PeriHack (© Roberto Dillon 2022, v1.1) 

A cybersecurity game for 2 players/teams. This game simulates a specific environment made of different components (DB server, PCs, Firewall etc.).

One team (BLUE TEAM) is in charge of defending the perimeter. The other team (RED TEAM) is the attacker.

The game can be played in different modes:

- **Breach**
  - Red Team has a specific objective (unknown to the Blue Team). Blue team sets up defenses and Red Team can initiate differen attacks to breach the perimeter as requested. Attacks can be repeated (e.g. if a USB drop fails, Red Team can repeat it again with a new card in the following rounds)
- **Penetration Testing**
  - Like Breach, but any winning condition is valid. Here, though, the same type of card/attack cannot be repeated.

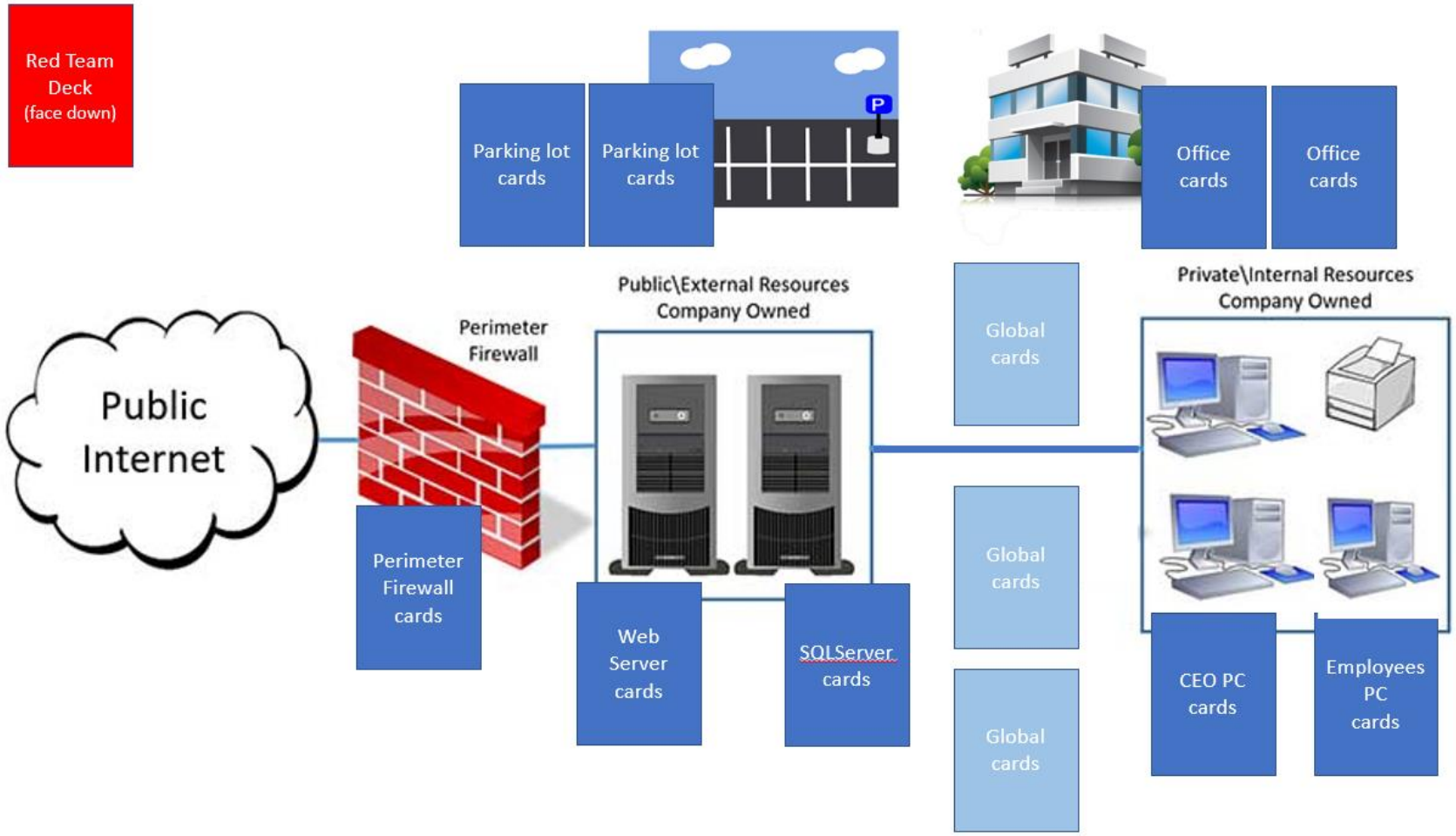
Time

A typical game can last between 5 to 10 minutes

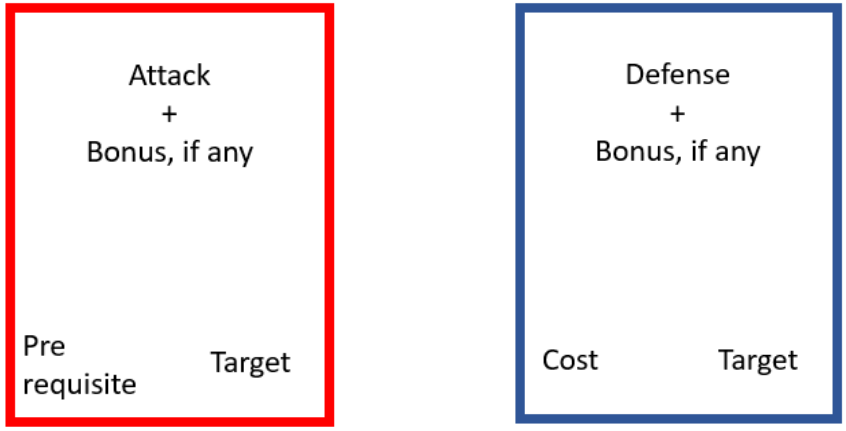
Materials

- One game board with specific layout for cards to be placed
- 18 different attack cards for a total of 54 cards (red team)
- 14 different defense cards: 10 hardening cards and 4 global cards (blue team)
- 7 Winning condition cards (red team)
- 20 coins
- 1D20

Game Board layout



Card Design/Structure



Possible Objectives/Winning conditions:

Winning conditions can be achieved in different ways. Some are straightforward while others require multiple phases.

1. DDOS. Can be achieved by the following means:
    a. Successful BOTNET or Ping Flood Attack
2. Database breach. Can be achieved by the following means:
    a. SQLi
    b. Zero Day on DB Server
3. Harvest website users' credentials. Can be achieved by the following means:
    a. Reflected XSS
    b. Stored XSS
4. Harvest employees' credentials. Can be achieved by the following means:
    a. Watering hole attacks
5. Shut down company operations. Can be achieved by the following means:
    a. Install ransomware on server or any PCs
    b. Zero Day on server
6. Spy. Can be achieved by the following means:

   a. Install backdoor on Server or CEO PC
   b. Zero Day on Server or CEO PC
7. Crypto Mining. Can be achieved by the following means:
   a. Gain control of PC (not CEO) to Install malicious SW

Red Team Cards

1.	Change an existing card for a new random one from the deck	X 5
2.	Zero Day Attack	X 1
3.	DOS attack via Botnet	X 3
4.	DOS attack via Ping Flood	X 3
5.	Tailgating	X 3
6.	USB Drop	X 3
7.	Man in the Middle	X 3
8.	SQLi Attack	X 3
9.	USB Rubber Ducky	X 3
10.	Watering Hole Attack	X 3
11.	Phishing Campaign	X 3
12.	Spear Phishing Campaign	X 3
13.	Stored XSS attack	X 3
14.	Reflected XSS attack	X 3
15.	Rogue AP Install	X 3
16.	Ransomware Install	X 3
17.	Backdoor install	X 3
18.	Install Crypto	X 3

Blu team cards

Best practices defenses for each item on the board, with a cost. Cards are to be placed face down and uncovered only if attacked by a red team card.

Global cards (GC) have a global effect and have to be placed face up on the board. There are 4 GC but only 3 slots on the board. Choose wisely! Once placed, they cannot be removed/exchanged later in the game.

