PenQuest QuickStart Guide

Version 1.0 (05-06-2022)

“A penetration test, colloquially known as a pen test, is an authorized simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.”

> The CISSP and CAPCM Prep Guide: Platinum Edition

A penetration quest (pen quest) is a totally made-up term describing what you are about to do in this game: playing out a no-nonsense cyber-attack or implementing a kick-ass defense strategy on a game board to pursue your quest of digital domination.

Visit https://www.pen.quest for more information! To request access to the current dev version, please contact robert.luh@fhstp.ac.at or sebastian.eresheim@fhstp.ac.at!

Please report bugs (screenshot, debug console output appreciated) to bug@pen.quest!

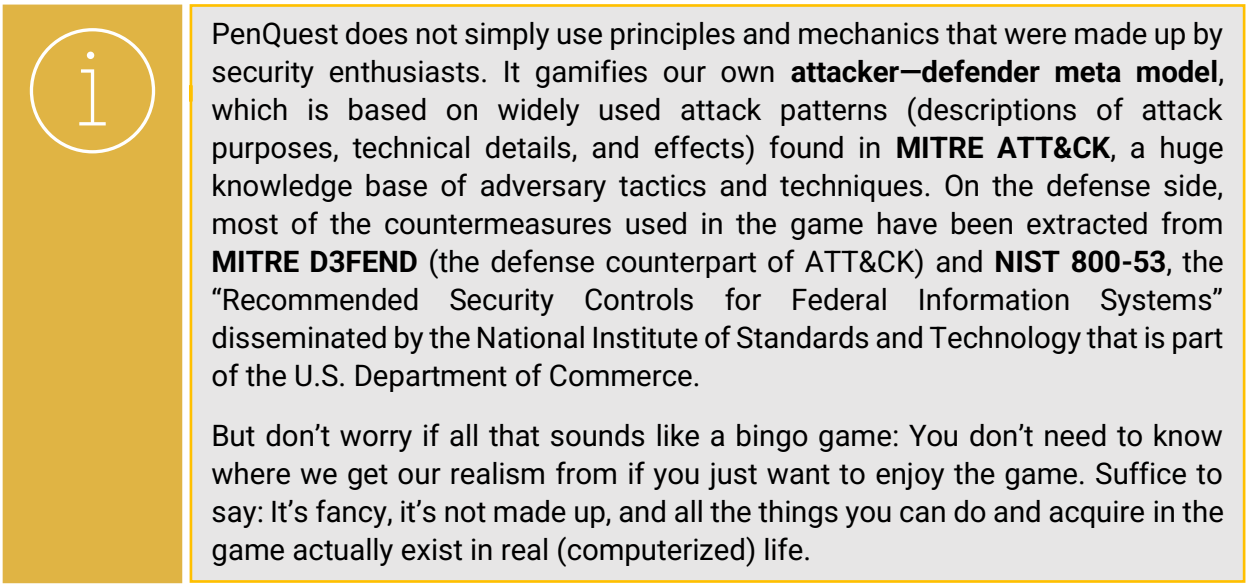
Contents

1. What is PenQuest (about)?

PenQuest is an attacker—defender meta model converted into an **educational strategy game**. It is intended to teach managers, techies, students, and other, hacking-affine folks about the ins and outs of cyber-attacks – including how to defend against them. One of the players will represent the **attacker** (hacker, pen tester, secret agent, etc.) while the other takes the role of **defender** (company, university, military organization, etc.), whose task it is to prevent the attacker from achieving their sinister goal.

Under the hood, PenQuest is a **digital two-player board game** using a card deck and different virtual tokens to keep track of things. The eponymous board typically represents an abstracted **IT infrastructure** that can range from a simple home network to a corporate Compu-Global-Hyper-Mega-Net (which is totally a thing).

An average game session can take everything from 15 minutes to several hours, depending on the complexity and size of the chosen scenario and game board.



PenQuest does not simply use principles and mechanics that were made up by security enthusiasts. It gamifies our own **attacker—defender meta model**, which is based on widely used attack patterns (descriptions of attack purposes, technical details, and effects) found in **MITRE ATT&CK**, a huge knowledge base of adversary tactics and techniques. On the defense side, most of the countermeasures used in the game have been extracted from **MITRE D3FEND** (the defense counterpart of ATT&CK) and **NIST 800-53**, the "Recommended Security Controls for Federal Information Systems" disseminated by the National Institute of Standards and Technology that is part of the U.S. Department of Commerce.

