

PeriHack

The Penetration Testing Board Game

v.0.1

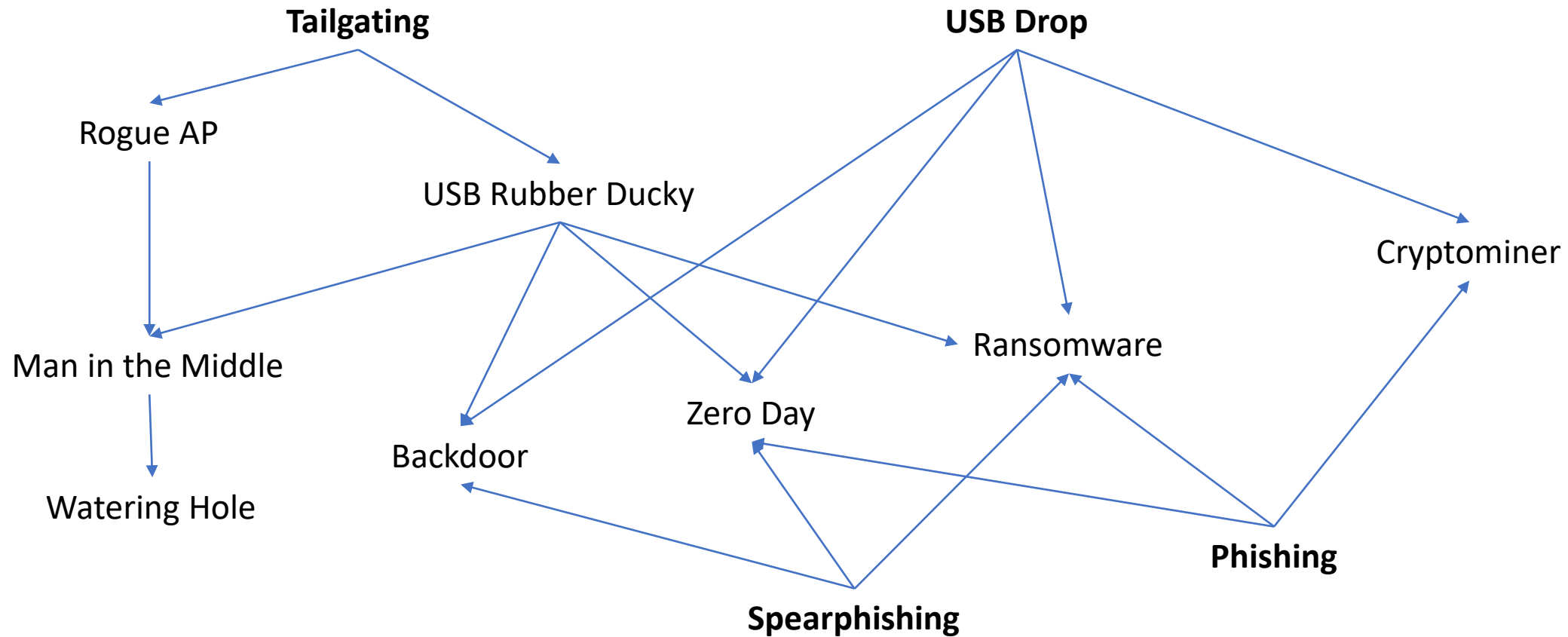
by Roberto Dillon (© 2022)



