability:	Cross site scripting
Vulnerability:	Package sniffing
Available:	3
Defense:	Sanitize user input
Defense:	Esacpe untrusted HTTP
Defense:	Configure firewall
Implemented:	1
Defense:	Encrypt all data

Figure 27: Updated info during gameplay

Here is an example of a node having changed during gameplay (Figure 27). We can still see the vulnerabilities, but the defender has implemented a defense since earlier (Figure 25).

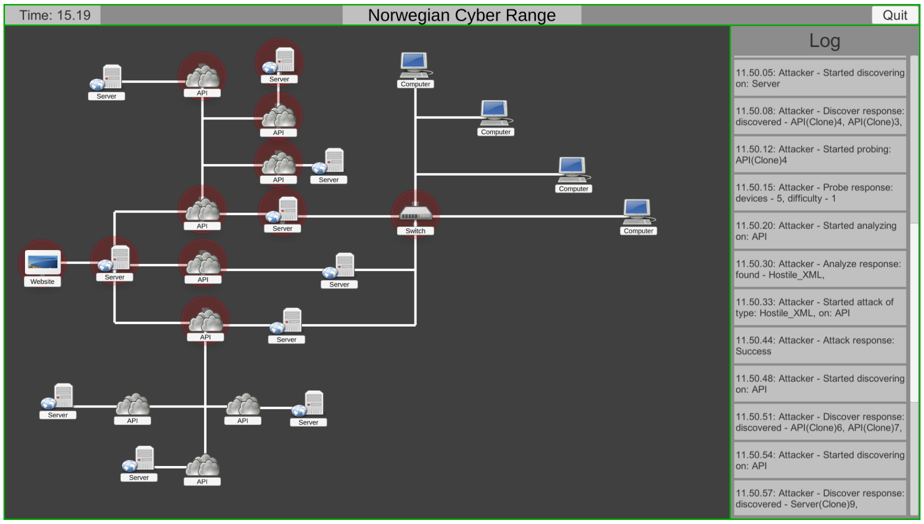


```
08.57.37: Attacker - Started discovering
08.57.40: Defender - Started probing: Server
08.57.40: Attacker - Discover response: discovered - GoogleAPI,
08.57.43: Defender - Probe response: devices - 2, difficulty - 5
08.57.44: Attacker - Started probing: GoogleAPI
08.57.47: Attacker - Probe response: devices - 1, difficulty - 1
08.58.20: Defender - Started probing: GoogleAPI
08.58.23: Defender - Probe response: devices - 1, difficulty - 1
08.58.28: Attacker - Started discovering on: GoogleAPI
08.58.31: Defender - Started analyzing on: GoogleAPI
08.58.31: Attacker - Discover response: discovered - Server,
08.58.34: Attacker - Started probing: Server
```

Figure 28: Log of events

During gameplay, every action taken in-game will be logged by the observer (Figure 28). The log will be sorted by time, and you are able to scroll up or down to see what happened when.

Once the attacker gets progress into the network, the nodes the attacker has access to will have a red circle behind then (Figure 29. This is in order to highlight the current progress of the attacker.



```
11.50.05: Attacker - Started discovering
on: Server
11.50.08: Attacker - Discover response:
discovered - API(Clone)4, API(Clone)3,
11.50.12: Attacker - Started probing:
API(Clone)4
11.50.15: Attacker - Probe response:
devices - 5, difficulty - 1
11.50.20: Attacker - Started analyzing
on: API
11.50.30: Attacker - Analyze response:
found - Hostile_XML,
11.50.33: Attacker - Started attack of
type: Hostile_XML, on: API
11.50.44: Attacker - Attack response:
Success
11.50.48: Attacker - Started discovering
on: API
11.50.51: Attacker - Discover response:
discovered - API(Clone)6, API(Clone)7,
11.50.54: Attacker - Started discovering
on: API
11.50.57: Attacker - Discover response:
discovered - Server(Clone)9,
```

Figure 29: Progress in gameplay

3.3 Win/Lose condition?

(To be implemented)
The win condition for each side is determined by the scenario creator. There will be different types of win/lose conditions like ”attacking or defending a certain node”, ”Have x amount of successful attacks” etc. The scenario creator will have the option to create descriptions for each side to explain the goal, which either side can read whenever they want during gameplay.