But don't worry if all that sounds like a bingo game: You don't need to know where we get our realism from if you just want to enjoy the game. Suffice to say: It's fancy, it's not made up, and all the things you can do and acquire in the game actually exist in real (computerized) life.

Now, without further ado, let's get started with your first games!

2. Getting started

2.1 This document

Please note that this document is not a game manual per se but merely acts as a QuickStart guide introducing PenQuest's scenarios as well as its most important mechanics. We are currently working on a full manual (with video guides), so please hang in there!

Specifically, we will walk through five tutorial scenarios currently in the game and explain how to play them. Please consider this document a companion guide and follow the given instructions.

Have fun!

2.2 Registering a user

In order to create an account, you need an invitation code. This code will be sent to you via e-mail (from office@pen.quest in case you need to check your spam folder) either by the game developers (us) or another privileged user. You can either click the link in the message or navigate to https://alpha.pen.quest, click “Sign In” and select “Register”.

You will be asked to paste in your registration code and choose a username (4 characters or longer), e-mail address, and password.

PenQuest requires you to pick a password that is at least 12 characters long. You need to include small and capital letters, a number, and a special character. Sorry about the hassle, but we kind of felt like we should get this particular point across 😉

After that, you are good to go: Enter your username and the password in the sign-in window and click “Login”. You will be greeted by the main menu.

2.3 Starting a game

To create a game, select the option “New” in the menu shown after log-in. You will be greeted by the game’s lobby.

