intrusion detection system

customer database

web server

[patch!]

[patch!]

[patch!]

client

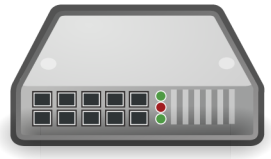
single sign-on service

IMAP server

backup
file server

wireless
router

VLAN
switch



[patch!]

[patch!]

[patch!]

VPN gateway

SMTP server

chat server

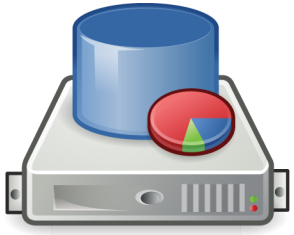
NAT device

network
file server

certificate
services

primary
DNS server

sales
database



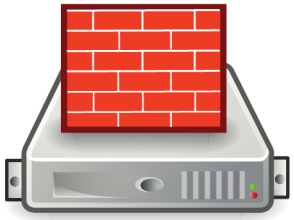
secondary
DNS server

VoIP server

client

client

firewall



client

internet gateway

[patch!]

[patch!]

[patch!]

Special Ability:

As one action, [give] or [exchange] a card to a player **anywhere** on the network.

[war driver]

Special Ability:

As one action, [move] across **two** compromised tiles.

[malware writer]

Special Ability:

As one action, [compromise] **two** adjacent tiles.

[the insider]

[d0x3d!]

[d0x3d!]

[d0x3d!]

Special Ability:

As one action, [move] or [compromise] diagonally.

[cryptanalyst]

Special Ability:

As one action, [move] to any compromised tile.

[social engineer]

Special Ability:

As one action, [give] or [exchange] two cards.

[botmaster]

[d0x3d!]

[d0x3d!]

[d0x3d!]

[loot]

[loot]

[loot]

[loot]

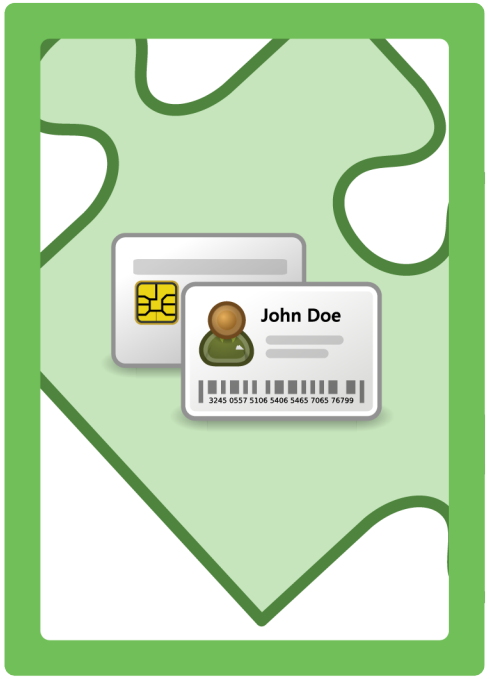
[loot]

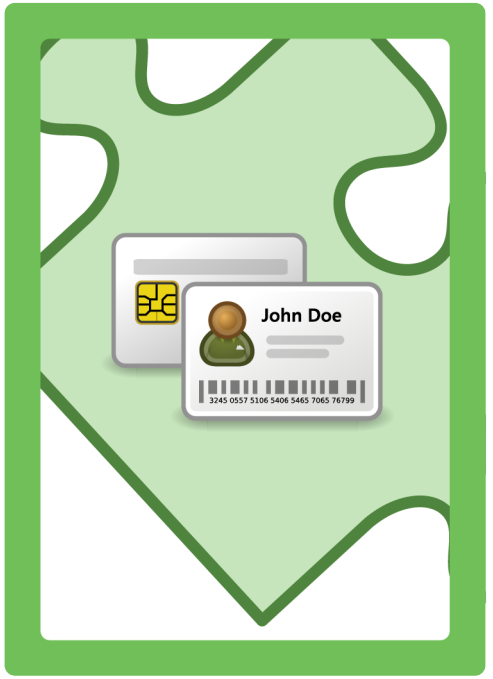
[loot]

