PenQuest Game Manual

Version 1.2.2 (08-20-2025)

> *"A penetration test, colloquially known as a pentest, 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 (penquest) is a totally made-up term describing what you are about to do in this game: playing out a cyber-attack or implementing a bulletproof defense strategy for an abstracted infrastructure in 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!

Contents

1. What is PenQuest (about)?

1.1 Introduction

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. In the game, one of the players represents the **attacker** (hacker, pentester, intelligence 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** of attack and defense actions as well as various equipment. The eponymous board typically represents an abstracted **IT infrastructure** that can range from a simple home setup to a huge company network.

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. In the following, we will expand on all the rules needed to understand and play the game.

> 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** 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!

2. Setting up the game

This section discusses the process of registering an account as well as creating and joining a game/event.

2.1 Creating an account & logging in

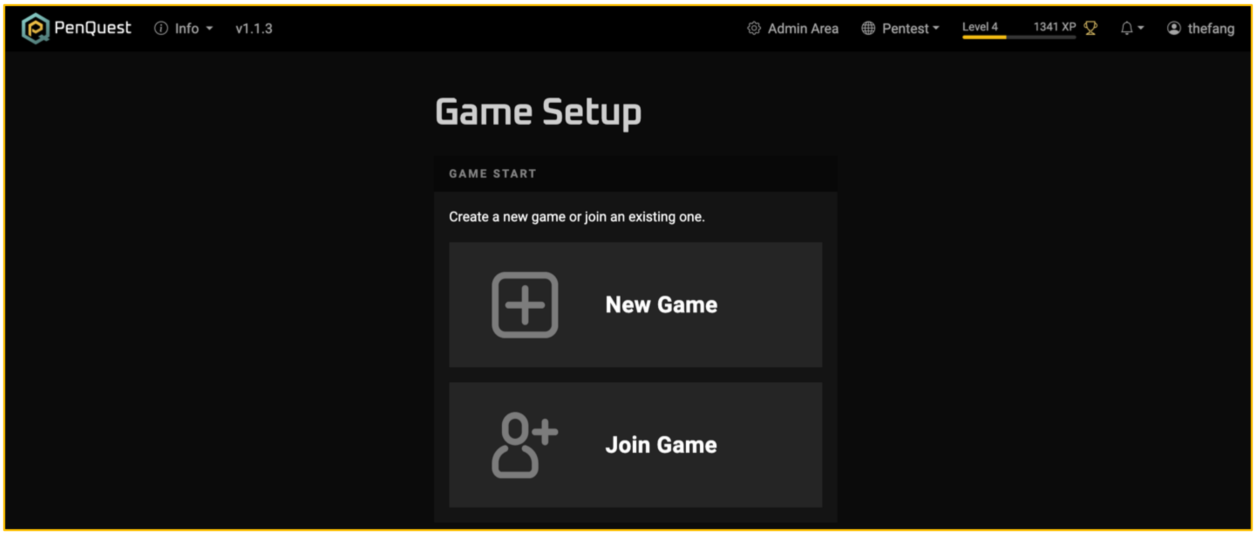
In order to create an account, you need an invitation code. This code will be sent to you via e-mail (from office@pen.quest in case you need to check your spam folder) either by the game developers or a privileged organization user. Click the link in the message within 2 days to complete registration.

> You can always change your username and password (or enable MFA) later via the main menu or by clicking “Forgot Password” on the login screen.
>
> Users at St. Pölten University of Applied Sciences can alternatively use the “FH Campus Login” button to use their student/employee account instead.

After that, you are good to go: Enter your username and password in the login window and click “Login”.

2.2 Navigating the main menu

Upon logging in, you will be greeted with the main menu (Figure 1). The big buttons in the center allow you to **create** and **join** a game, respectively. These options will be explored in the following two subsections.



Create a new game or join an existing one.

Figure 1: Main menu

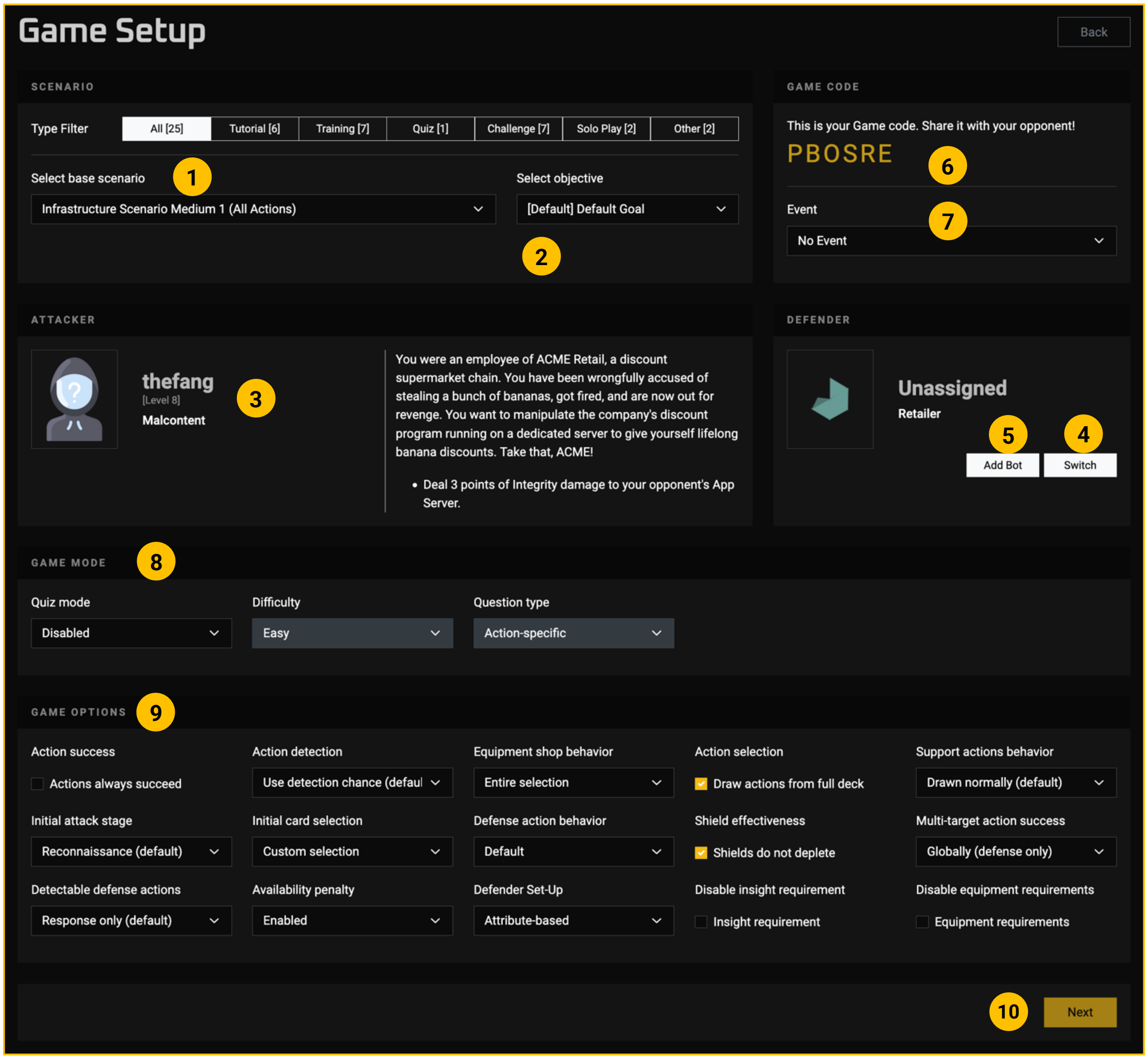
Other than a logo and an **info** menu (About, Imprint, version number), the menu bar at the top shows (from left to right) the current **realm**, which defaults to the public “Community” realm but may instead show your own (private) organization that, if you are its manager, show a link to an **admin area** that provides user management.

Next to the realm you see your current **player level** and **experience points** (XP) as well as the “cup” shortcut that will show the current high scores. The **notification bell** to the right will light up if you receive new messages such as event invites.

In the rightmost corner you see your **username**. Clicking it will bring you to a new screen that allows you to change your details (name, password, avatar, etc.) and log out.

2.3 Creating a game

Clicking “New Game” will bring up the game’s lobby (Figure 2). This is where you configure your new adventure.



Game Setup

SCENARIO

Type Filter: All [25] | Tutorial [6] | Training [7] | Quiz [1] | Challenge [7] | Solo Play [2] | Other [2]

Select base scenario: Infrastructure Scenario Medium 1 (All Actions)

Select objective: [Default] Default Goal

GAME CODE

This is your Game code. Share it with your opponent!

PBOSRE

Event: No Event

ATTACKER

thefang
[Level 8]
Malcontent

You were an employee of ACME Retail, a discount supermarket chain. You have been wrongfully accused of stealing a bunch of bananas, got fired, and are now out for revenge. You want to manipulate the company's discount program running on a dedicated server to give yourself lifelong banana discounts. Take that, ACME!

