**Cyber Attack Chain**

**The Game Rules**

*"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. "*

*Sun Tzu, The Art of War*

**Introduction**

This is a card game designed to simulate cyber-attacks against a business and how the business defends itself. The game is intended to be a teaching tool for information security awareness in the workplace.

The game is designed for two teams and an Umpire.

The Red Team are the attackers, and the Blue Team are the defenders. The rules for each team are slightly different as shown below and as provided in the separate team rule books.

The game is run as a series of turns. In each turn the two teams play cards from their respective decks and then the umpire adjudicates the turn as described below.

**Target Audience**

This game is aimed at anyone in a modern business that needs to gain a greater understanding of cyber security. It can form part of a wider security awareness program. It can also be played recreationally as a wargame.

**Learning Outcomes**

The aim of this game is to illustrate the ways in which an organization can be subject to cyber-attack and how it can defend itself against such attack.

Learning outcomes:

* Understand the different types of cyber-attack available to a "hacker". Know your enemy.
* Understand how a number of attacks can be blended together to form an Advanced Persistent Threat.
* Understand the various forms of defense and what attacks they each defend against.
* Be able to weigh the cost benefits of various defenses against the likelihood of specific attacks.
* Assess priorities

**Preparing to Play the Game**

The game is ideally played between two teams of players. One team takes the role of the attackers - the "Red Team" and the other are the defenders- the "Blue Team". The teams should be roughly equal in numbers. The maximum size of each team should not exceed about 8 players. The minimum size for a team is theoretically 1 but it is better if there are 2 or more. If the participants are a mixture of people with different levels of experience or expertise in information security then it is preferable for those with more experience to be assigned to the Red Team (at least for the first game). A typical game session will take approximately 90 minutes.

The game structure is what is known as asymmetric. That is, each team has a separate set of rules that are not the same. The rules for each team are given below.

The venue needs to be of sufficient size to allow each team to discuss and plan their actions without being easily overheard by the other team. It is possible to place each team in a separate room, but that means that the umpire will have to move between the rooms. A single larger room is usually preferred.

While it is not outside the bounds of possibility to run multiple games simultaneously, it is however recommended that there be an umpire for each game and a suitably large venue!

Before play, the umpire should set up the venue with a table for each team and provide materials so that the players can take notes.

At the beginning of the session the umpire should introduce the game and explain how it will operate. The umpire should have a means of indicating when the tum is finished, and adjudication takes place. This can be a bell, buzzer, timer or simply a loud voice!

The umpire controls the length of each turn, either by deciding when each team has made their action decisions or by setting a fixed time.

The game will typically run for about seven turns but there is no fixed turn limit. The umpire should keep records of attacks and defenses played in each turn.

At the end of the game, time should be set aside for all the players to come together to discuss the experience. In some contexts, it may be beneficial for the umpire to prepare and issue an After-Action Report describing what happened tum by turn.

The game is designed to be repeatable. The simplest thing to do is to play a second session with the team roles reversed i.e. the team that played Red will now play Blue and vice versa.

**Winning the Game**

The game ends after a specified number of turns of play or when an attack has resulted in a situation that the Blue Team can no longer counter, or when the Blue Team decide they can do no more. The Red Team's aim is to play one or more Black attack cards that are not countered by the Blue Team. The Blue Team's aim is to avoid the Red Team achieving their aim. Having said that, winning and losing are not that important since the learning outcomes can be achieved whatever the game result.

**Red Team Rules**

The aim of the Red Team is to attack the systems controlled by the Blue Team. Each possible attack is shown on a card, and the idea is to build attack chains leading to data exfiltration or other effects.

There are three types of cards:

* **Yellow cards** - these are attacks that can be used without any previous attacks in place, they are known as Initial Attacks.
* **Red cards** - these are "intermediate attacks" that must be preceded by either a yellow card or another red card. The Attack Chains table shows what cards can follow a particular yellow or red card. Note that there is more than one possible next card for some attacks.
* **Black cards** - these are cards that make the final attack in the chain and complete it. No more cards can be added to a complete chain.

**Optional Rule**

There is also a blank card. If a member of the Red Team wishes to add a new attack, then it should be written on a sticky note and affixed to the blank card. The Red Team must identify the new attack car das Yellow, Red or Black and except in the case of a Black attack, define the cards that can follow it in a chain. The umpire will determine if this new card is valid. If so, it can be played in the normal way. If not, it is removed from play.

**Red Sequence of Play**

The Red Team are not aware of any structure or activity of the business they are attacking. They will need to use attacks to find out.

In each tum the Red Team can play up to THREE cards. The Red Team can remove an attack card from the end of a chain and play an additional card.

Only one card can be added to an active chain in a turn.