1. Ask board for additional budget (roll die at beginning of round 3 and, if successful, buy and deploy additional resources before round 4 starts)
2. Renew all SW licenses and Patch all SW
3. Staff Awareness Training
4. Regular offsite backups

Blue cards (can be stacked on specific equipment):

1. No Additional Defenses Here
2. Firewall rules to limit ICMP traffic
3. Network Load Balancing
4. Refactor website to protect against XSS and SQLi
5. Add Firewall rules: all 3rd party traffic is untrusted until otherwise verified
6. Database Honeypot
7. Server Honeypot
8. Security on Lookout for USB drops
9. Security on lookout for Rogue AP
10. Security on lookout for Tailgating
11. Implement 2FA for logins on PCs

Breach Mode: Achieve a specific hack within 8 rounds max

The game (Breach Mode) is played in two phases.

First Phase:

All card decks are shuffled.

Red team starts with 5 coins and draws 5 cards. If any Swap card is drawn, it does not count and a new card can be drawn. Based on the 5 cards, Red Team can pick one suitable Winning Condition card that they believe they can achieve.

Blue team starts with a specific budget (10 cyber coins) and uses it to buy specific cards to harden the perimeter. All cards, except for global cards, are to be placed facing down and only revealed if the specific component is attacked. Placeholder cards are available for areas left unprotected due to budget constraints.

Second Phase: When the Blue team is ready, the Red team steps in. It has 8 rounds max to satisfy the winning condition.

- Executing one card counts as one round.
- If Blue Team played the “Additional Budget Request” global card, during round 3 they roll the D20 and, if successful, buy and deploy additional resources before round 4 starts.
- Unless otherwise specified, a failed attack can be tried again in the later rounds but the blue team will get an additional +1 defense bonus for that specific attack. The card will remain in place rotated 90 degrees.
- Red Team can have up to 8 attacking cards in hand plus any number of swapping cards.
    - When using a swapping card, the swapping card itself gets discarded, a new card from the deck is drawn and the card to be removed goes at the bottom of the deck.
- Each round, Red Team can use coins to buy up to 2 cards, as long as there is available budget and the number of cards in hand does not exceed the above mentioned card limit. If the limit is reached, a card has to be discarded first before buying a new one.

If, after 8 rounds, the winning condition is not achieved, the Blue Team is declared the winner.

Note:

For Red Team beginner-level players, it is recommended to ask them for an explanation of their actions at the end of the game to grant a successful victory, i.e. explain how the winning condition was ultimately achieved by their actions. For example, if a man-in-the-middle (MITM) attack to sniff network traffic and then hijack employees towards a malicious website (watering hole attack) was achieved by installing a USB rubber ducky (RD), they may articulate the process like this:

- RD script launches a browser and tries to access a local AP/router/etc
- If the browser has stored credentials for it, then there’s free access!
- Otherwise, RD can grab a hacked firmware for the device from some CnC server, then upload it
- Now you can MITM with a hacked AP

Penetration Testing Mode: Hack the perimeter within 5 rounds max

Same as Breach Mode but Red Team wins by achieving any winning condition. Red Team can only buy 1 new card per round.

If Blue Team plays the “additional budget” global card, the die is rolled in Round 2 and additional resources deployed in Round 3.

Simulating an Attack

- Red team attack cards can only be launched on their specific targets.

- Red Team cards may have an attacking bonus modifier score (e.g. AB = 1)
- Blue team defense has a defense bonus modifier score given by relevant perimeter cards plus any eventual bonus due to Global Cards (GB) (e.g. DB = 2 + GB)
- When an attack is being launched, the Red Team rolls 1D20, getting value R1.
    - Attacking card bonus (if any) is added to result, R2 = R1+AB
    - If R2 is greater than target T = 10 +DB, attack succeeds. If R2 is minor or equal than T, attack fails.
- A used attack card stays in place if successful or is rotated 90 degrees if the attack failed.
- If the place holder blue team card is present on a location that is attacked, the defense modifier is 0 and the target value for the attacker to beat is the default 10.

Special Thanks

Ms. Arushi, Dr. Steve Kerrison