- Deal 3 points of Integrity damage to your opponent's App Server.

DEFENDER

Unassigned
Retailer

GAME MODE

Quiz mode: Disabled

Difficulty: Easy

Question type: Action-specific

GAME OPTIONS

Action success: □ Actions always succeed

Action detection: Use detection chance (defaul

Equipment shop behavior: Entire selection

Action selection: ☑ Draw actions from full deck

Support actions behavior: Drawn normally (default)

Initial attack stage: Reconnaissance (default)

Initial card selection: Custom selection

Defense action behavior: Default

Shield effectiveness: ☑ Shields do not deplete

Multi-target action success: Globally (defense only)

Detectable defense actions: Response only (default)

Availability penalty: Enabled

Defender Set-Up: Attribute-based

Disable insight requirement: □ Insight requirement

Disable equipment requirements: □ Equipment requirements

Figure 2: Game lobby

Scenarios

Scenarios are how PenQuest delivers its player experience. They can be freely defined by a game architect (this is currently us but will be opened to the community in the future). Scenarios define the infrastructure and goals and may contain only a subset of actions to train certain situations. Some scenarios are basically a “free for all” and do not limit you in any way. Since those may be overwhelming for beginners, filter for **scenario types**: “Training” scenarios with limited actions are typically better suited to get started than “Challenge” scenarios with a full action set.

If you prefer to test your knowledge instead or in addition of your strategic skills, play a “Quiz” mode game or activate **quiz mode** via game mode (8) for a compatible scenario of your choosing.

To begin the process, select a **base scenario** (1). The default **game objective** will be selected when you do. Since some scenarios have alternative goals for you to choose from, feel free to select them by opening the objective menu (2).

Roles

Underneath the scenario and goal selection you can see your **current role** (3). By default, the player who creates the game acts as the attacker. If you want to switch your role to that of the defender, click “Switch” (4). If you want your opponent to be computer-controlled, click “Add bot” (5). If you want to play against a fellow human, take note of the game code in the upper right corner (6).

No matter who you want to play as, a brief **mission summary** is displayed next to the role description. This will be explained in more detail in subsection “

Game objectives”.

For finetuning or fundamentally changing your PenQuest experience, look at “Game mode” and “Game ” sections below. Otherwise, skip to Section 2.4. When both players are ready, they can click “Next” (10) to continue.

Game mode

Game mode (8) allows the lobby creator to switch between alternative ways to play the game. Currently, we have implemented one additional mode in addition to PenQuest’s default, strategy-driven gameplay:

- **Quiz mode** (Disabled | Modify Success | Determine Success): Quiz mode is an entirely new way to play PenQuest. Depending on the specific option, the success of actions will either be determined by the player answering correctly a quiz question, or they will receive a bonus of for a correct answer. This way, it’s not only the player’s strategic and tactical acumen that will decide the game, but also their domain knowledge.
    - If quiz mode is enabled, you can choose the difficulty of the questions (Easy | Moderate | Hard) and…
    - …whether the questions are specific to the action currently played (recommended) or randomly drawn from a number of general security questions.

> Please note that, since there are hundreds of actions currently in the game that need to be quizzed, we have generated most quiz questions using an LLM. Therefore, the accuracy of the answers should always be challenged.
>
> If you notice inaccuracies or incorrect answers, please let us know!

Game options

Game options (9) are a means to **customize your experience**. They exist to make a game more (or less) realistic, offer additional strategic depth, or reduce complexity for beginner use cases. Note that options can be pre-set by a scenario in line with its educational goals and might even be fixed. Most of the time, however, they are freely configurable. Here is the list of current **options**:

- **Action success**: When this checkbox is ticked, all actions will automatically succeed. Use this to eliminate chance in e.g., educational settings.
- **Action detection** (Use detection chance | Always detect, if detectable | Always detect): This option determines when actions are detected by the defender. Using the detection chance defaults to the value on each action card, while the latter to options will always unveil the attacker's activity, provided the action can realistically be detected – or no matter what.
- **Equipment shop behavior** (No shop | Random selection | Entire selection): This option controls the equipment shop. You can disable equipment entirely (which will also eliminate equipment requirements on action cards), set it to provide a random selection of items each turn (less choice for faster gameplay), or set it to always offer everything as per the scenario definition (most realistic).
- **Action selection**: This box makes sure that the players can always draw action cards from the full deck defined through the scenario. If you uncheck this, only a handful of playable actions will be offered. This makes the game easier but significantly reduces strategic options.
- **Support actions behavior** (No support actions | Drawn normally | Always on hand): Support actions can be played alongside normal actions to provide bonuses. Since they make the game more complex, you can switch them off here. Alternatively, you can opt to always have all support actions readily available in your hand – no need to draw them at all. This offers more flexibility and gameplay variety. Use this to represent an especially crafty attacker.
- **Initial attack stage** (Scenario defined | Reconnaissance | Initial Access | Execution): The attack stage determines the state of the assets at the beginning of the game. Normally, the attacker starts from scratch (Reconnaissance). With this option, you can tell the game to begin with a later state; if set to Initial Access, the game assumes that the attacker has already completed recon and is ready to make their way inside. Execution means that the attacker already has access to all assets. Use this to make the game shorter and more action heavy.
- **Initial card selection** (Random cards | Playable cards only | Custom selection): This setting controls which actions are available in the first turn. Random cards can be anything – even those you cannot currently use because of e.g., equipment constraints. Playable cards can be used immediately but are typically very basic. For experienced players, the custom selection allows them to build their starting hand in accordance with their strategy. This makes for a more exciting and strategic game.
- **Defense action behavior** (Default | Convert to… | Offer only…): There are three kinds of defense actions (we'll get to that). With this option, you can either overwrite their type and set it to something else (e.g., changing all prevention measures into response actions that can be used after an attack instead of ahead), or force the game to only provide the attacker with a certain type of actions. Use this option with care; you might break your game.
- **Shields do not deplete**: If you set this option, all the defender's successful prevention measures will last forever, making certain attacks impossible for the rest of the game. Without this checkbox, prevention actions eventually expire or are "used up" by certain attacks. Use infinite shield duration for more realistic gameplay that, however, may not be as accessible.
- **Multi-target action success** (per asset | globally (defense/attack/all)): Some actions in the game affect several assets at once. By default, the game determines the success of such actions on each asset individually. With this option, you can switch this to a "global" success or fail, which is more intuitive. "Globally (Defense only)" is arguably the most realistic option.
- **Detectable defense actions** (Response only | Prevention & response | Detection & response | All defense actions): The attacker does not normally see what the defender is doing. Only

immediate responses to attacks are disclosed. With this option, you can change that and include other types of defense actions. Use this to play "openly" in educational settings.

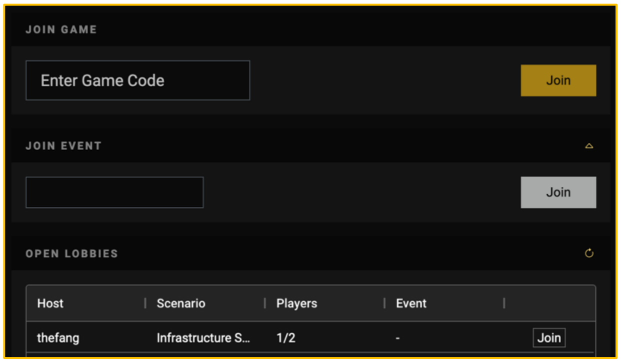
- **Availability penalty** (Enabled | Disabled): A scenario can define a penalty (money, automatic defeat, etc.) when one of the defender's assets is taken offline for too long. You can override this by switching this option to disabled.
- **Defender set-up** (Scenario-based | Attribute-based | Disabled): Defender set-up allows the defender to play some actions for free before the game starts. This establishes a security baseline, which is more realistic than starting with an entirely unsecured infrastructure. Like "Initial card selection", it needs more insight into the game and is not recommended for beginners. It is a powerful tool for risk exploration, however. Simply replicate your security status quo in the game before letting loose the attacker. Set this option to "attribute-based" if you want to force its use; otherwise, you have to rely on the scenario to enable it.
- **Disable insight** & **equipment requirements**: If checked, action constraits imposed by the actor's current Insight value or the lack of purchased equipment are lifted.

Keep your eyes open for new game options – we are tuning this list constantly to provide more, well, options.

Note that the default for some actions may also change. If the game does not behave the way you want, open a new lobby and check/alter the settings.