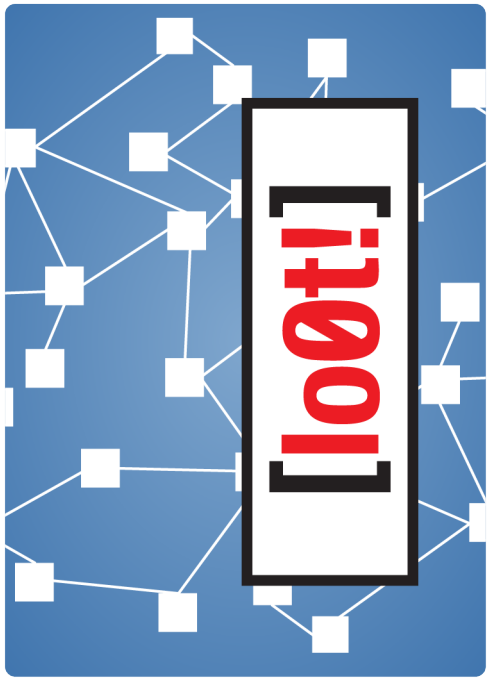
[lo0t!]

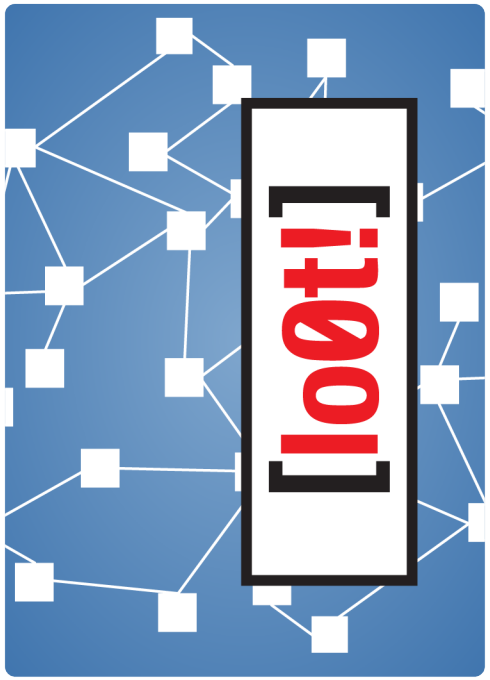
[lo0t!]

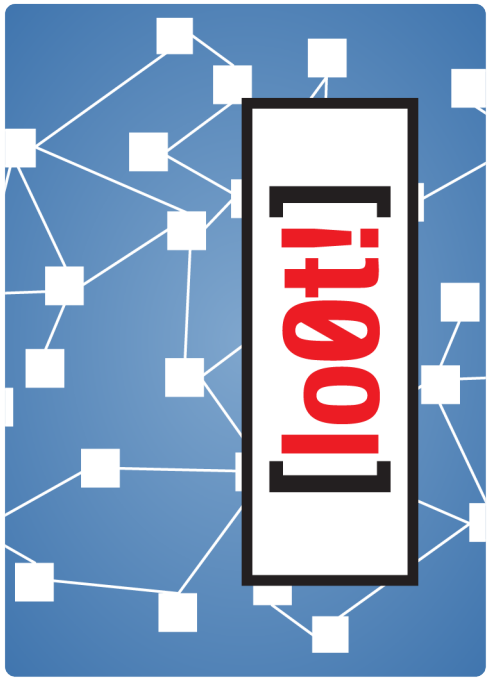
[lo0t!]

