#exploits

a hackers card game by scott wambold
one bold plant games

****

#load config

2 - 4 players
60 minutes
12 and up

#ls /etc/exploits/*contents*

rules
34 vulnerability (firewall) cards
3 award cards
24 target cards
59 attack cards

A video version of these rules is available on Youtube, look up “One Bold Plant Games Exploits Rules” or visit www.oneboldplantgames.com

****

#say *objective*

In exploits, players will take on the dual role of hacker and admin, and attempt to hack each other by scanning their opponents' firewalls for vulnerabilities, then using exploits to deliver point earning payloads through the vulnerabilities to the target servers. All while trying to defend their own servers. The player with the most point (not hacks) wins the game. Players simulate scanning their opponents by searching their firewall, and attacking by using an exploit to deliver a payload through the opponents firewall to their server

****

#make /bin/*setup*

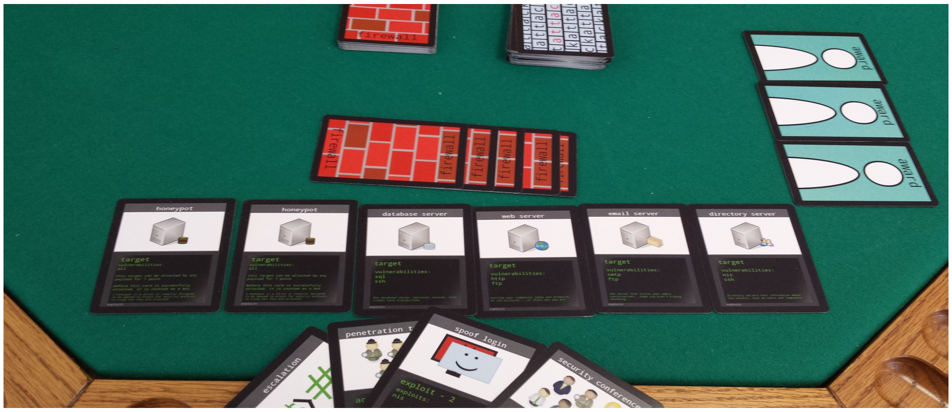
Each player places their 6 target cards (directory, database, web, email and 2 honeypot servers) in front of themselves face up. Deal each player 5 vulnerability cards, these cards are placed in a pile in front of their servers. **You may not look at these vulnerability cards.** Place the three award cards aside for the end of the game.

Each player then draws 5 cards from the attack deck. Play begins with the player with the most unread emails at home (or at random).

****

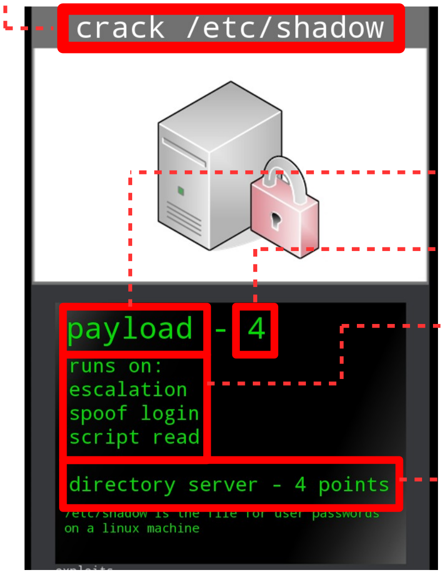
#which *attack_cards*

The majority of the game focuses on the attack cards in your hand. There are 4 types of attack cards. Exploit, Payload, Action, and 0-Day. Action and 0-Day provide unique actions described later in these rules.



a player's setup, the decks go in the center for all players to reach

Title-Name of the card


crack /etc/shadow
payload - 4
runs on:
escalation
spoof login
script read
directory server - 4 points
/etc/shadow is the file for user passwords on a linux machine
exploits

Card Type - A payload, exploit, action, or 0-Day

Card Power - Used to determine number of cards seen in a *scan* action or removed in an *audit* action

Runs on/ exploits - On a payload card, this shows the exploits this card links to in an attack, on an exploit, it shows the vulnerabilities in a firewall the exploit links to. On an action or 0-day card, this is used to explain that cards ability in detail

points - On a payload card, this is the points scored when attacking this particular server, you can attack other servers, but you will not earn any points from doing so

#bash /bin/*gameplay*

On their turn, a player draws 1 card from the attack deck and performs one of the 5 actions on the next page. *After the action, take the listed amount of vulnerability cards and add them to the top of your firewall* as the cost of the action. Play then continues clockwise until the end condition is met.