AGE framework analysis

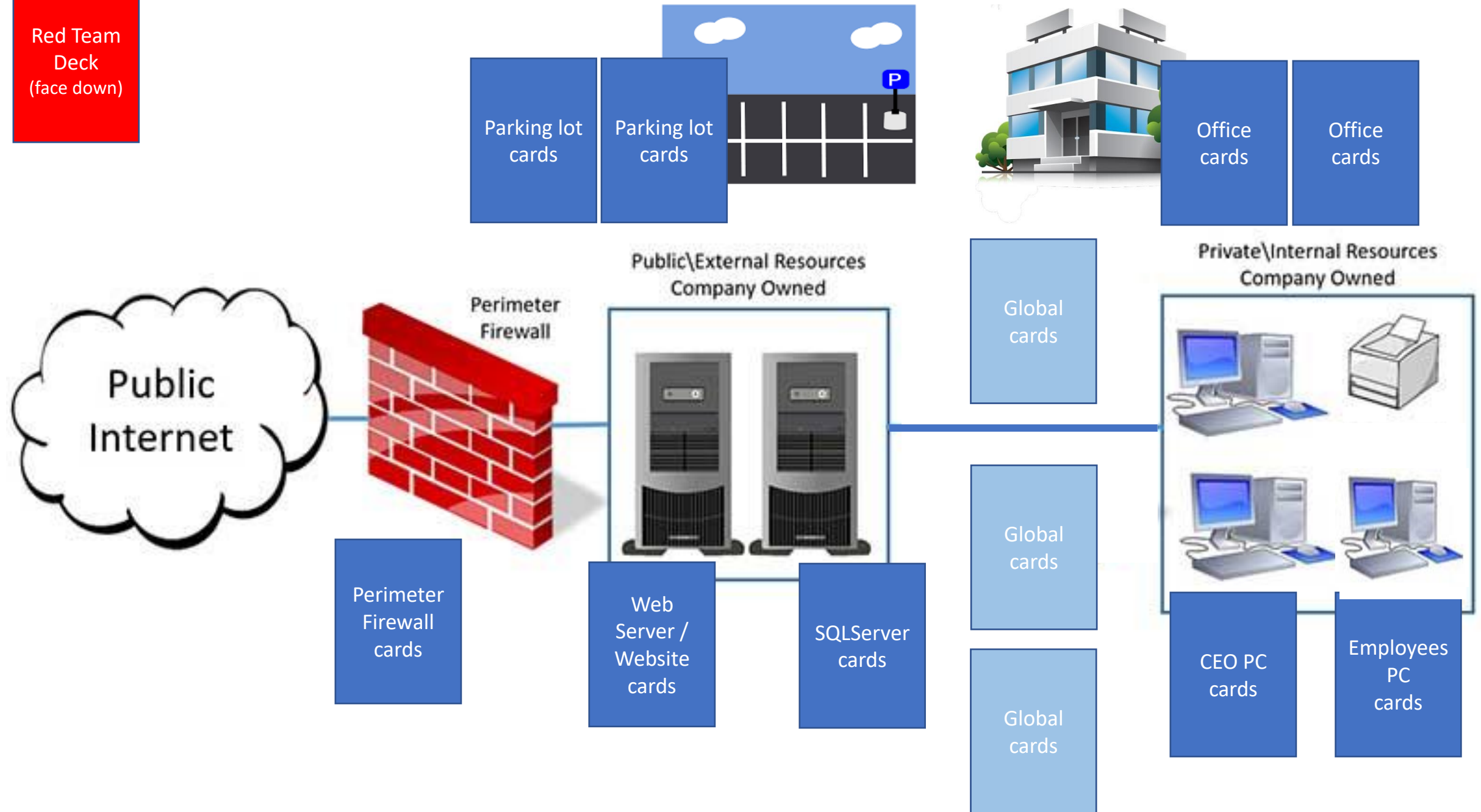


Card Relationships (Red Team)



Stand Alone Attacks: DDOS Botnet/Ping flood, SQLi, Stored/Reflected XSS

Red Team
Deck
(face down)



Attack
+
Bonus

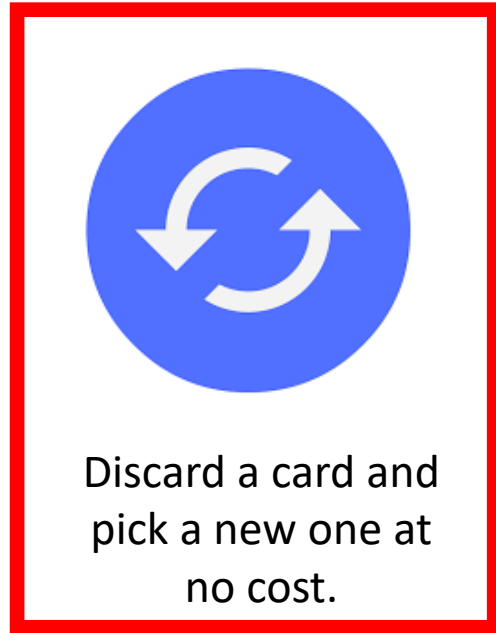
Pre
Requisite Target
(if any. Only one pre-req is needed)