2.4 Joining a game

Now that one player has created a game and keeps the lobby open, another player can **join**. Click "Join game" in the main menu to be brought to this screen:



JOIN GAME

Enter Game Code | Join

JOIN EVENT

Join

OPEN LOBBIES

Host	Scenario	Players	Event	
thefang	Infrastructure S...	1/2	-	Join

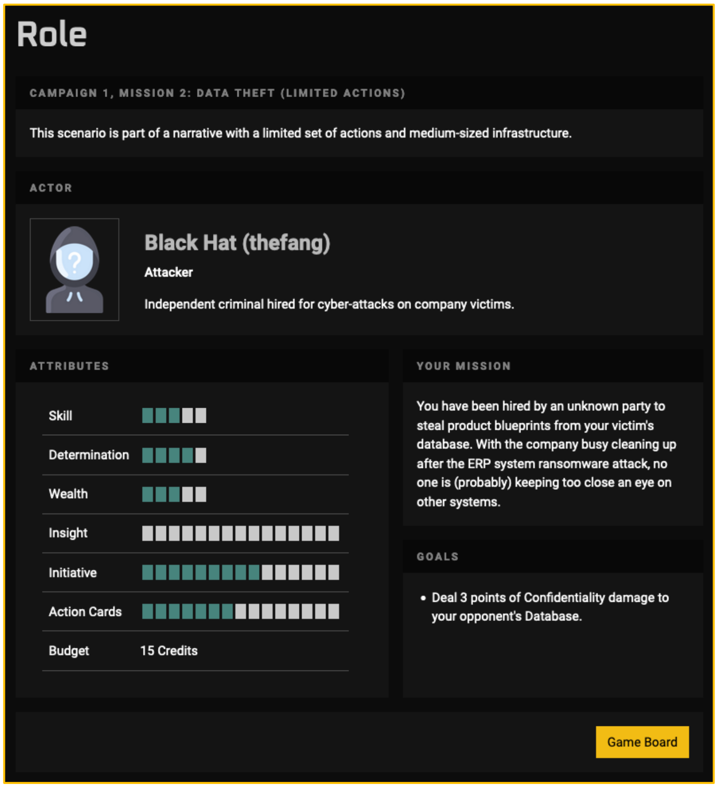
Figure 3: Game join menu

Either enter a **game code** that was shared with you or pick the respective game from the **list** and click "Join". You will be taken to the lobby and see the perspective of the *other* actor, depending on which slot Player 1 left open.

Both players can now click "Next" (9) to continue. After a loading screen with some optional meta information, clicking "Next" (or pressing Enter) again will bring you to the game objectives and actor details.

Game objectives & actor details

This screen offers you **detailed information** about your alter ego and game objective(s):



Role

CAMPAIGN 1, MISSION 2: DATA THEFT (LIMITED ACTIONS)

This scenario is part of a narrative with a limited set of actions and medium-sized infrastructure.

ACTOR

Black Hat (thefang)

Attacker

Independent criminal hired for cyber-attacks on company victims.

ATTRIBUTES

Skill	🟩🟩🟩⬜⬜
Determination	🟩🟩🟩🟩⬜
Wealth	🟩🟩🟩⬜⬜
Insight	⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜
Initiative	🟩🟩🟩🟩🟩🟩🟩🟩🟩⬜⬜⬜⬜⬜⬜
Action Cards	🟩🟩🟩🟩🟩🟩🟩⬜⬜⬜⬜⬜⬜⬜⬜
Budget	15 Credits

YOUR MISSION

You have been hired by an unknown party to steal product blueprints from your victim's database. With the company busy cleaning up after the ERP system ransomware attack, no one is (probably) keeping too close an eye on other systems.

GOALS

- Deal 3 points of Confidentiality damage to your opponent's Database.

Figure 4: Role & game objective screen

As depicted in Figure 4, “Actor” defines your **role**, “Your mission” provides a bit of **narrative**, and “Goals” lists your **objective** in game terms. In our case, we are supposed to deal 3 points of Confidentiality damage to the defender’s database. See subsection “Attacking an asset” for more information.

Lastly, we see our persona’s **attributes**. They are defined in the scenario and determine which actions are at our disposal, how many cards we have at our disposal every turn, and how much money we have available for shopping. Here is a breakdown:

- **Skill** (1..5): IT security knowledge of the actor. This enables the use of more sophisticated attacks as well as defense measures and provides a bonus to action success and detection.
- **Determination** (1..5): Motivation to go above and beyond. Motivation increases the number of turns before the attacker gives up and provides you with a larger hand of cards.
- **Wealth** (1..5): Money available to buy equipment. Each point translates to 5 in-game credits.
- **Insight** (0..15): Level of knowledge about the opponent. Each point provides a bonus to action success and detection chances.
- **Initiative** (0..n): Turns available for the attacker to reach their goal. This number can either be set through the scenario or is derived from Determination.
- **Action Cards** (3..8): Number of cards on hand. Derived through Skill and Determination.
- **Budget**: Monetary unit for purchasing equipment. Derived from Wealth. The defender earns a fraction of this amount each turn as part of their war chest; the attacker has to make do with what they have or generate money through illegal means (e.g., ransomware attacks).

Mouse over the attributes for an explanation of the value displayed. When you are ready, click “Game Board” or press Enter to start the game for real.

Skip to Section 3, “Playing the Game”, or keep reading to learn about events.

2.5 Joining an event

Events are time-constrained game challenges that are either by invite or require an event code to join. To join an open event by code (you will get one from the event organizer, typically in person or by mail), enter it in the “Join Game” screen by expanding “Join Event”. For invited events, check the notification bell in the top menu bar to any accept pending invites.

Once you have joined an event you can create or join games created within its context. If you try to join a game that is part of an event you haven’t joined, an error message will be displayed.

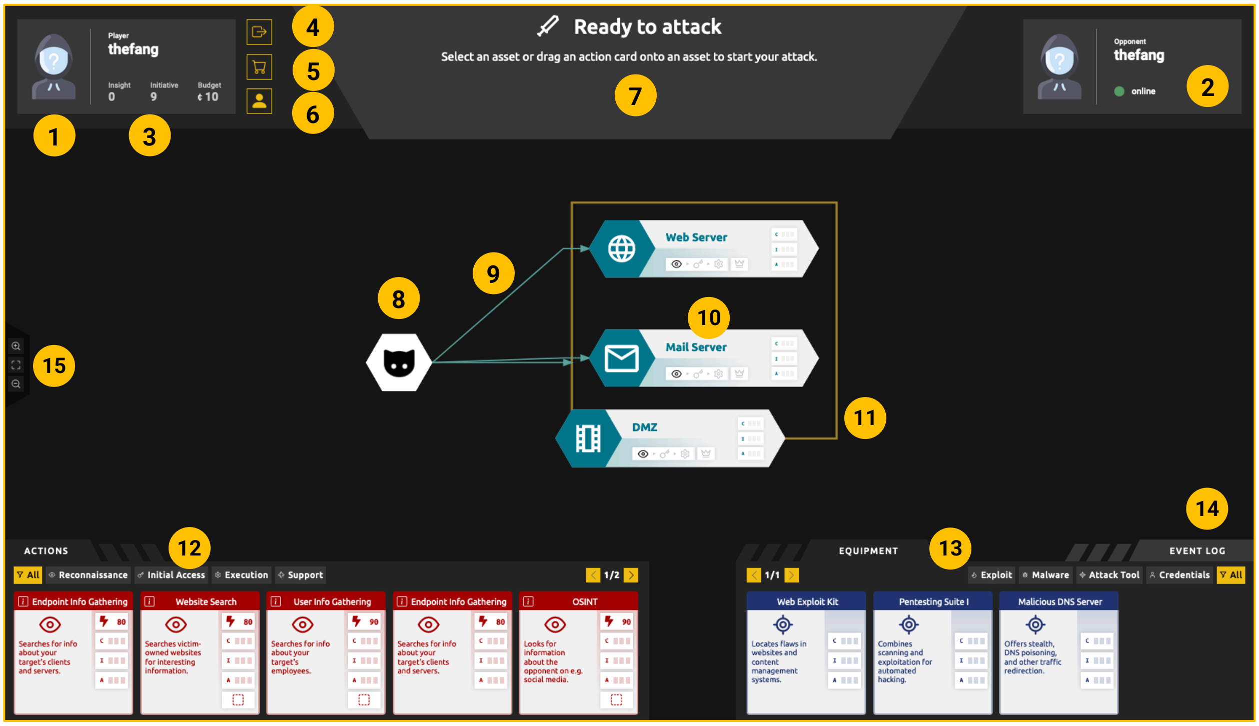
> Events are used to keep track of XP independent of the global score, meaning that an event can have a clear “winner” in terms of accumulated experience points. In the future, we will also provide a tournament mode for additional fun.

3. Playing the game

This section introduces the game's interface as well as game loop. Keep reading to know how it all ties together!

3.1 Understanding the interface

When entering the game, you will be greeted by the game board (Figure 5).



Ready to attack

Select an asset or drag an action card onto an asset to start your attack.

Endpoint Info Gathering 80: Searches for info about your target's clients and servers.

Website Search 80: Searches victim-owned websites for interesting information.

User Info Gathering 90: Searches for info about your target's employees.

Endpoint Info Gathering 80: Searches for info about your target's clients and servers.