scan-*take 1 vulnerability card -* You may discard an attack card from your hand in order to look at a number of cards in an opponents firewall equal to the attack cards power. After you look, your opponents shuffles their firewall, taking care not to look at any cards. You cannot scan yourself.

card action-*2 vulnerability cards*- A player can use an action printed on an action card from the attack deck. After the card is used, the card is discarded. *Note that some actions are powered by bots you have scored and your honeypots.*

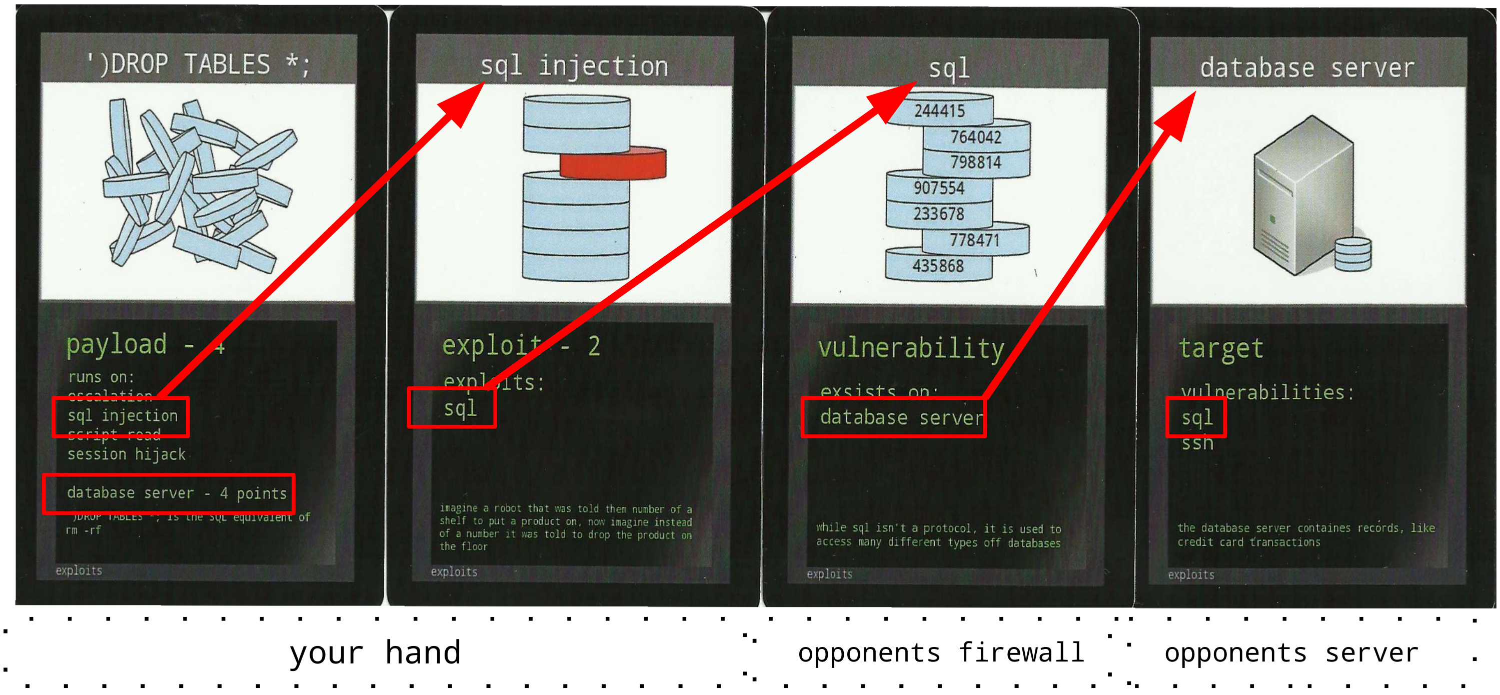
audit-*take 0 vulnerability cards* - Play an attack card and remove a number of your choice from your firewall (yes, you can look at your firewall when you perform this action) equal to that cards power. *Note that you must always have 5 cards in your firewall*

research-*take 1 vulnerability card* - Discard your entire hand and draw 5 new attack cards.