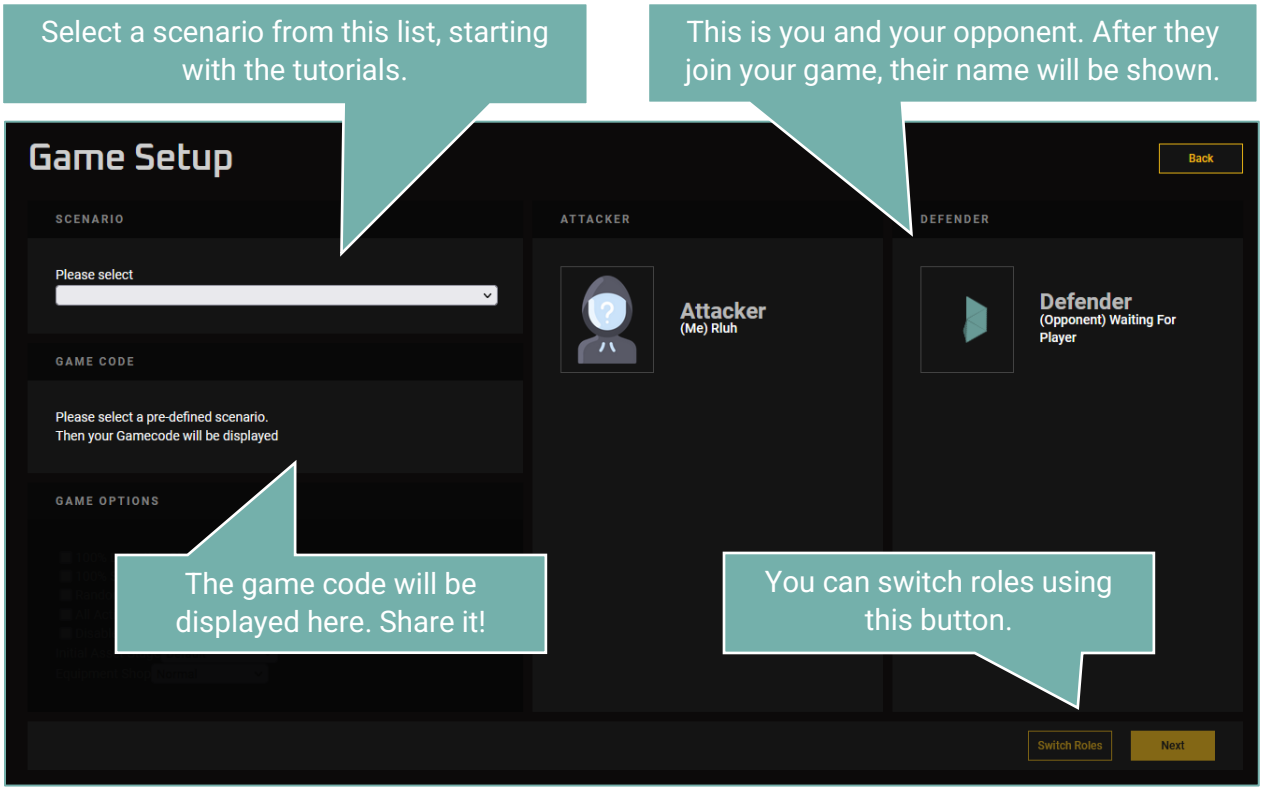


Figure 1: Game lobby

Select the scenario you want to play from the pull-down menu and share the displayed game code with your opponent. They can use the “Join” option in the main menu to enter the code or select

your game from the list of open sessions. Once both players are ready, the host can click “Next”. You will be shown an info screen followed by the game objectives window. Read your mission goals carefully – you will need to meet them in order to win the game.

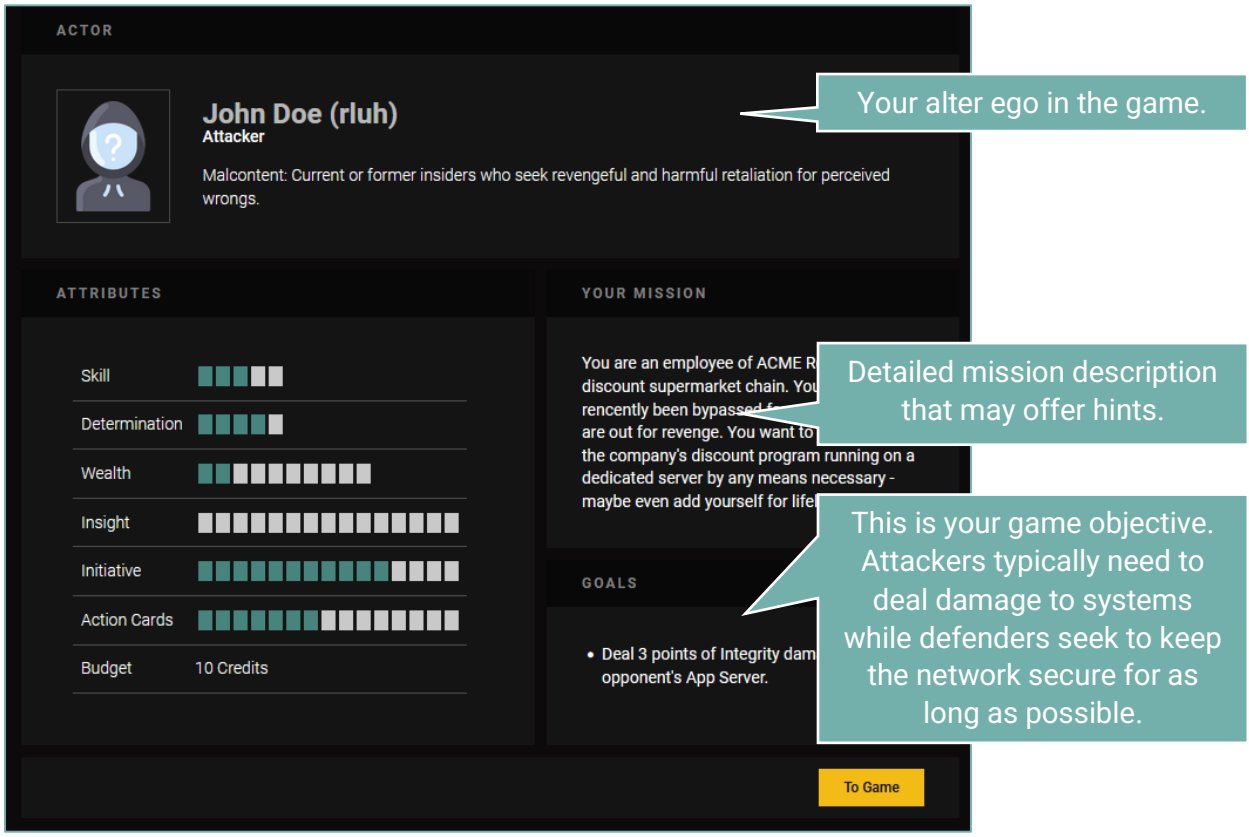


Figure 2: Objective & player info window

To learn more about the attributes shown on this screen, hover your mouse over them to display an explanatory tooltip. Attributes generally increase your chances of success, the number of cards available to you at a given time, and your financial resources.