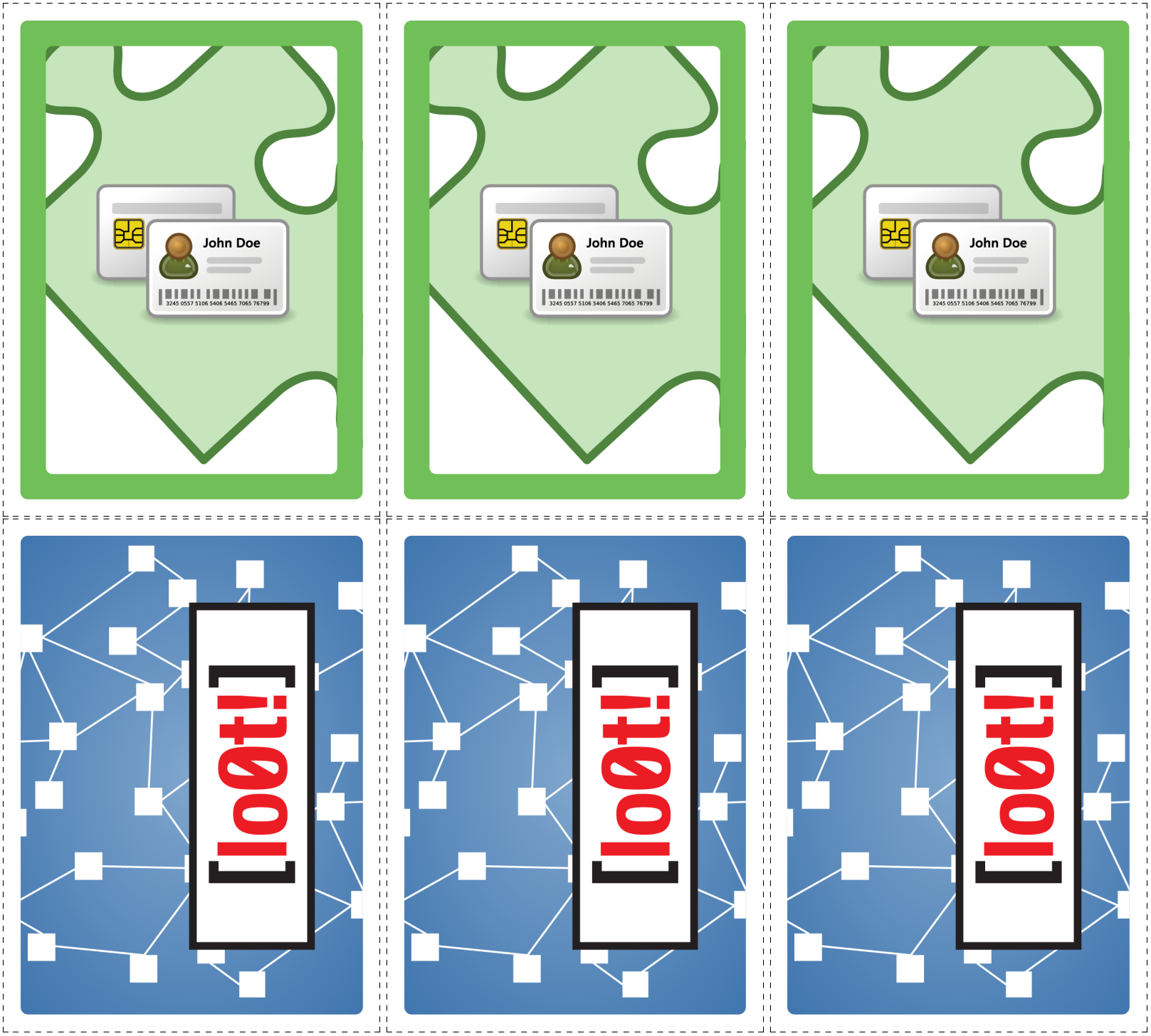

John Doe
3245 0557 5106 5406 5465 7065 76799


John Doe
3245 0557 5106 5406 5465 7065 76799


[loot]


[loot]

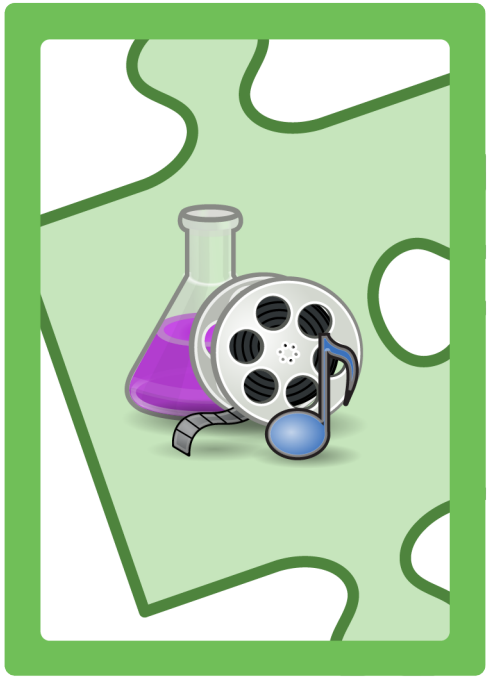

[loot]