Defense
+
Bonus

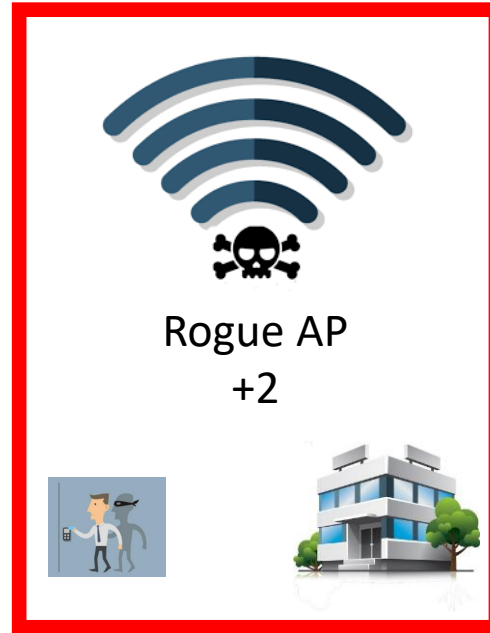
Cost Target



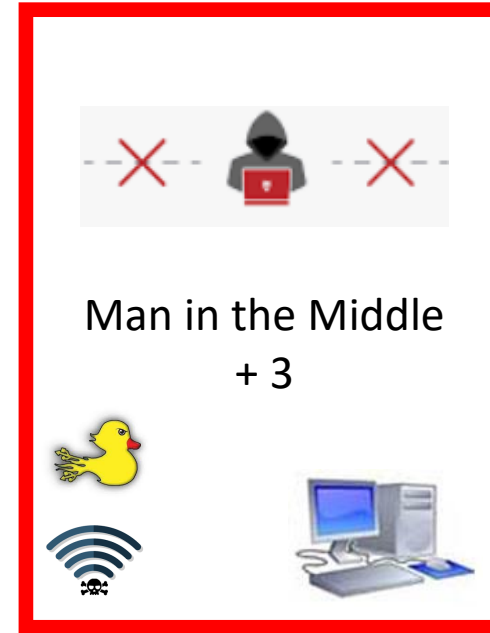
Red Team Cards



X 5



X 3



X 3



X 3

Red team starts with 5 random cards + 5 coins. Each coin can be used to buy a new card but only up to 5 cards can be held at a time (discard cards do not count). Discarded cards are put back at the bottom of the deck.