The umpire will adjudicate the tum based on the cards played and the actions of the Blue Team. If the Blue Team have initiated an action that will block an attack, then that Attack card is turned over. No further attacks can be added to that chain.

The game ends after a specified number of turns of play or when an attack has resulted in a situation that the defenders can no longer counter.

**Attacks**

Note that there is more than one card for some attacks. The number of cards is shown below. If no number is given then there is a single card for that attack.

| **Attack** | **Type** | **Description** |
| --- | --- | --- |
| Brute Force Attack | Yellow | The attackers use a password cracker to find the login credentials of an account. |
| Business Email Compromise | Red | The attackers send a spoofed email purporting to be from the CEO, requesting an urgent payment be made to a supplier. |
| Compromised Account *(2 cards)* | Red | The attackers gain control of a user's account. |
| Compromised PC *(3 cards)* | Red | The attackers gain control of one or more PCs. |
| Compromised Server *(2 cards)* | Red | The attackers gain control of a server. |
| Credential Theft | Black | A recipient of a phishing email tries to download the file at the link in the email but in so doing gives away their credentials. |
| Database Vulnerability | Red | The attackers identify the production database and exploit a vulnerability to gain access to it. |
| Data Exfiltration (Database) | Black | The attackers exfiltrate sensitive data such as corporate or personal data from the database. |
| Data Exfiltration (PC) | Black | The attackers exfiltrate sensitive emails and technical data from the infected PC. |
| Data Exfiltration (Server) | Black | Sensitive data (email, HR records, client contracts, banking details, etc.) is exfiltrated from the server. |
| Defaced Web Site | Red | The attackers, having gained control of the web server, deface the web site. |
| DDOS Attack | Yellow | Floods the network with traffic generated by thousands of infected computers (bots). |
| Domain Dominance | Black | The attackers successfully compromise a highly privileged user (with domain admin rights). |
| Email Reconnaissance | Yellow | The attackers send emails to likely email addresses looking for a “null” response (indicating a valid email address). |
| Infected USB | Yellow | An infected USB drive is left in the company’s car park. An employee plugs it in and unknowingly installs malware. |
| Internal Phishing Attack | Red | Using a compromised account, the attacker sends phishing emails to all the victim's contacts. |
| Intruder (HQ) | Yellow | An intruder enters the HQ and hides a malicious device with remote access on the network. |
| Intruder (Production) | Yellow | An intruder enters production and installs malware on the IoT controller. |
| IoT Destruction | Black | The attackers send commands from the IoT Controller that completely destroy the IoT system. |
| IoT Disruption | Red | The attackers update the controller’s software with a malicious patch that disrupts production. |
| IoT Vulnerability | Red | The attackers exploit a vulnerability to gain control of the IoT controller. |
| Lateral Movement *(5 cards)* | Red | The attackers gain access to other machines on the network and identify sensitive data on them. |
| Lost or Stolen PC | Yellow | A user's laptop is lost or stolen. |
| Malware *(3 cards)* | Red | Emails with malicious links or infected attachments deliver malware to the recipient's machine. |
| Payment Diversion Fraud | Black | Using a compromised email account, attackers persuade recipients to transfer funds to a fraudulent account. |
| Phishing Attack | Yellow | Emails designed to persuade the recipient to divulge personal or sensitive information. |
| Port Scanning | Yellow | The attacker scans the Internet, looking for vulnerable systems. |
| Privilege Escalation | Red | The attacker gains privileged access to a PC and uses it to access sensitive data. |
| Remote Access Trojan | Red | A malicious attachment delivers a Remote Access Trojan to the recipient’s machine. |
| Reputational Damage | Black | A defaced web site embarrasses the company and results in reputational loss. |
| Simple Web Server Hack | Yellow | Exploits a well-known vulnerability in a web server to gain access. |
| Spamming Attack | Yellow | Floods the email system with spam, making it unusable. |
| Spear Phishing | Red | A targeted phishing email aimed at a specific individual or organization. |
| Targeted Scanning | Yellow | Attackers scan from the Internet and identify a vulnerable IoT controller. |
| Unsecured Wireless Network | Yellow | Attackers find an open Wi-Fi network and connect a device to launch further attacks. |
| Zero Day Attack *(2 cards)* | Red | The attacker uses a zero-day vulnerability to gain control of a machine (no patch exists). |

**Attack Chains**

Note that some attacks can be followed by more than one attack. For example, if a Compromised Account has been played then the next attack can be one of: Business Email Compromise, Internal Phishing Attack or Lateral Movement. There are some attacks that have no next attack.