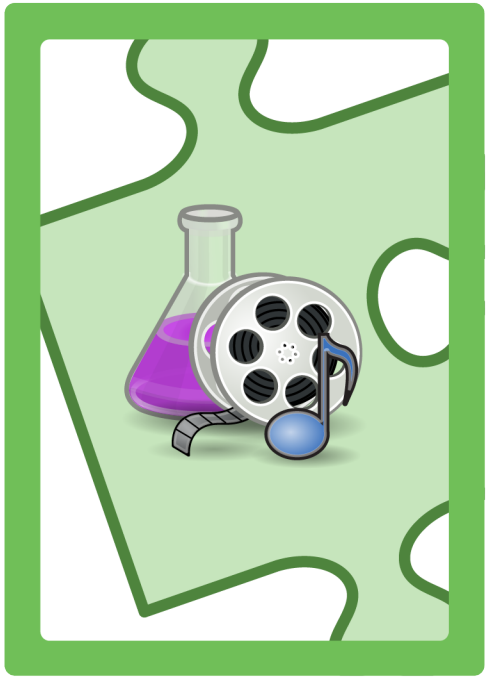

John Doe
3245 0557 5106 5406 5465 7065 76799
John Doe
3245 0557 5106 5406 5465 7065 76799
John Doe
3245 0557 5106 5406 5465 7065 76799
[l0t!]
[l0t!]
[l0t!]

[lo0t]

[lo0t]

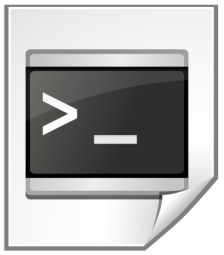
[lo0t]



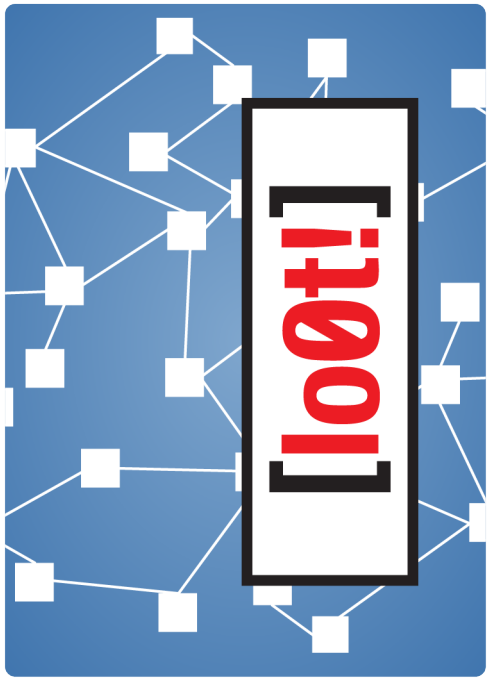


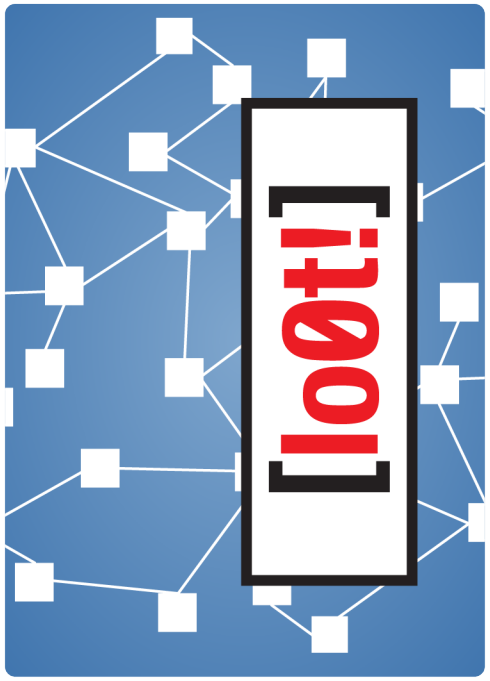
[zero-day exploit]