OSINT 90: Looks for information about the opponent on e.g. social media.

Web Exploit Kit: Locates flaws in websites and content management systems.

Pentesting Suite I: Combines scanning and exploitation for automated hacking.

Malicious DNS Server: Offers stealth, DNS poisoning, and other traffic redirection.

Figure 5: Game board

Let's go over the individual **elements**:

(1) Player **avatar**, **role**, and **name**.

(2) The **opponent**'s **avatar**, **role**, and **name** as well as their **online status**.

(3) From left to right: The player's current **Insight**, **Initiative** (turns remaining; only as attacker), and **budget** in credits.

(4) The "Surrender" button (i.e., **Quit** game button): Clicking this will forfeit the game and offer a game summary as well as display the actual "Leave Game" button. Note that closing the tab without surrendering/leaving will keep the game open.

(5) **Shop**: This opens the on-demand shop, an overlay that offers equipment to procure (see "Shopping" as well as Figure 6).

(6) Game objectives & player details: This button reopens the **role screen** shown in Figure 4.

(7) **Info box**: This central element provides you with **important game messages** and calls to action. If you are unsure about what to do next, look here. Depending on the context, a button may be displayed (e.g., for drawing new cards).

(8) The Evil Cat: This icon represents the outside world, i.e., the **attacker**.

(9) Arrows denote **connections** between assets. If the attacker compromises an asset, they unlock all connections originating from said asset. Dotted lines permit only certain attacks.

(10) An **asset** (i.e., system). The hexagonal shape displays **status information**, **damage**, and as well as the asset's current **attack stage**. More on that later!

(11) Asset-within-an-asset. This is used to represent things like network segments. Attacking the outer asset usually has an effect on the ones within.

(12) **Actions on hand**. These are the actions (i.e. attacks, defense measures) the player can choose from. Drag and drop an action onto an asset (if targeted) or into the empty space on the central board (if untargeted, multi-targeted). See Section 3.3 for more info.

(13) Equipment **inventory**. All items procured or gathered are listed here. Equipment is used automatically in many cases. See Section 3.4 for more information.

(14) **Event log** tab. Clicking here will switch from the equipment list to the event log, which displays details about the game that may be useful for advanced players.

(15) **Zoom** buttons: Use them to change the view on the game board for better overview.

Note that the action and equipment list provide **filters** for certain types of cards. **Paginators** provide a means to switch between multiple pages of actions and items.

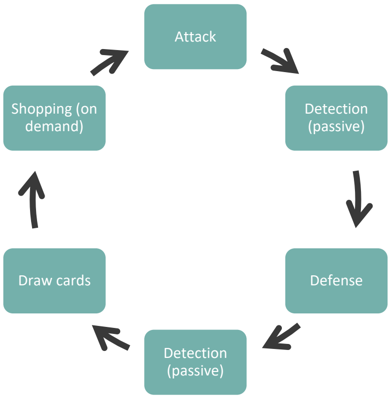
Many UI elements allow the use of the mouse wheel: For example, it will zoom in or out of the assets or switch between pages of actions or equipment – depending on where you have placed your mouse pointer.

BTW: If any game elements overlap, alter your DPI settings (anything above 100% will cause issues) or zoom out using your browser's zoom function.

3.2 Understanding the game sequence

In short, the general **game sequence** looks as follows, whereas the actual **loop** (pictured on the right) only starts with point 3 and repeats these stages until the game ends.

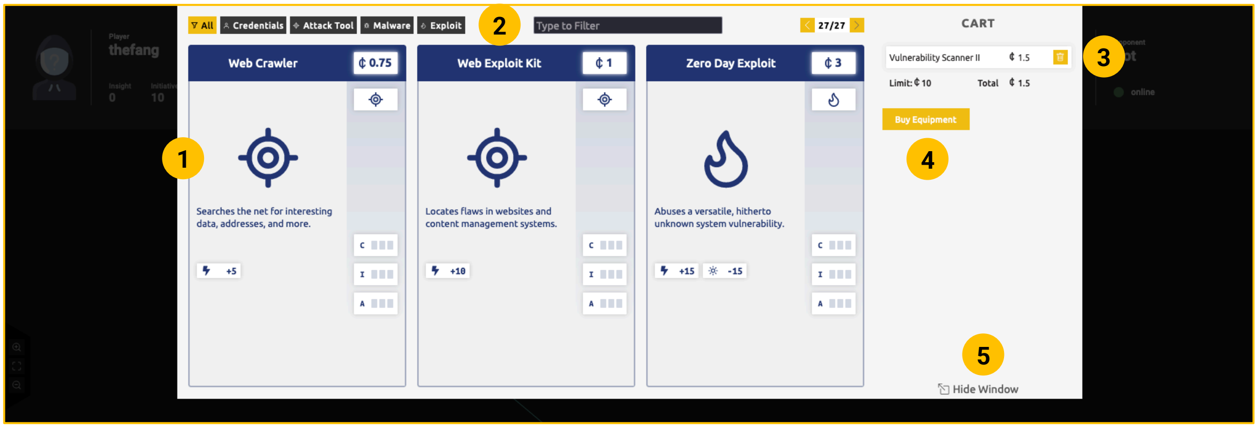
1. Defender **set-up** (optional, via game option): The defender plays a number of actions to establish a security baseline.
2. Attacker and defender put together their **hand** (optional, via game option)
3. Both players go **shopping** (optional, any time they want)
4. **Attacker plays action(s)**
    - Defender detects the attack (or not)
5. **Defender plays action(s)**
    - Attacker detects the action (or not)
6. Both players **draw new cards** to replenish their hand
7. (repeat from 3)



This, in a nutshell, is the PenQuest game loop. Refer to the following subsections for more information.

Shopping

Players can **procure new equipment** any time they want. Simply click the shopping cart icon in the upper left corner of the game board.



Searches the net for interesting data, addresses, and more.

Locates flaws in websites and content management systems.

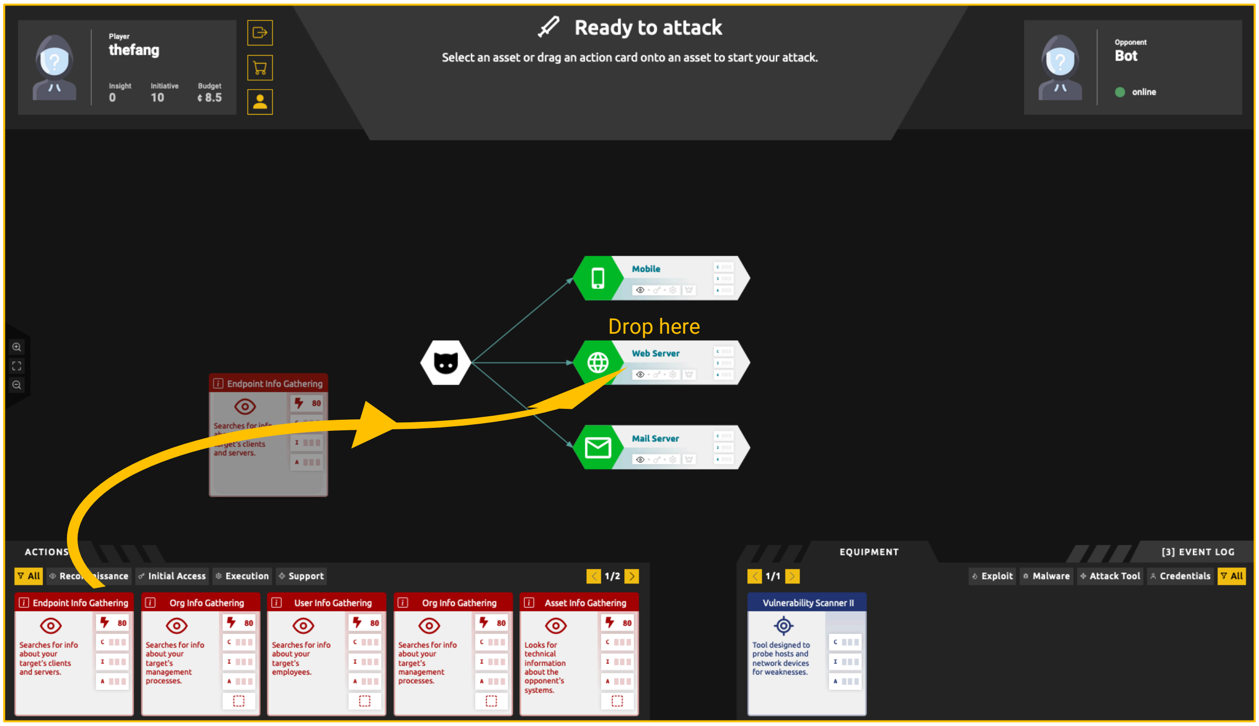
Abuses a versatile, hitherto unknown system vulnerability.