| **Attack** | **Next Attack(s)** |
| --- | --- |
| Brute Force Attack | Compromised Account |
| Business Email Compromise | Payment Diversion Fraud |
| Compromised Account | Business Email Compromise  Internal Phishing Attack  Lateral Movement |
| Compromised PC | Lateral Movement  Data Exfiltration (PC) |
| Compromised Server | Lateral Movement  Data Exfiltration (Database)  Data Exfiltration (Server) |
| Database Vulnerability | Lateral Movement |
| DDOS Attack | *(end state — no follow-up)* |
| Defaced Web Site | Reputational Damage |
| Email Reconnaissance | Spear Phishing |
| Infected USB | Malware |
| Internal Phishing Attack | Credential Theft  Malware |
| Intruder (HQ) | Zero Day Attack |
| Intruder (Production) | Zero Day Attack  IoT Vulnerability |
| IoT Disruption | IoT Destruction |
| IoT Vulnerability | IoT Disruption |
| Lateral Movement | Privilege Escalation  Compromised PC  Compromised Server |
| Lost or Stolen PC | *(end state — no follow-up)* |
| Malware | Compromised PC  Remote Access Trojan |
| Phishing Attack | Malware |
| Port Scanning | Database Vulnerability |
| Privilege Escalation | Domain Dominance (Persistence) |
| Remote Access Trojan | Lateral Movement |
| Simple Web Server Hack | Defaced Web Site |
| Spamming Attack | *(end state — no follow-up)* |
| Spear Phishing | Compromised Account |
| Targeted Scanning | IoT Vulnerability |
| Unsecured Wireless Network | Compromised PC |
| Zero Day Attack | Lateral Movement |

**Blue Team Rules**

The Blue Team are charged with the information security of a business. The nature of the business is not defined except that its production facility uses a network of loT (Internet of Thmgs) devices. The HQ office of the business is located at some distance from the production facility and the two sites are linked by an Internet connection. There are computers and servers located across the two sites.

The aim of the Blue Team is to defend their systems against cyber-attack. Such attacks can take a variety of forms and exploit different vulnerabilities so it will be necessary for the Blue Team to decide what they defend and how.

The Blue Team has a set of cards, each representing a particular type of cyber defense. Each card has a point value that represents a measure of time and cost to implement the defense. Some cards are marked "SP". These can only be played on a subsequent tum after the "Security Platform" card has been played.

**Optional Rule**

There is also a blank card. If a member of the Blue Team wishes to add a new defense, then it should be written on a sticky note and affixed to the blank card. The umpire will assign a points value and thereafter it may be played in the same way as any other card.

**Blue Sequence of Play**

In each turn the Blue Team has a budget of 70 points available. With these funds they can play as many defense cards as they wish up to the limit of the available points. Any unused points may be carried over to the next tum.

The umpire will adjudicate the turn based on the cards played and the actions of the Red Team.

**Defenses**

| **Defense Name** | **Cost** | **SP** | **Description** |
| --- | --- | --- | --- |
| Advanced Security Training | 30 |  | More in-depth training to give staff better skills at spotting various attacks. |
| Anti-malware | 30 |  | Detects and removes malware; more sophisticated than anti-virus software. |
| Antivirus | 25 |  | Signature-based software to detect and remove viruses. |
| CCTV (HQ) | 40 |  | Security cameras and alarms at HQ; alert security to intruders. |
| CCTV (Production) | 40 |  | Security cameras and alarms at production site. |
| Complex Passwords | 10 |  | Requires strong passwords with defined complexity. |
| Data Loss Prevention | 20 | SP | Controls what information can leave the organization. |
| Database Software Patching | 50 |  | Implements a patching program for database software. |
| Firewall (HQ) | 25 |  | Filters unauthorized Internet traffic to HQ. |
| Firewall (Production) | 25 |  | Filters unauthorized Internet traffic to production network. |
| Hard Drive Encryption | 25 |  | Encrypts PC drives to protect client data and documentation. |
| Identity Protection | 30 | SP | Detects leaked credentials, anomalous logins, sign-ins from infected devices. |
| IoT Controller Upgrade | 25 |  | Upgrades IoT controller to latest firmware. |
| Multi-factor Authentication | 20 | SP | Adds a second authentication factor (SMS, token, app). |
| Network Monitoring | 40 |  | Records and monitors all network activity. |
| PC Operating System Patching | 25 |  | Implements patching program for PC operating systems. |
| Penetration Test | 30 |  | Simulated attacks to assess infrastructure and find vulnerabilities. |
| Phishing Simulation | 30 |  | Sends fake phishing emails to train employees. |
| Role-Based Access Control | 20 | SP | Access limited to what users need based on job roles. |
| Security Awareness Training | 25 |  | Basic cybersecurity awareness course for all staff. |
| Security Platform | 50 |  | Required before playing any card marked "SP". |
| Server Operating System Patching | 25 |  | Patching for server operating systems. |
| Spam Filters | 10 |  | Blocks known spam domains/senders. |
| Threat Analytics | 50 | SP | Analyzes user behavior and flags unusual activity. |

**Umpire Eyes Only**

**Umpire Adjudication**

The umpire will adjudicate the turn based on the cards played by the Teams. See the Cyber Attack Countermeasures table.