After clicking “To Game”, you will be taken to the game board (Figure 3).

3. Playing the game

Follow the instructions in the info bar on the top center – they will guide you through the entire turn. In short, the game sequence is as follows:

1. Shopping (both): Procure tools and appliances that help you with your mission.
2. Attack (Attacker): Select an attack action from the lower left and drag them on the asset (system) you want to attack. In the appearing attack window, select your desired mode:
    a. Confidentiality (data theft, data gathering)
    b. Integrity (system manipulation, required to take control and unlock new vectors)
    c. Availability (taking a system offline)
3. Drawing cards (Attacker): Pick a new card to use in the next turn(s).

4. Detection (Defender, optional): If the defender spots the attack (your attributes and equipment will determine that), an alert will be shown, prompting for response.
5. Defense (Defender): Drag a defense action on the asset you want to secure. You can either react to a detected threat ("Response"-type actions), boost future detection ("Detection"), or harden your system against future threats ("Prevention").
6. Drawing cards (Defender): Pick a new card to use in the next turn(s).

You can click an asset on the game board at any time to display additional information about it.

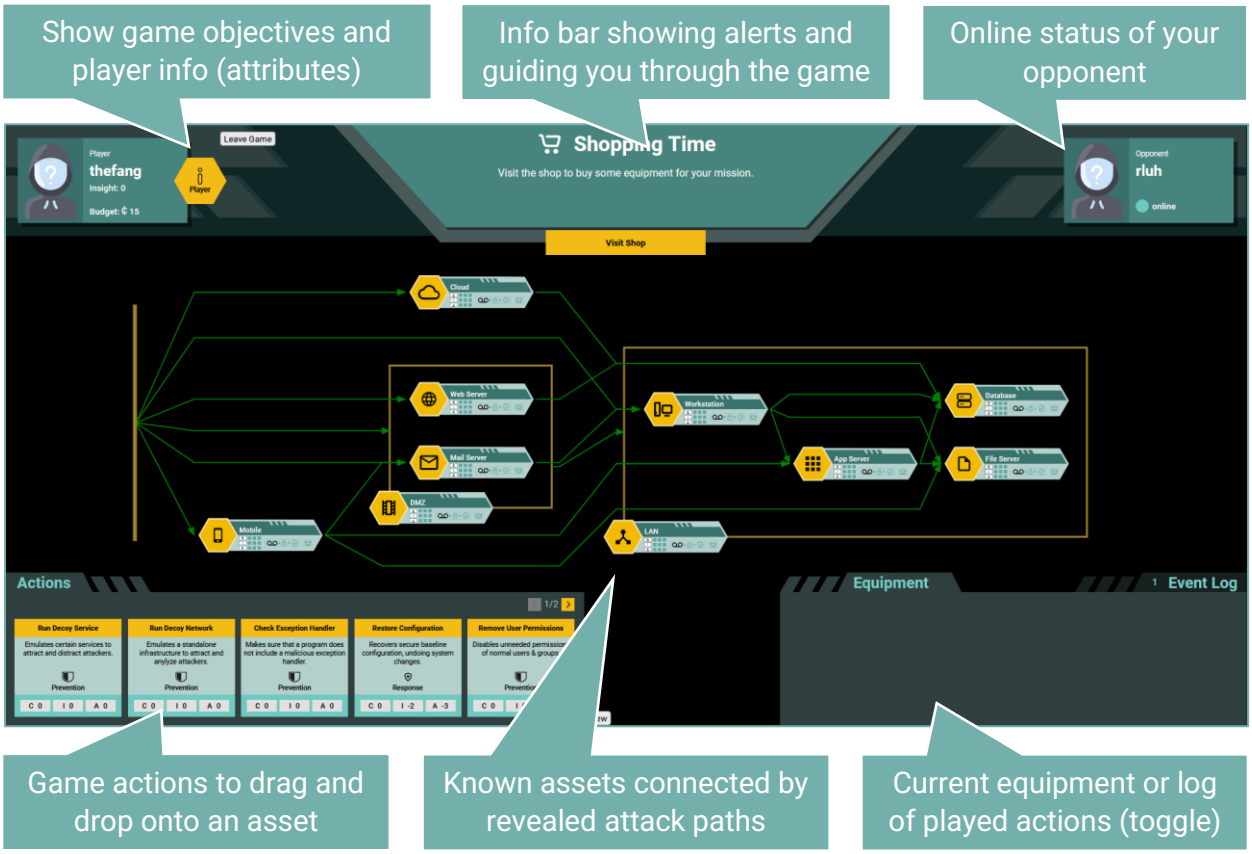


Figure 3: Game board

In the following, we will go through the tutorial missions available in PenQuest. Follow the instructions in the respective sub-section to complete them.

There are currently 5 tutorials in the game. It is recommended to play them all either against yourself (open two tabs and log in with two different accounts) or openly against a human opponent. Secrecy is not needed here – it is important to observe and understand both sides. Once you've completed the tutorials, feel free to try one of the larger testing scenarios.

By the way: Should your game crash for some reason or a refresh happen, or should you want to take a break, you can resume past games by selecting "Rejoin Game" from the main menu. Stored progress can be discarded by clicking "Leave Game".