Figure 6: Shopping interface

The **available equipment** (1) is shown as full-size card. You can mouse over some icons on the card to get an explanation of the effect. Above the card are the type **filters** and a **search** bar (2) that help you look for specific items. Click an equipment card to add it to your **shopping cart** (3). Click the trash bin icon to remove it again. Once you are happy with your selection, press “Buy Equipment” (4). Alternatively, hide the window (5) to return to the game board.

Attacking an asset

Attacking an asset with a **single-target** attack card is as simple as **dragging** the action **onto that asset**. If the attack can be launched (i.e., all prerequisites are met), the asset will light up green:



Select an asset or drag an action card onto an asset to start your attack.

Searches for info about your target's clients and servers.

Searches for info about your target's management processes.

Searches for info about your target's employees.

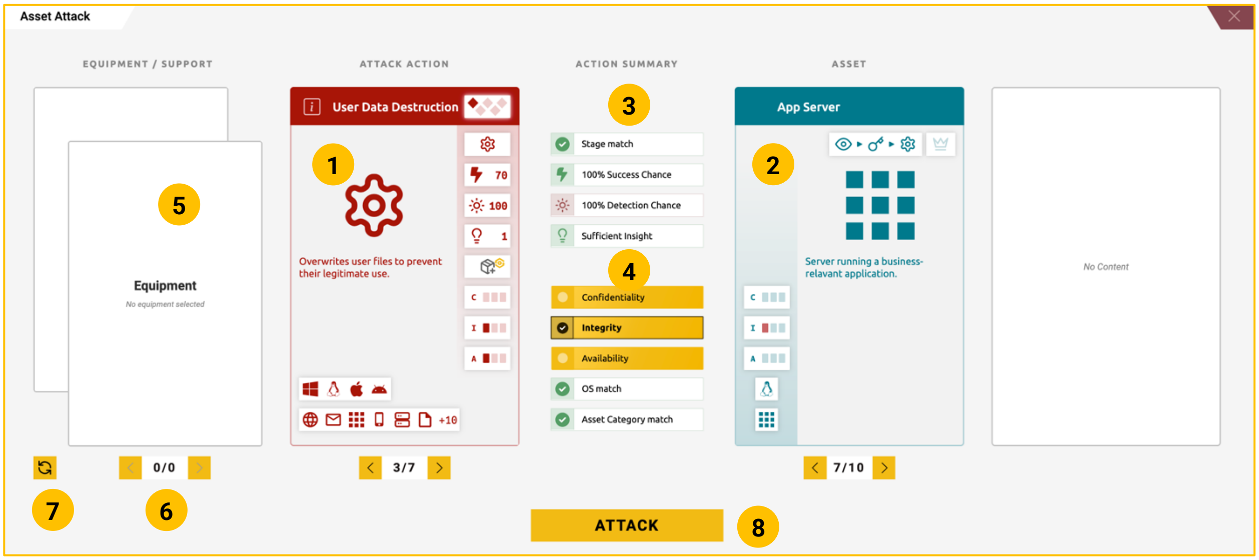
Searches for info about your target's management processes.

Looks for technical information about the opponent's systems.

Tool designed to probe hosts and network devices for weaknesses.

Figure 7: Playing a single-target action

Untargeted actions (marked with a dotted ⬚ icon in the lower right corner of the small card) and **multi-target** actions which hit several assets at once (⛶ icon) can be dropped anywhere on the game board.



Overwrites user files to prevent their legitimate use.

Server running a business-relavant application.

Figure 8: Attack window

When you drop the card (be it targeted or not), the **attack window** (Figure 8) will open. The chosen action (1) and target (2) are displayed in the center. The **action summary** (3) provides information about the attack: Whether the stage matches, the projected success and detection chance, and whether all necessary equipment or Insight is available. Below that is the **damage selector** (4). Here, you can pick which type of damage you want to cause. Note that some actions deal no damage or have their damage type pre-selected.

On the left of the action, you can add **optional equipment** and **support actions** (5). You can add them by clicking the paginator (6) or by using the mouse wheel. Click (7) to switch between equipment and support action selection.

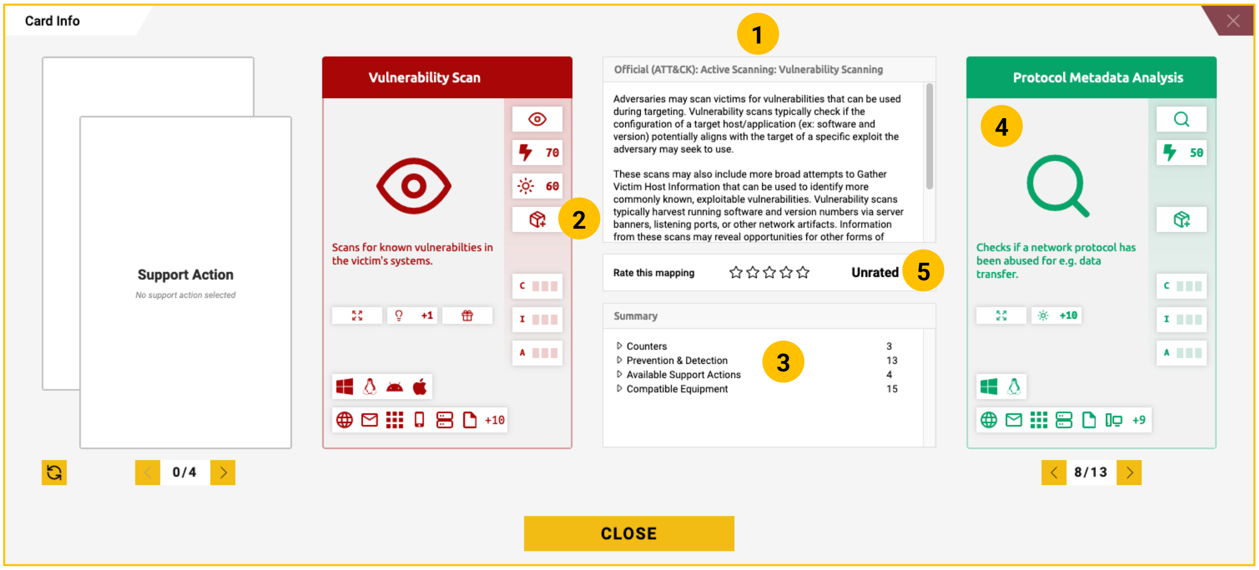
Once you are ready and there are no error messages, hit "Attack" (8). If you want to abort, hit the red X in the upper right corner.

Learning more about an action

If an action can't be played and you want to figure out why, or if you want to know more about an action in general, you can always click on the **[i]** icon or anywhere on the small action card itself. This will take you to the "**Card info**" window (Figure 9). Here, you can read the official description of the attack (1, taken from e.g. MITRE ATT&CK) as well as check the card's effects and equipment prerequisites (2).

In addition, the "Summary" box will tell you how that particular attack could be countered, prevented, or detected as well as which support actions and equipment it is compatible with (3). When you click and card from the expandable list, it will be shown in the respective field. In our case, a compatible defense action will be displayed (4).

The mapping itself can be rated (5) to help us improve the game. Thank you kindly!


Card Info
Support Action
No support action selected
0/4
Vulnerability Scan
70
60
Scans for known vulnerabilties in the victim's systems.
+1
+10
1
2
3
4
5
Official (ATT&CK): Active Scanning: Vulnerability Scanning
Rate this mapping ☆☆☆☆☆ Unrated
Summary
Counters 3
Prevention & Detection 13
Available Support Actions 4
Compatible Equipment 15
Protocol Metadata Analysis
50
Checks if a network protocol has been abused for e.g. data transfer.
+10
+9
8/13
CLOSE