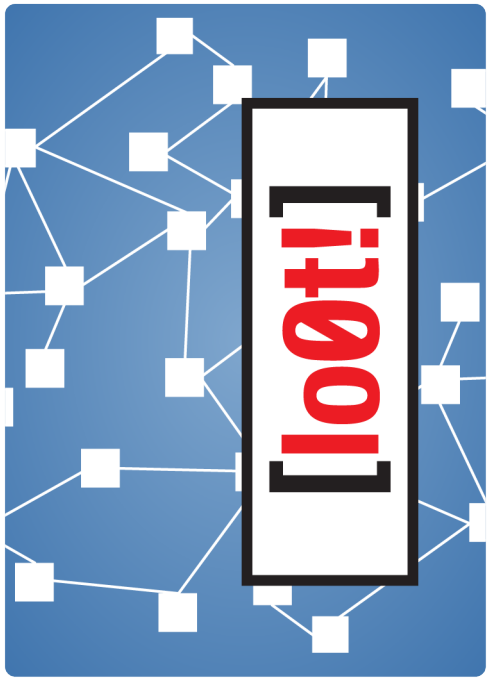
logic bomb



compromise
any node







[intrusion detected]
virus
signature
matched

[zero-day exploit]
integer
overflow

compromise
any node

[zero-day exploit]
buffer overflow

compromise any node
and move any hacker
to that node

[zero-day exploit]

trojan horse

EB F6
52 00
90 80
4E FF

compromise any node and move any hacker to that node

[root]

[root]

honeypot audit

[root]

[intrusion detected]

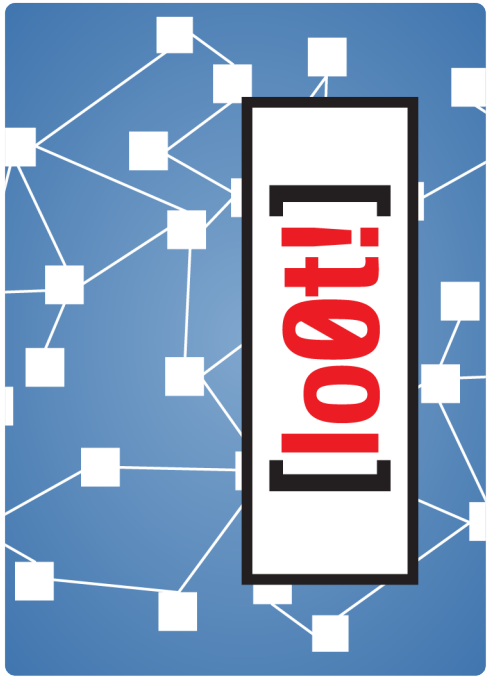
network anomaly observed

[root]

[zero-day exploit]

format string vulnerability

compromise any node



order of play

1. [action]
   Take up to 3 actions: **[move], [compromise], [drop], [give], [exchange], [pickup], [recover]**
2. [loot]
   Draw 2 **[lo0t!]** cards. Resolve **[intrusion detected]** and **[honeypot audit]** cards.
3. [patch]
   Draw and resolve **[patch!]** cards, as indicated by the **[infocon]** level.
4. [check]
   Discard, to obey the hand limit.

[intrusion detected]: Raise the **[infocon]** level.

[honeypot audit]: Immediately draw a **[patch!]** card. If the pictured **[node]** is compromised, raise the **[infocon]** level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play **[zero-day exploits]** before discarding them.

[patch] situations:

- Any **[lo0t!]** cards left on a **[node]** being patched are discarded.
- If a player is on a node being patched, she must **[move]** to a compromised node (obeying normal movement rules), then **[decommission]** the node and its **[patch!]** card.
- **[zero-day exploits]** can be used to prevent all **[patch]** effects.

order of play

1. **[action]**
   Take up to 3 actions:
   [move], [compromise], [drop], [give], [exchange], [pickup], [recover]
2. **[loot]**
   Draw 2 **[lo0t!]** cards. Resolve **[intrusion detected]** and **[honeypot audit]** cards.
3. **[patch]**
   Draw and resolve **[patch!]** cards, as indicated by the **[infocon]** level.
4. **[check]**
   Discard, to obey the hand limit.

order of play

1. **[action]**
   Take up to 3 actions:
   [move], [compromise], [drop], [give], [exchange], [pickup], [recover]
2. **[loot]**
   Draw 2 **[lo0t!]** cards. Resolve **[intrusion detected]** and **[honeypot audit]** cards.
3. **[patch]**
   Draw and resolve **[patch!]** cards, as indicated by the **[infocon]** level.
4. **[check]**
   Discard, to obey the hand limit.

order of play

1. **[action]**
   Take up to 3 actions:
   [move], [compromise], [drop], [give], [exchange], [pickup], [recover]
2. **[loot]**
   Draw 2 **[lo0t!]** cards. Resolve **[intrusion detected]** and **[honeypot audit]** cards.
3. **[patch]**
   Draw and resolve **[patch!]** cards, as indicated by the **[infocon]** level.
4. **[check]**
   Discard, to obey the hand limit.