3.1 Tutorials

Tutorial 1: Insight

Insight is one of PenQuest's most important resources. It will award you with a flat bonus to your action success (both sides) and detection chances (defender only). It represents your knowledge about your opponent and may even serve as a victory condition. In the case of the first tutorial, you need to reach 1 Insight as the attacker to win.

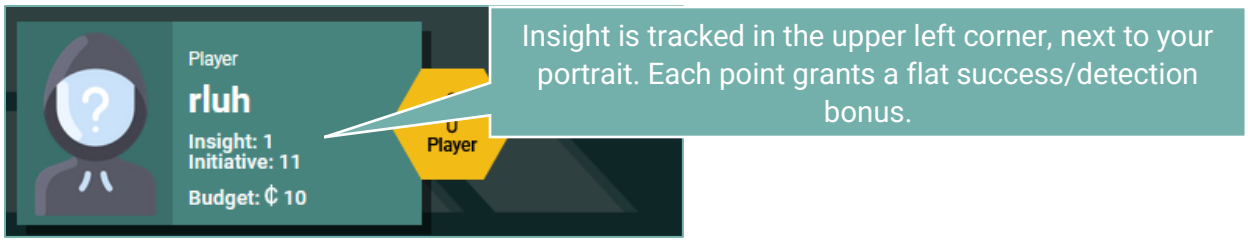


Figure 4: Player icon with current points

There is only one asset in tutorial 1 – a web server. As the attacker, you want to learn everything you can from the information shared on its public website. In turn, the defender side keeps itself informed through security advisories.

Walkthrough:

1. Attacker: Open the shop and purchase a "Web Crawler". This tool will help you with your reconnaissance.
2. Defender: Open the shop and procure a "Threat Intel Subscription", which will provide you with information about current threats coursing in the wild.
3. Attacker: Play the card "Search Victim Website" in Confidentiality mode. This will search the web server for information about employees and system settings, providing insight into the defender's operation. Draw any card to finish your turn.
4. Defender: Drag "Read Security Advisory" onto the web server (any mode). The knowledge you gain will be awarded as 1 point of Insight. Draw any card to finish your turn and the game.

In future games, it will be a viable strategy to collect more Insight if too many of your actions fail. The more you know about your opponent, the better!

Tutorial 2: Detection & damage

Dealing damage to and removing damage from assets is at the core of PenQuest's gameplay. Many action cards either add or remove damage points in one of the three scales: Confidentiality, Integrity, and Availability. Damage ranges from 1 (minor effect) to 3 (fully affected/system compromised).

Figure 5: Game board asset with damage

Tutorial 2 comprises only a web server that the attacker wants to harm.