Attack - take 4 vulnerability cards are the method of removing opponents servers from the game and scoring points. An attack consists of 2 cards from your hand (a payload that runs on an exploit in your hand), a vulnerability from your opponents firewall, and a target owned by your opponent. A payload runs on a exploit from your hand, the exploit exploits a vulnerability card in your opponents firewall, which is connected to the target server. Declare the opponent *and the server* you wish to attack. search their firewall for an appropriate vulnerability. If you can complete the chain from a payload to the target, the attack is successful and you score the number of points listed on the bottom of the payload card

If the attack is successful, the attacker sets the payload and server next to themselves for scoring at the end of the game. The opponent then shuffles their firewall in with the vulnerability deck and draws 5 new vulnerability cards, you take 4 vulnerabilities into your own firewall. discard the exploit card you used.

If the attack is not successful, the payload and exploit are discard. your opponent still shuffles their firewall in with the vulnerability deck and draws 5 new vulnerability cards, you still take 4 vulnerabilities into your own firewall.


')DROP TABLES *;
payload - 4
runs on:
escalation
sql injection
script read
session hijack
database server - 4 points
')DROP TABLES *; is the SQL equivalent of rm -rf
exploits
sql injection
exploit - 2
exploits:
sql
imagine a robot that was told them number of a shelf to put a product on, now imagine instead of a number it was told to drop the product on the floor
exploits
sql
244415
764042
798814
907554
233678
778471
435868
vulnerability
exsists on:
database server
while sql isn't a protocol, it is used to access many different types off databases
exploits
database server
target
vulnerabilities:
sql
ssh
the database server containes records, like credit card transactions
exploits
your hand
opponents firewall
opponents server

example: alice is holding drop tables and sql injection and saw a sql vulnerability in bob's firewall and knows bob still has his database server. she declares an attack on bob's database server and finds the sql vulnerability. alice scores 4 points (listed on the bottom of the payload) and sets aside the drop tables payload and database server to the end of the game. bob shuffles his remaining firewall with the vulnerability deck and draws 5 new cards. alice takes 4 vulnerability cards into her own firewall and ends her turn.

****

#cat *0-day cards*

In the attack deck are 3 cards called 0-day cards. These cards provide unique bonuses and can be played any time the condition on the card is met, regardless of who initiated the action. 0-day cards do not add vulnerabilities to your firewall

****

#sudo apt-get install *botnet_cards*

Bots are any opponent servers you have successfuly attacked with the 'add to botnet' payload. Bots help power certain action cards, such as ddos and spam. Honeypot cards start out as bots to help power these cards early on, but are not longer considered bots after they have been attacked.

example: Bob plays the spam action cards, he points out he still has one of his honey pots remaining and took alice's email server and database server with 'add to botnet' payloads, alice takes 3 vulnerability cards from the card. Bob then takes 2 vulnerability cards because he played an action card

****

#tail -f /var/*ending_the_game*

The game immediately ends when either any player loses all of their servers or when a player reaches 11 points. At this point, distribute the 3 award cards to the players for having the most hacks, bots, and servers remaining. If 2 or more players tie for an award, both players receive the award.

Players then count their points and the player with the most points wins. In the case of a tie, the first tiebreaker is who has the most servers remaining, the second tiebreaker is the player with fewest payloads scored (more elegant hacks), and the third tie breaker is the player with the least amount of cards in their firewall.

****

#ls -al /mnt/faq/*special_cases*

*you can never go below 5 cards in your firewall, even with the *penetration testers* action

*when you run out of firewall or attack cards, no cards are drawn until cards are discarded and shuffled to make a new deck

*you cannot split a scan between 2 players

*honeypot targets only offer their action bonus to the player who owns them

*on *rm -rf / ** and *cp -rf hda*, round up the 1/4th cards

*yes, *less* hacks is a tiebreaker, the reason being you performed more specific hacks

*if there are not enough cards when resolving the spam action, the player to the left and continuing clockwise draw 1 card at a time until cards run out

*the most up to date version of this ruleset as well as the video rules are available on: www.oneboldplantgames.com

****

#ls -al ~/*credits*/*

*all artwork done using the GIMP image editor and LibreOffice

*network images provided by *VRT Systems* LibreOffice gallery

*Game and components printed by *The Game Crafter*, in sunny Madison, WI

*thank you to my family, friends, and kickstarter backers

*special thanks to Guy Hembroff, Todd Arney, Danny Miller, and the rest of the CNSA staff at *Michigan Technological University*

*for more games, visit www.oneboldplantgames.com or like One Bold Plant Games on Facebook

*the default password for this service is 'toor'