Red Team Cards



Ransomware
+ 3



X 3



Spear Phishing
+ 1



X 3



Phishing
+ 1



X 3

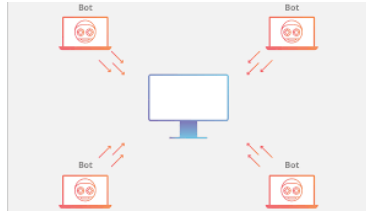


Tailgating
+ 1



X 3

Red Team Cards



DDOS: Botnet
+ 2



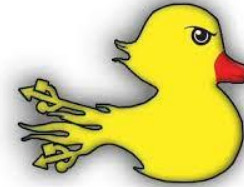
X 3



DDOS: Ping Flood
+ 2



X 3



USB Rubber Ducky
+ 3



X 3



Zero Day Exploit
+ 5



X 1

Red Team Cards



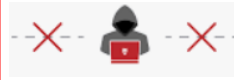
SQLi Attack
+ 1



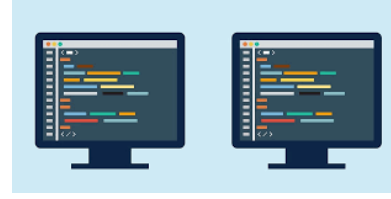
X 3



Watering Hole
+ 4



X 3



Stored XSS
+ 1



X 3



Reflected XSS
+ 1



X 3

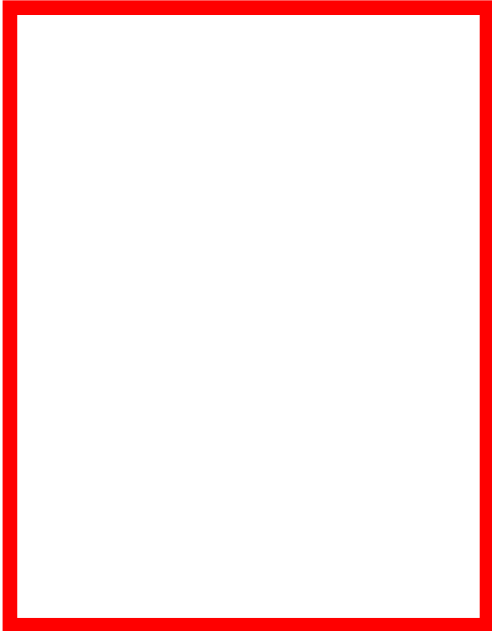
Red Team Cards



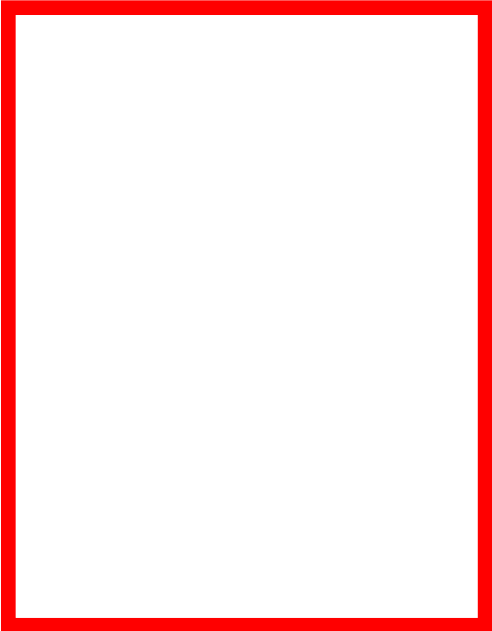
X 3



X 3



X 3



X 3

Blue Team Cards: Global Cards

Ask Board for additional budget

1D20 > 12: + 5 



X 1

Renew all SW licenses and patch all SW



+ 2 

 3 

X 1

Staff Awareness Training





+ 1 



 2 

X 1

Offsite Backups



+ 3 

 2 

X 1

Blue Team has a starting budget of 10 coins

Blue Team Cards

No additional
defenses here



X 5



Server Honeypot



+ 2



1



X 1



Database Honeypot



+ 2



1



X 1



Refactor Website



+ 2

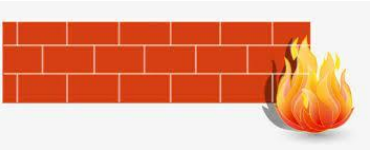


1





X 1

Blue Team Cards




All 3rd Party traffic
is untrusted until
otherwise verified


+2 



 1 

X 1