Walkthrough:

1. Attacker: Buy the equipment card “Port Scanner”.
2. Defender: Buy “Packet Filter Firewall” from the shop.
3. Attacker: Play the attack action “Aggressive Scan” in Availability mode. This will slow the system down and deal 2 points of damage. If you would have managed to cause 3 points of “A” damage, the system would have shut down. Draw any card to finish your turn.
4. Defender: Use the action “Block Connection” to mitigate some of the damage. Observe how the damage tracker reflects your response both in the preview and on the board after playing your action. Draw any card to finish your turn and the game.

Dealing damage (and healing it) is vital: 3 points of “C” damage awards the attacker Insight, 3x “I” damage will take over the system and open up new attack routes, and 3 “A” damage will take an asset offline.

Tutorial 3: Attack stages

Attack actions are linked to an attack stage, determining when they can be played. There are three stages that each contain a number of action types (credential gathering, C2, etc.):

These stages need to be completed in sequence; you cannot use a high-impact “Execution” action without first gaining access to the system. Each access attempt is in turn preceded by recon.

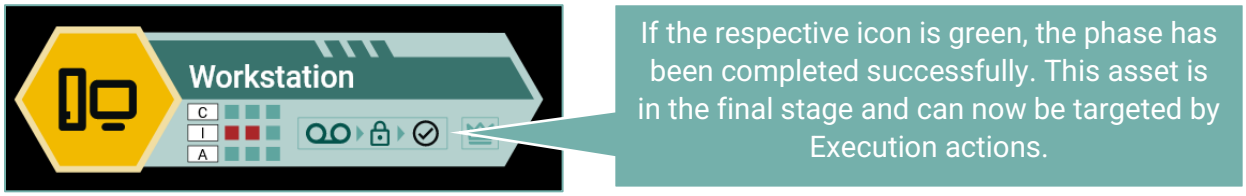


Figure 6: Attack stage indicator

There is one system in this tutorial’s infrastructure: A client workstation. As the attacker, you want to send a phishing mail to the user, executing a script that steals the cookie of an online banking session. The defender is fairly clueless in this scenario and will not mount a serious defense.

Walkthrough:

1. Attacker: Buy a “Mail Generator” from the shop. This represents tools used by the bad guys to automate the creation of (more or less) believable phishing messages.
2. Defender: You aren’t really aware of what is going on. Buy a “Banking App” to manage your finances like a pro.
3. Attacker: Play the action “Search Social Media” in any mode to complete the reconnaissance stage. This will tell you more about your victim’s preferences. Draw the card “Send Phishing Mail” from the deck. This will be your next attack.
4. Defender: Play the action “Trade Stocks”. Because why not. Draw the card “Open Funny Picture”. You are in the mood for some adorable cats.

5. Both: Skip shopping.
6. Attacker: Play the previously drawn card “Send Phishing Mail” in “C” mode. This is your way in that will complete stage 2 (Initial Access). Draw the card “Steal Cookie”.
7. Defender: What a nice mail! You open the attachment by playing the card “Open Funny Picture”. Draw “Eat Cookie”, because you are hungry.
8. Both: Skip shopping.
9. Attacker: To advance to the final stage and hijack your victim’s banking session, play the card “Steal Cookie” in “C” mode. Draw any card.
10. Defender: Eat your cookie (while losing another) and draw any card. Game over!

Keep in mind that advancing stages is usually necessary to win the game – the most powerful attacks are of type “Execution”!

Tutorial 4: System compromise

If the attacker wants to move from asset to asset, they first need to fully compromise (i.e., take over) a potential gateway system. In PenQuest, dealing 3 points of Integrity damage will unlock all attack routes originating from a compromised system.