[intrusion detected]: Raise the **[infocon]** level.

[honeypot audit]: Immediately draw a **[patch!]** card. If the pictured **[node]** is compromised, raise the **[infocon]** level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play **[zero-day exploits]** before discarding them.

[patch] situations:

- Any **[lo0t!]** cards left on a **[node]** being patched are discarded.
- If a player is on a node being patched, she must **[move]** to a compromised node (obeying normal movement rules), then **[decommission]** the node and its **[patch!]** card.
- **[zero-day exploits]** can be used to prevent all **[patch]** effects.

[intrusion detected]: Raise the **[infocon]** level.

[honeypot audit]: Immediately draw a **[patch!]** card. If the pictured **[node]** is compromised, raise the **[infocon]** level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play **[zero-day exploits]** before discarding them.

[patch] situations:

- Any **[lo0t!]** cards left on a **[node]** being patched are discarded.
- If a player is on a node being patched, she must **[move]** to a compromised node (obeying normal movement rules), then **[decommission]** the node and its **[patch!]** card.
- **[zero-day exploits]** can be used to prevent all **[patch]** effects.

[intrusion detected]: Raise the **[infocon]** level.

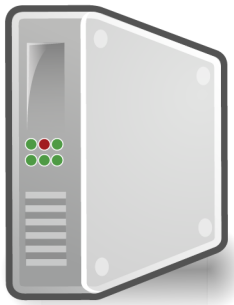
[honeypot audit]: Immediately draw a **[patch!]** card. If the pictured **[node]** is compromised, raise the **[infocon]** level.

[check]: The hand limit is five cards. Every card in excess of the hand limit must be discarded. You may play **[zero-day exploits]** before discarding them.

[patch] situations:

- Any **[lo0t!]** cards left on a **[node]** being patched are discarded.
- If a player is on a node being patched, she must **[move]** to a compromised node (obeying normal movement rules), then **[decommission]** the node and its **[patch!]** card.
- **[zero-day exploits]** can be used to prevent all **[patch]** effects.