Security on lookout
for **Intruders**


+1 



 1 

X 1




Security on lookout
for **Rogue AP**


+ 1 



 1 

X 1



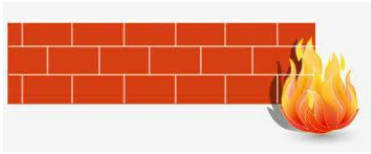
Security on lookout
for **USB Drops**

+ 1 

 1 

X 1

Blue Team Cards



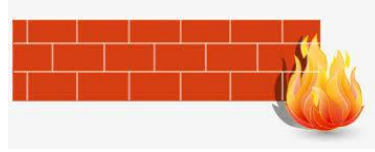
Limit ICMP Traffic



1



X 1



Network Load Balancing



1



X 1



Two Factor Authentication

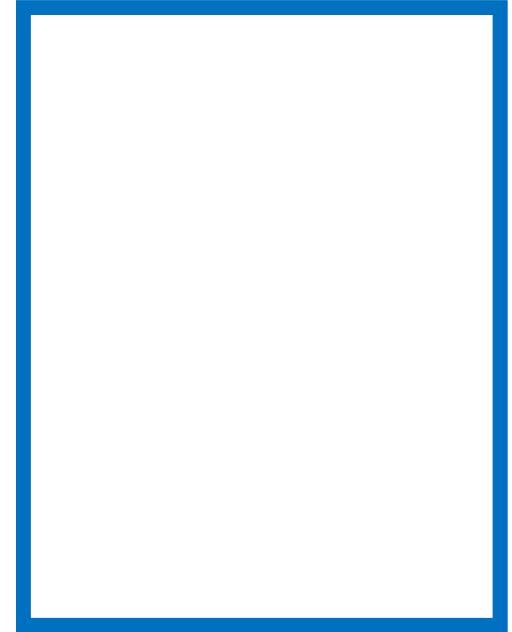
+ 2



1



X 1



X 1

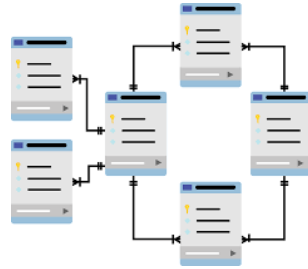
Winning Condition Cards



DDOS

Bring down the Network
via successful BOTNET or
Ping Flood Attack

X 1



Breach the DataBase

Gain access via SQLi attack
or a Zero Day on the DB
Server

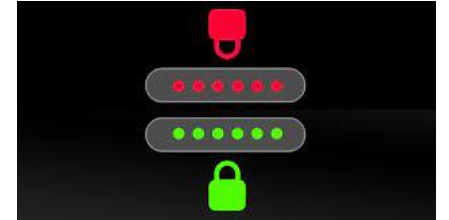
X 1



Harvest Users' Credentials

Break the Website via XSS

X 1



Harvest Employees' Credentials

Deliver a successful
Watering Hole Attack

X 1

Winning Condition Cards



Shut Down Company Operations

Install Ransomware on the
Server or any PCs
Or
Deploy a Zero Day on the Server

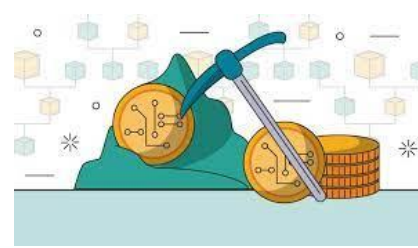
X 1



Spy

Install Backdoor on Server or
CEO PC
Or
Deploy Zero Day on Server or
CEO PC

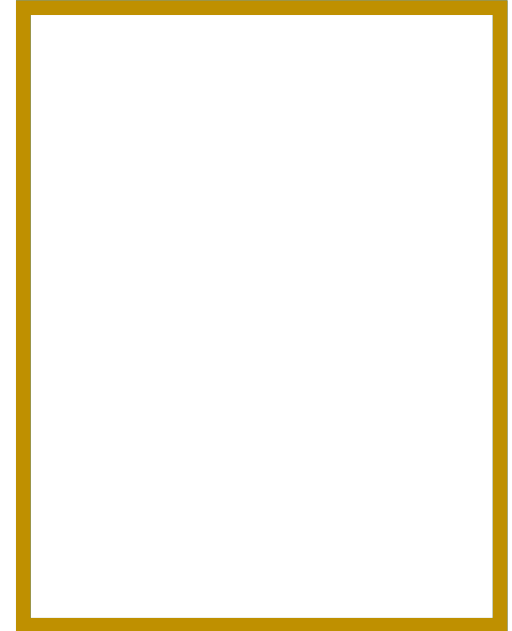
X 1



Crypto Mining

Gain control of employee's
PC to install relevant
malware

X 1



X 1