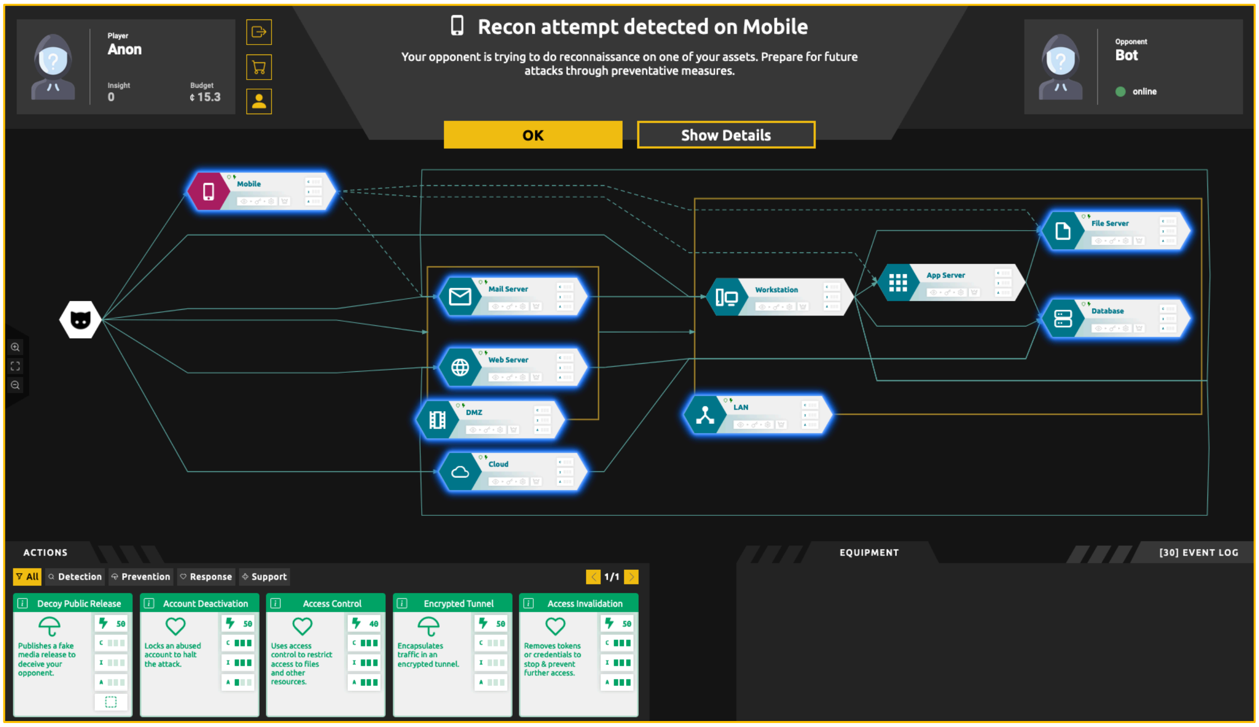
Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to Gather Victim Host Information that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts. Information from these scans may reveal opportunities for other forms of

Figure 9: Card info window

Detecting an attack

Detection is done passively and will be dependent on many factors: The defender's equipment, their active detection actions, their attributes, and a certain amount of luck. If you **detect an attack** in your current turn, it a warning will be shown in the info bar (Figure 10). In addition, all affected assets will be highlighted in purple. Note that detected attacks do not necessarily need to be successful ones; even attempts like the one shown below can often be spotted. Check the text and details ("Show Details") if you want to know more.



Recon attempt detected on Mobile

Your opponent is trying to do reconnaissance on one of your assets. Prepare for future attacks through preventative measures.

Publishes a fake media release to deceive your opponent.

Locks an abused account to halt the attack.

Uses access control to restrict access to files and other resources.

Encapsulates traffic in an encrypted tunnel.

Removes tokens or credentials to stop & prevent further access.

Figure 10: Detection warning

Once you feel sufficiently informed, click “OK” to dismiss the message and get ready to defend.

Don’t worry if you dismiss the message too quickly. You can always check out the details later by clicking the targeted asset and selecting “Show History”.

Additionally, the event log in the lower right keeps track of every action played.

Defending an asset

It’s now the defender’s turn to act. Playing a **defense** action works exactly like an attack: Simply drag and drop the action onto the asset (single-target) or on somewhere on the board (untargeted, multi-target). The defense window offers the same information and options as previously discussed. Click “Defend” to execute your action.

If the defense action is detectable or the respective game option is set, the attacker will also be informed via the info bar about which action the defender has played.

Drawing action cards

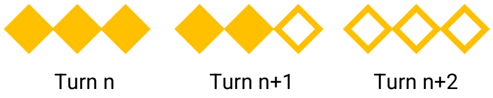
Whenever actions have been played, the players get to **replenish their hand**. The game will inform you via the info bar that you can draw cards. Click the respective button and add the new card(s) to your cart – just like you did when shopping. If you have played several cards, you get to draw that number of new cards. Once your hand is replenished, it’s the attacker’s turn again and game loop starts over.

3.3 Using actions

So far, we have only talked about the user interface and the general game loop. It is now time to go into detail and take a closer look at the **actions**.

Action Point cost

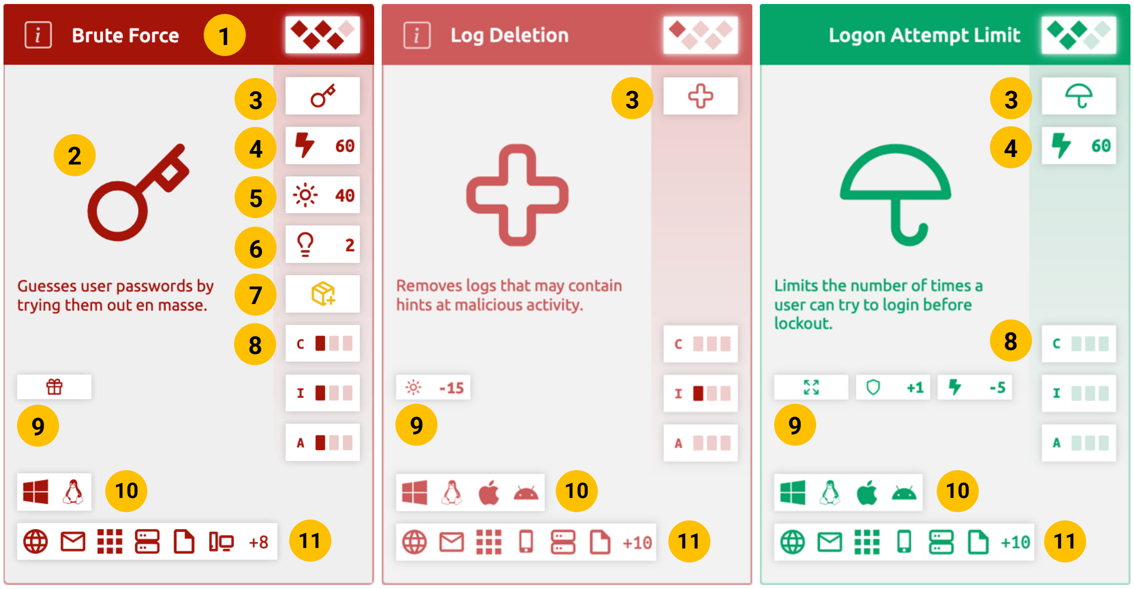
First of all, it is important to know that each action comes with a cost of so-called **Action Points** (AP). These AP represent the time required to implement an action and ranges from 1 (immediate) to 5 (long-term implementation). 3 AP represent one turn. This means that the most time-consuming action uses 2 additional AP from the next turn, thereby reducing the maximum available AP in that follow-up turn. No more that 2 AP from the following turn may be used in any situation. Whenever your AP budget is not full, you are allowed to skip the turn to refill it.



Example: *An action played in Turn n costs 5 AP. In the subsequent turn, the player may use up to 3 AP (1 AP remaining in Turn n+1 and 2 additional AP from Turn n+2).*

Main & support actions

There are two fundamental types of actions: main and support actions. **Main actions** (solid red for the attacker and green for the defender) are what you drag on the game board. They represent the task you perform. **Support actions** (light red) do not exist on their own; they aid in your endeavor by providing bonuses for the main action. They typically signify things like evasion techniques.



Guesses user passwords by trying them out en masse.

Removes logs that may contain hints at malicious activity.

Limits the number of times a user can try to login before lockout.

Figure 11: Main and support actions

Each action card comes with a number of visual **elements**:

(1) **Title, information link**, and **AP cost**: Name of the card and link to the “Card info” window on the left, and AP cost (1 to 5) on the right.
(2) **Card icon**: Pictogram representing the card. This is currently the same as (3).
(3) **Attack stage indicator** (attack), **support** icon (support), or **defense action type** (defense): See the subsections below for more information.
(4) Base **success chance** in percent. Note that this number can be modified in many ways; unbeknownst to you, even your opponent may alter this chance.
(5) Base **detection chance** in percent: The higher the number, the more likely it is that the defender spots the attack.
(6) **Insight requirement**: Number of Insight points required by the actor to play this action.
(7) **Equipment requirements** and **quick-buy button**. Mouse over this icon to see the equipment required to play this action. Note that you need only one of the listed items, not all of them. Click the icon to purchase any of the items directly from the current screen.
(8) **Damage** (attacks & support actions) or **healing** (defense). See below for more info.
(9) **Card effects**, of which there are many. See below for a list of possible effects. Support actions transfer their effects onto their main action.
(10) Compatible **operating systems**. Each asset runs a certain OS (click the asset to find out) the card needs to be compatible with.
(11) Compatible **asset types**. This list (tooltip available) shows which assets (web servers, workstations, IoT devices, etc.) can be targeted by the card.

Success & detection chance

As mentioned before, **success chance** is a highly relevant metric. Don’t despair if an action is very unlikely to succeed as-is; chances are it will benefit from certain equipment that will turn a mediocre choice into an effective tool.

When it comes to **detection**, the attacker needs to keep in mind that the clock (Initiative) will only start to tick down once the defender managed to detect an action for the first time. Picking less aggressive actions or playing support actions to evade detection might be the key to success.