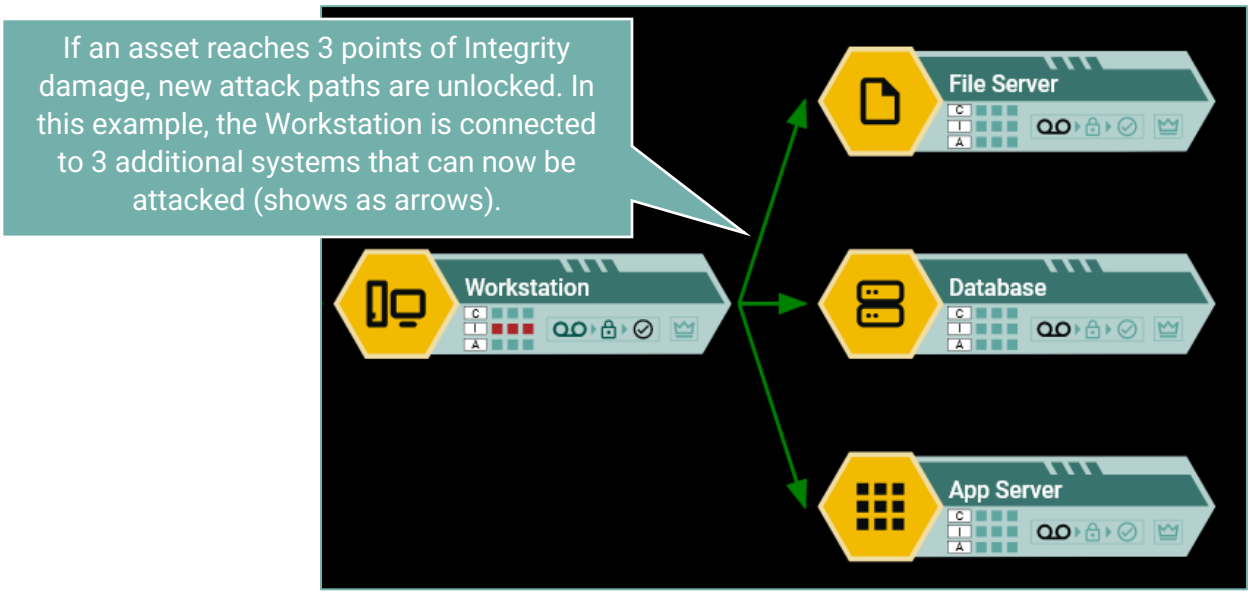


Figure 7: System compromise

There are two assets in the game: A webserver, and a database that is not exposed to the outside world by default. The attacker is something of a lucky opportunist and will discover an existing backdoor to exploit and fully compromise the server.

Walkthrough:

1. Both: Skip shopping.
2. Attacker: In our scenario, you are just plain lucky: Play “Discover Backdoor” in “I” mode to find an existing opening in the system that you can use as-is. You will immediately take over the system. Note that the database that is connected to the web server becomes visible. Draw the card “Steal Data” in anticipation of future data theft.

3. Defender: Luckily, you were alerted to the presence of the backdoor and decide to lock the account responsible for the connection: Play “Lock Account” in “I” mode. The attacker will notice this defense activity and its effect: The previously uncovered database is once again hidden, since the damage was reduced to 1. Draw any card to end the game.

Keep in mind that “I” damage is the way to go when compromising systems and unlocking new attack paths!

Tutorial 5: Damage prevention

Like in real life, most actions a defender can take are not actually responses to detected threats, but preventative measures. PenQuest models these by providing a shielding mechanic: “Prevention”-type actions absorb future incoming damage instead of healing it after the fact.

Figure 8: Damage shield

In this tutorial, there are two web server assets: the hoster’s own site and one of its customers. The attacker is only interesting in one of them.

Walkthrough:

1. Attacker: Buy a “Port Scanner”. Afterwards, click both assets on your game board and read their description to determine which is actually your victim! You don’t want to hit a random customer, after all.
2. Defender: Buy an “Intrusion Detection System” to start the game with.
3. Attacker: Kick off by scanning the (correct) system by using “Scan System”. This will complete reconnaissance. Draw the card “Brute-Force Login” for stage 2.
4. Defender: You want to be prepared for some of the more obvious attacks. Use the card “Limit Logon Attempts” on your own web server (not your customer’s). This will create a shield that will negate any damage that might be dealt through brute-force-like actions. Draw “Analyze Traffic Pattern” – it’s always good to be ready for some forensics.
5. Both: Skip shopping.
6. Attacker: Use “Brute-Force Login” (any mode) on your victim. The action succeeds, but there is no damage. Some preventative measure seems to have foiled your plans (not shown in current client; work in progress)! Now you are pissed: Draw “Denial of Service” – it’s time the annoying hoster is brought down.
7. Defender: Seems like your preventative measure was helpful. See if you can learn more (i.e., generate Insight) by using “Analyze Traffic Pattern”. Draw “Shut Down” to be ready to pull the plug, if necessary.
8. Attacker: Use your “Denial of Service” Card to deal fatal Availability damage to the server. Note that it disappears – the system is down. Draw any card.
9. Defender: Unfortunately, you do not have any backups – better to shut down the overloaded system to avoid more trouble. Use “Shut Down”. Draw any card to finish.