For each active attack (each face up attack card):

* If the attack is countered by an active Blue Team defense, then the attack card is turned over. The attack chain is no longer active.
* If the attack is not countered, but is detected by an active Blue Team defense, then the Blue Team is informed. The attack is still active, and the Blue Team knows about it (so can possibly make suitable countermeasures in a later turn).
* If the attack is neither countered nor detected, then any potential symptoms are reported to the Blue Team. The umpire has the latitude to tell a story applicable to the situation.

It should be noted that the Countermeasures table should only be available to the Umpire and not seen by the teams.

**Cyber Attack Countermeasures**

If an attack is countered by an active defense, then the attack is rendered ineffective and that attack card is turned over.

If an attack is detected by an active defense or generates observable symptoms, then the umpire informs the Blue Team. Note that not all attacks are detectable.

| **Attack** | **Countered By** | **Detected By** | **Symptoms** |
| --- | --- | --- | --- |
| Brute Force Attack | Complex Passwords  Multi-Factor Authentication | Threat Analytics | — |
| Business Email Compromise | Advanced Security Training | — | — |
| Compromised Account | Identity Protection | Threat Analytics | — |
| Compromised PC | Data Loss Prevention | Threat Analytics | — |
| Compromised Server | — | Threat Analytics | — |
| Database Vulnerability | Database Software Patching | Penetration Test (if in scope) | — |
| DDOS Attack | Firewall (HQ & Production) | — | Services run slowly; users can't access web site |
| Defaced Web Site | — | — | Adverse publicity due to defamatory content |
| Email Reconnaissance | — | Advanced Security Training | — |
| Infected USB | Security Awareness Training | — | — |
| Internal Phishing Attack | Advanced Security Training | Security Awareness Training | Users may report (not 100%) |
| Intruder (HQ) | — | CCTV (HQ) | — |
| Intruder (Production) | — | CCTV (Production) | — |
| IoT Disruption | IoT Controller Upgrade | — | Performance downgrade |
| IoT Vulnerability | — | Penetration Test (if in scope) | — |
| Lateral Movement | — | Threat Analytics | — |
| Lost or Stolen PC | Hard Drive Encryption | — | User reports |
| Malware | Anti-virus | Threat Analytics | — |
| Phishing Attack | Security Awareness Training | — | — |
| Port Scanning | Firewall (HQ) | — | — |
| Privilege Escalation | Role-Based Access Control | Threat Analytics | — |
| Remote Access Trojan | Anti-malware | Threat Analytics | — |
| Simple Web Server Hack | Server OS Patching | Threat Analytics | — |
| Spamming Attack | Spam Filters | — | Inboxes full of spam |
| Spear Phishing | Phishing Simulation | — | — |
| Targeted Scanning | Firewall (Production) | — | Firewall logs show scanning activity |
| Unsecured Wireless Network | Penetration Test | Penetration Test | — |
| Zero Day Attack | — | Threat Analytics | — |
| Credential Theft | Multi-Factor Authentication | Threat Analytics | — |
| Data Exfiltration (Database) | Database Patching | Network Monitoring | — |
| Data Exfiltration (PC) | PC OS Patching | Network Monitoring | — |
| Data Exfiltration (Server) | Server OS Patching | Network Monitoring | — |
| Domain Dominance | — | Threat Analytics | — |
| IoT Destruction | — | — | IoT network destroyed |
| Payment Diversion Fraud | Advanced Security Training | — | Monthly cash reconciliation detects a loss |
| Reputational Damage | — | — | Drop in sales, falling share prices |

**Running the Game**

After breaking up the group into two teams (attackers and defenders), the umpires should distribute each team's cards. Letting the players sort and discuss them is part of the learning process. The defenders will start to prioritize, and the hackers will start to construct possible attack chains. After both sides have chosen and played their initial cards, the umpire can raise the tension by telling the defenders that 'it is just another week at work, nothing happens of note, except for the office party". As each turn happens, the umpire should aim to impose a narrative on the cards as this helps the players relate and engage in the game. For example, when the Blue plays Advanced Security Training, they can add that "some staff say they are busy and do not want to do the training" or if reputational damage occurs they can say "The chief executive is very angry and demanding what are the IT staff going to do about falling sales". These informal comments can add greatly to the atmosphere.