Attack stage

The attacker needs to advance through so-called **attack stages** in order to fully compromise a system. You can only play an action of the following stage after an action of the previous stage has been successfully played. There are 3 stages, which represent a simplified kill chain model:

- **Reconnaissance**: In this stage, the attacker gathers information about an asset or the organization itself. If successful, they know enough to proceed.
- **Initial Access**: This stage is about getting into an asset and establishing a first foothold. Once successful, the attacker can get started in earnest.
- **Execution**: These actions are all about causing damage and reaching the attacker's goal.

The respective icon on the asset (see Figure 12, left) will light up once the attacker has unlocked a new stage. Match the icon to the card you want to play.

Defense action types

Defense action types are the defender's equivalent of the attack stage. Here, they do not represent a certain attack maturity but a **fundamental type** of action they can use. There are 3 of said types:

- **Detection**: These actions are all about boosting the detection chance against certain types of attack. Depending on their specific effects, this boost may last only briefly or for several turns.
- **Prevention**: Preventative actions negate incoming damage before it is applied to an asset. This "shield" may last forever or only briefly and may have diminishing returns over time. Shields absorb anything from 1 to 3 damage points.
- **Response**: These actions represent incident response measures which heal damage that was dealt by the attacker.

It's a good idea to start the game with a solid mix of detection and prevention measures in place.

Damage, healing & prevention

Referencing the infamous CIA triad, **damage** in PenQuest is modeled in 3 dimensions and ranges from 0 (no damage) to 3 points (full compromise):

- **Confidentiality** damage represents data theft; if an asset reaches 3 "C" damage, all valuable data on that asset is considered stolen. Three points of "C" damage also generate 1 point of Insight for the attacker.
- **Integrity** damage stands for the malicious modification of data or a system's configuration. If the attacker manages to score 3 points of "I" damage, they take over the system and unlock all attack paths leading to other assets.
- **Availability** damage is synonymous to denial-of-service attacks; with 3 points of "A" damage, the asset will be taken offline. Defender penalties may apply when this happens.

Damage prevention negates damage, shielding the asset from harm. Protected assets are shown with a blue outline (see Figure 12, right). Keep in mind that prevention measures protect only against certain attacks!

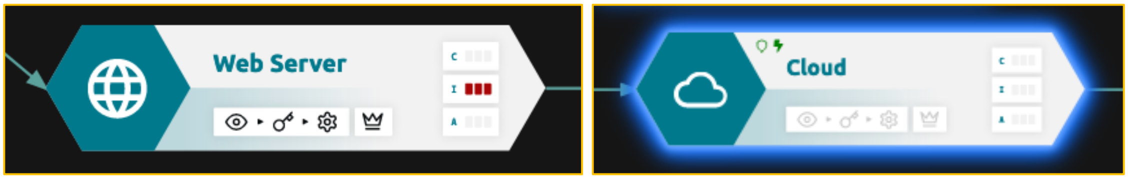


Figure 12: Asset attack stages, damage, and shield

The ♕ icon on the asset represents the attacker's administrative privileges which are granted by certain actions (see below).

Effects

Cards can have a multitude of **effects** that correspond to various game mechanics implemented in PenQuest. Grey icons represent effects that are found on both attack and defense cards, while red or green icons are unique to their side.

💡 +1 **Insight gain**: This effect grants a number of Insight points which in turn provide bonuses for future attacks or defense measures. Insight points are often prerequisites for more complex attacks.

⚡ +5 **Success boost**: (Support) actions with this effect increase the player's success chance.

⚡ -5 **Success penalty**: Actions with this effect reduce the opponent's success chance.

🎁 **Item gathering**: This action has a chance to grant equipment cards such as credentials, exploits, or fixes. Granted equipment is automatically placed in the player's inventory.

₵ -0.25 **Cost**: Actions with this icon cost money to play. Note that this cost may be multiplied by the amount of assets affected; read the tooltip to find out. If the cost exceeds the player's budget, the action will fail.

☼ -10 **Detection penalty**: Attack actions with this effect reduce defender's detection chance.

✳ **Discovery**: These attack actions have the useful ability to unveil hidden but exposed (reachable) assets. Assets need to be unveiled before they can be attacked.

♕ **Privilege escalation**: Actions with this icon grant administrative privileges on the asset, which may be required for some of the more effective attacks.

Permanent access: These actions create a direct attack path from the outside to the affected asset. This means that the attacker will retain access even if previously used jump host is healed. Permanent access is removed by healing the causing action.

🔥 **Persistence**: Attacks that grant persistence deal their damage every turn until the effect is removed or the damage is fully healed.

₵ +1 **Income**: Certain attacks may increase the budget of the attacker. Note that the defender's regular income or the selling of items is not reliant on individual actions but is awarded automatically or by using the "sell" icon in the inventory.

+2 **Detection boost**: Detection actions often grant a bonus to detection chance that lingers for a certain number of turns.

+1 **Reactive Insight gain**: Provides Insight if an attack is detected with the help of the respective action, modeling on-demand analysis actions in particular. The effect can only trigger once per asset.

+2 **Shield**: Prevention-type actions provide a shield that absorbs the stated amount of CIA damage dealt by any compatible attack. Shields are typically permanent and may shut down certain avenues of attack. Keep in mind that they often have a certain chance to trigger; few prevention actions are perfect.

Remove persistence: This effect cancels any recurring damage caused by persistent actions.

Remediate privilege escalation: This effect negates privilege escalation, removing the attacker's admin privileges from an asset.

Revoke credentials: Invalidates credentials for this asset gathered by the attacker up until this point. These credentials are not removed from the game, however. The attacker will only learn of their ineffectiveness when he/she tries to use them.

Remediate vulnerability: Makes vulnerabilities (exploit cards) previously found by the attacker for this asset ineffective. Again, the attacker will only learn of this when they try to employ them.

Insight prevention: Negates future Insight gain by the attacker. Can be untargeted (vs. e.g. OSINT) or specific to an asset.

Clone asset: Duplicates an asset on the game board. Since the asset is nearly distinguishable from the real deal, this may lure the attacker into attacking the honeypot instead of the actual system. Clones are uncovered once the attacker deals 3 C damage. Note that an asset can only be cloned once.

3.4 Using equipment

Equipment is used in two ways: **Permanent equipment** is applied automatically when playing an action, **one-time equipment** must be added manually in the attack or defense window (Figure 8). **Revocable equipment** can be invalidated by the opponent. Note that equipment may provide bonuses or have additional effects just as actions do. You can always check the icons or hover the mouse over the success and detection chance calculation to learn how certain equipment contributes to the total.

Attack tools & security systems

Attack tools (icon: ⌖) are **permanent equipment** that aid the defender in their task. They include various scanners, cracking tools, or exploit suites. **Security systems** (icon: 🔒) are the defender's equivalent (IDS, IPS, firewalls, etc.) and provide permanent bonuses when defending.

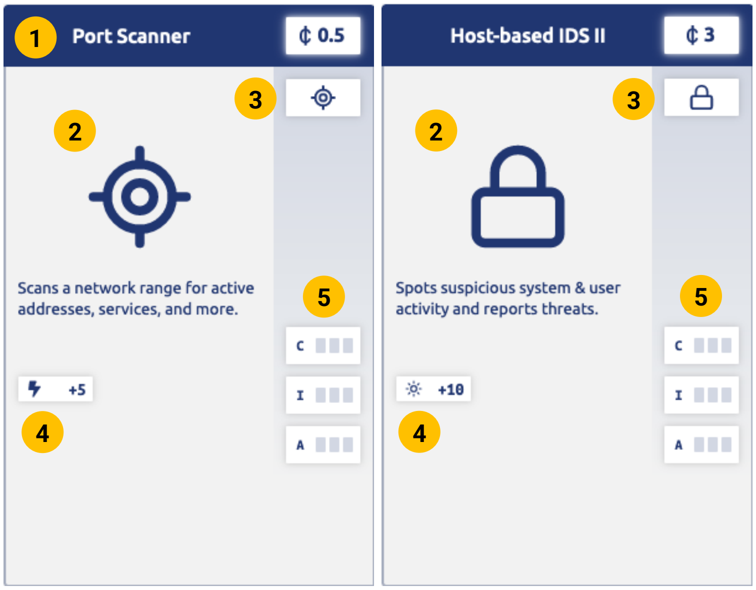

1
Port Scanner
₵ 0.5
2
3
Scans a network range for active addresses, services, and more.
5
C
I
A
+5
4
Host-based IDS II
₵ 3
2
3
Spots suspicious system & user activity and reports threats.
5
C
I
A
+10
4

Figure 13: Attack tools and security systems

Next to the title and cost (1), the card (Figure 13) shows an icon (2) and type (3) as well as effects (4) and damage (5), which is added to the corresponding main action just like support actions.

Policies

Organizational **policies** (icon: 🗎) are **permanent items** that provide significant bonuses and enable certain organization-wide defense actions. They are a significant investment but usually worth the cost.