Damage shields are powerful! Keep in mind that the type of action must still match the attack in order to be effective. Some shields do not last forever, either.

3.2 Testing scenarios

Now that you are familiar with some of PenQuest's most important mechanics, it's time to play the game for real! Pick any of the available testing scenarios to give it a try.

Our testing scenarios are really just that: testing scenarios. Not all the action mappings are final, and we have not yet completed balancing. It is very likely you will encounter weird game situations. Also note that the game client does not yet tell the defender in advance what they are countering – this feature is work in progress!

Here is a list of available scenarios at the time of writing this guide:

- "Campaign 1, Mission 1: Ransomware": This is a simplified mission where you have to conduct (and defend against, respectively) a ransomware attack on a medium-sized business.
- "Campaign 1, Mission 2: Data Theft": This more complex scenario continues the story of the first mission and offers a lot more actions.
- "Solo Scenario: Stuxnet": In this early proof-of-concept, you will play against a bot ("Add Bot" as defender) to relive the infamous Stuxnet attack.

The remainder of scenarios is primarily used for testing but can still be played normally.

- "Normal Infrastructure Testing Scenario": These scenarios use a medium infrastructure (10 assets) and the full set of controls to mitigate/prevent attacks. Play this one if you want to test out all the options and have some time on your hands.
- "Small Infrastructure Testing Scenario": Here, the infrastructure only encompasses 6 assets – pick this one if you want to play a quick test game.
- "Large Infrastructure Scenario": There are 18 assets in this game, including several networks – pick this scenario if you have more time and want to complete several objectives.
- "Huge Infrastructure Testing Scenario": There are 36 assets in this game, making it the hardest scenario to win. Knock yourself out!

We do not really recommend you play the rest of the list – it only really exists for testing purposes. If you want to explore game mechanics without any kind of realism, you can check out the "Dumb Testing Scenario", though.

Depending on the version of the game client there might be additional options you can choose from when starting a new session. Have fun experimenting!

Please report bugs to bug@pen.quest! It would be great if you could include a screenshot and/or debug console output to enrich your description!

Thanks a bunch!

Credits

Permanent team

Sebastian Eresheim	Backend development, AI
Simon Gmeiner	Bot development, AI
Robert Luh (project lead)	Idea, security model, game rules, didactics
Thomas Petelin	Frontend & backend development, database
Maximilian Rieger (supporting member)	Visual design

Previous contributors

Thomas Bechtel	Backend
Stefanie Größbacher	Visual design, HTML, CSS
Peter Judmaier	Didactics
Vanessa Kraut	Visual design
Manuel Leithner	Backend development, AI
Gehart Marc	Testing
Florian Mayr	Lobby design, visual design, frontend development
Kathrin Neuherz	Logo, animations
Stefan Pfeiffer	Backend development
Pascal Pizzini	Security model
Gernot Rottermanner	Frontend development (Vue.js)
Michael Sailer	Didactics
Kathrin Schneller	Security model
Michael Tuchny	Didactics
Miriam Widhalm	Logo
Christoph Wiedner	Testing

Additional testing and feedback

Nicholas Lutz
Alexander Topf
Nico Wagner
Special thanks
Wolfgang Aigner
Peter Kieseberg
Hannes Raffaseder
Sebastian Schrittwieser
Simon Tjoa

Funding

InnovationCall 2019, St. Pölten University of Applied Sciences (https://www.fhstp.ac.at)
Austrian Science Fund (FWF): Project “INODES” (https://informatik.univie.ac.at/en/research/projects/project/328/)
DIH-OST Digital Innovation Hub (https://dih-ost.at/product/penquest-ein-cyber-security-spiel-fuer-planung-und-lehre/)
...and a healthy amount of spare time

Visit https://www.pen.quest for alpha access, current news, and additional material.