Malware & analysis tools

Malware (icon: 🐞) is **one-time** equipment that can be appended to compatible attacks for various benefits: Ransomware may generate income, spyware will generate Insight, and so forth. **Analysis tools** (icon: 💡) represent one-shot efforts to better understand certain attacks; they usually make it easier to defend and generate Insight.

Credentials

Credentials (icon: 👤) are **revocable** equipment used by attackers to gain access to an asset by using a valid account. They can be purchased from the shop or generated through certain actions; gathering credentials is a key mechanism of the game and should always be part of a good strategy.

Exploits & fixes

Exploits (icon: 🔥) represent the attacker's knowledge about a vulnerability in an asset. The powerful "Exploit (…)" attack actions can only be used in concert with an exploit equipment card. Unlike malware, exploits provide lasting bonuses on an asset that remain in place until removed by a fix or invalidated by defense cards with the "Remediate vulnerability" effect.

Fixes (icon: 🔧) are required by the appropriate actions to remove exploits and provide lasting bonuses as well.

Both exploits and fixes can be purchased or generated for free by using actions with the "Item gathering" effect.

Selling & discarding equipment

Some equipment has a **resell value**, allowing the players to turn it into credits by clicking the 🛒 icon when hovering over the item in the inventory. This is particularly useful when the attacker wants to sell gathered credentials or exploits they don't need.

If an item has no value, it can still be discarded. In this case, the icon displayed is a bin 🗑.

3.5 Resuming or leaving a game

During your PenQuest session, you may encounter connectivity issues or want to **continue** a game at a later time. To do so, you can...

- simply **close the tab** or leave the PenQuest website, or
- use the "**Exit**" ⎘ button in the menu.

The game will offer you the option to **resume** or **leave** the existing game when you log in the next time. Only one game can be kept open at the same time.

If you use the "**Surrender**" ⚑ button, the game will end and show the game summary (see below).

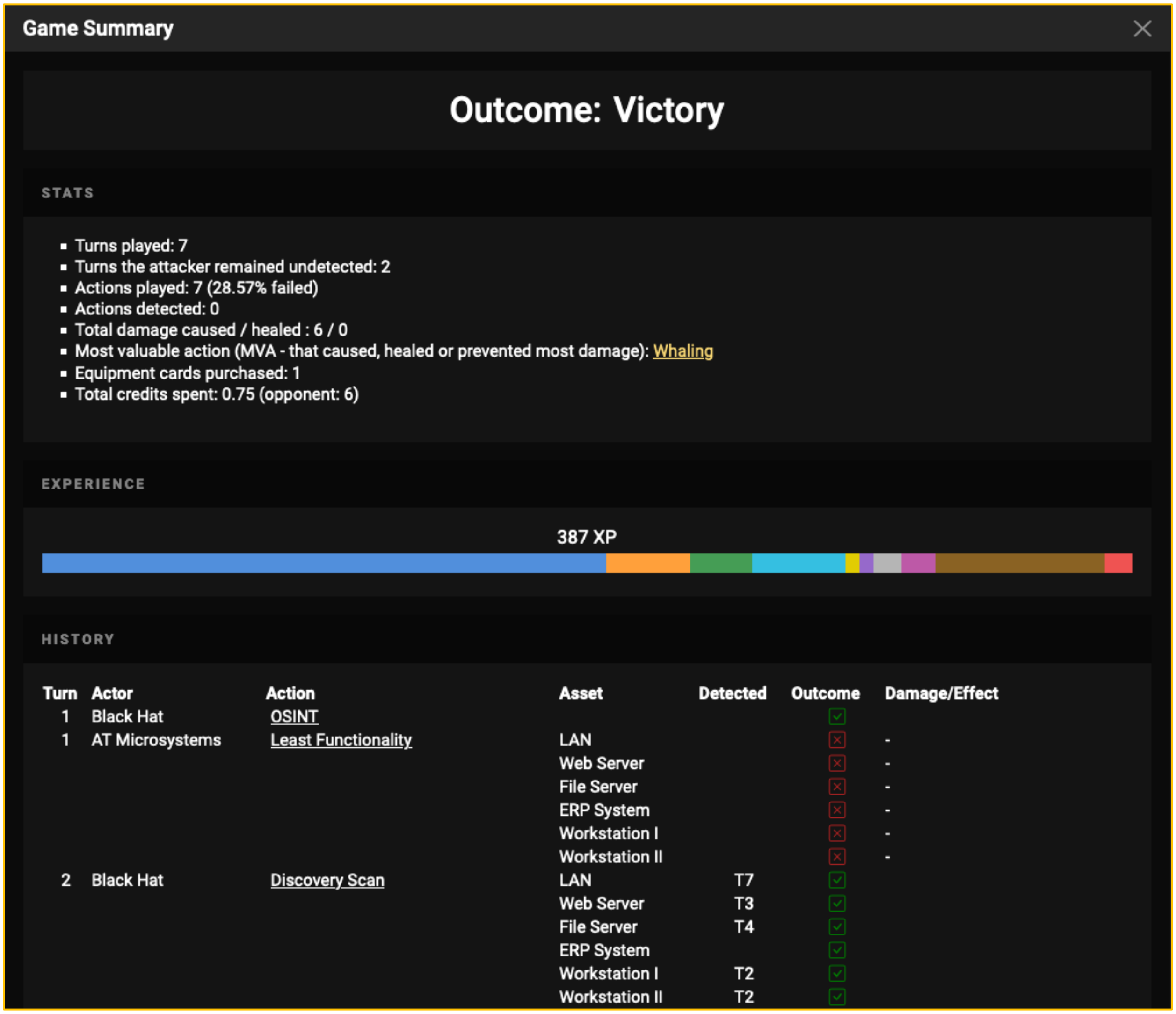
> Please keep in mind that the server will run regular cleanup tasks that might close your game after a while.
>
> If you run into problems such as server crashes, please wait for up to 30 seconds before refreshing the page and logging in again.

3.6 Winning the game

There are 4 possible **outcomes** to a game of PenQuest: If the attacker reaches their goal within the number of turns determined by Initiative, they win. If they do not meet their goal and time runs out, the defender is victorious. If either player surrenders the game before it reaches its conclusion, the outcome will be inconclusive. If the defender triggers an availability penalty by failing to restore a vital system that was taken offline, the game ends in a draw, since neither player achieved their goal.

No matter the outcome, both sides will be presented with a **game summary** (Figure 14) and the **unveiled game board** that shows the actual sequence of events. The summary lists all actions that were played and all damage caused or mitigated. Each action can be clicked for additional information. In a workshop format, it is recommended to use this summary as template for a "lessons learned" discussion.

Lastly, both players will be shown a number of **experience points** (XP) earned.



Game Summary

Outcome: Victory

STATS

- Turns played: 7
- Turns the attacker remained undetected: 2
- Actions played: 7 (28.57% failed)
- Actions detected: 0
- Total damage caused / healed : 6 / 0
- Most valuable action (MVA - that caused, healed or prevented most damage): Whaling
- Equipment cards purchased: 1
- Total credits spent: 0.75 (opponent: 6)

EXPERIENCE

387 XP

HISTORY

Turn	Actor	Action	Asset	Detected	Outcome	Damage/Effect
1	Black Hat	OSINT			☑	
1	AT Microsystems	Least Functionality	LAN		☒	-
			Web Server		☒	-
			File Server		☒	-
			ERP System		☒	-
			Workstation I		☒	-
			Workstation II		☒	-
2	Black Hat	Discovery Scan	LAN	T7	☑	
			Web Server	T3	☑	
			File Server	T4	☑	
			ERP System		☑	
			Workstation I	T2	☑	
			Workstation II	T2	☑	

Figure 14: Game summary

This wraps up our short manual. There are **many strategies** that can lead to victory – make sure to experiment! **Have fun playing PenQuest!**

Credits

Permanent team

Robert Luh (project lead)	Idea, security model, game rules, didactics, testing
Sebastian Eresheim	Backend development, bot, AI
Thomas Petelin	Frontend & backend development, database
Nico Gentilini	Additional coding (scenario generator)
Maximilian Rieger	Visual design, usability, UI (redesign, WIP)

Previous contributors

Thomas Bechtel	Backend development
Simon Gmeiner	Bot, AI
Stefanie Größbacher	Visual design, frontend development
Peter Judmaier	Didactics
Vanessa Kraut	Visual design
Manuel Leithner	Backend development, AI
Gehart Marc	Testing
Florian Mayr	Visual design, frontend development
Kathrin Neuherz	Logo, animations
Stefan Pfeiffer	Backend development
Pascal Pizzini	Security model
Gernot Rottermanner	Frontend development
Michael Sailer	Didactics
Kathrin Schneller	Security model
Michael Tuchny	Didactics
Miriam Widhalm	Visual design
Christoph Wiedner	Testing

Additional testing and feedback

Nicholas Lutz
Andy Papastefanou
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.