client



client

client

client

intrusion detection system

requires two actions to compromise

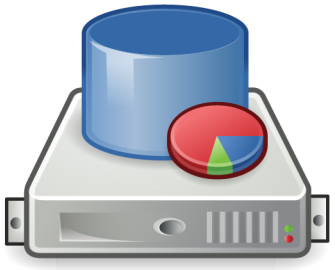
intrusion detection system

requires two actions to compromise

chat server

chat server

sales database



sales database

primary DNS server

primary DNS server

SMTP server

SMTP server

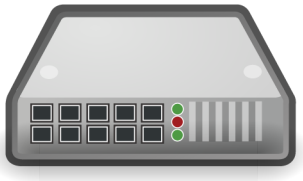
single sign-on service

single sign-on service

backup
file server

backup
file server

VLAN switch



VLAN switch

wireless router

wireless router

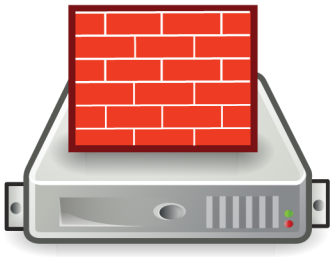
client

client

client

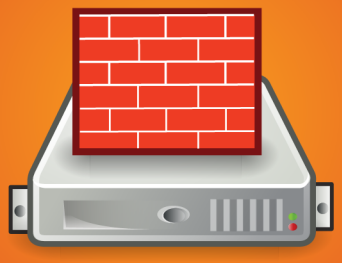
client

firewall



requires two actions
to compromise

firewall



requires two actions
to compromise

secondary
DNS server

secondary
DNS server

internet
gateway

internet
gateway

IMAP server

IMAP server

VPN gateway

requires two actions
to compromise

VPN gateway

requires two actions
to compromise

certificate services

certificate services

VoIP server

VoIP server

web server

web server

NAT device

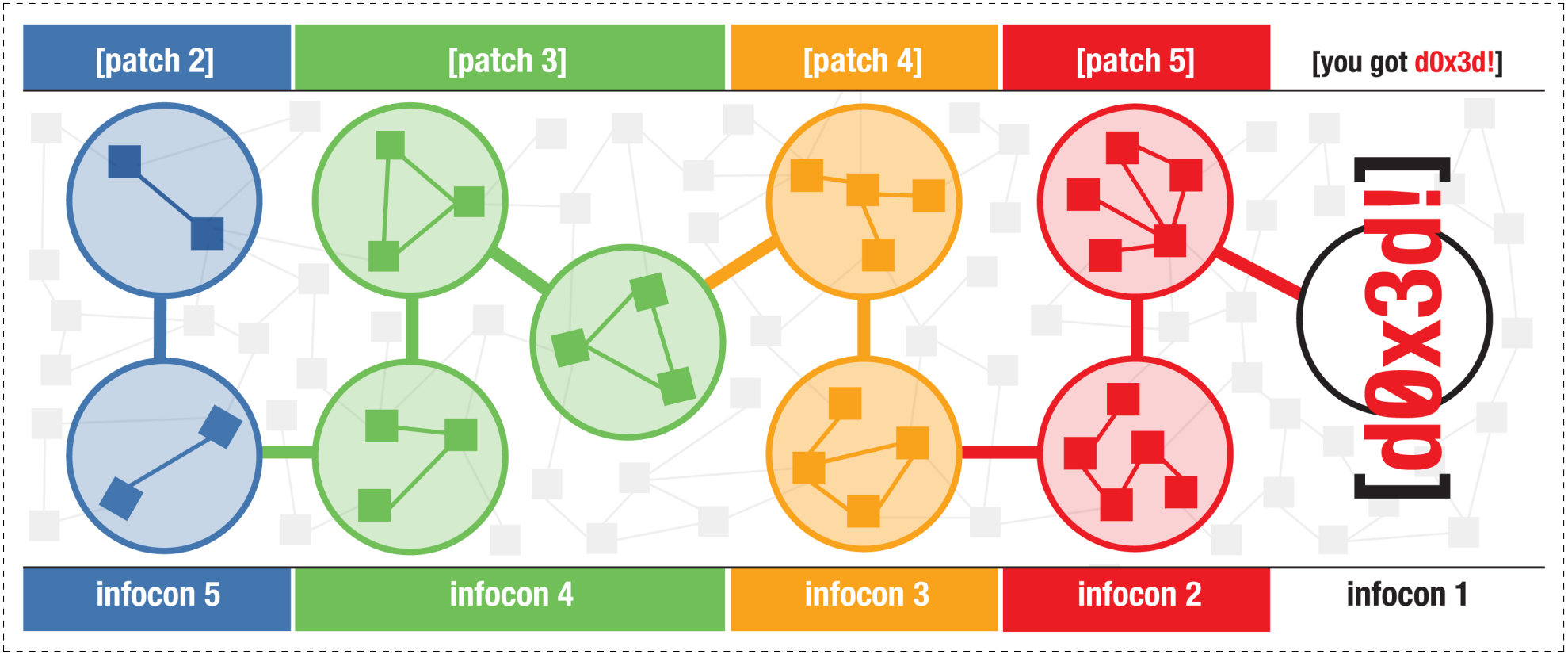
NAT device

network
file server

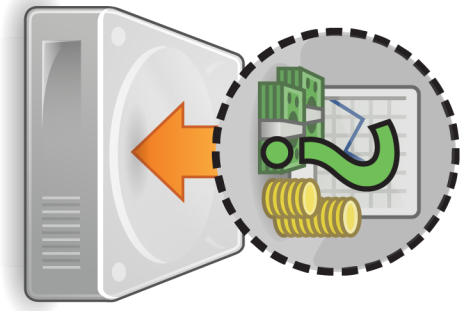
network
file server

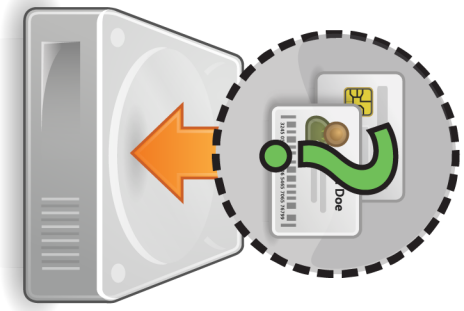
customer
database

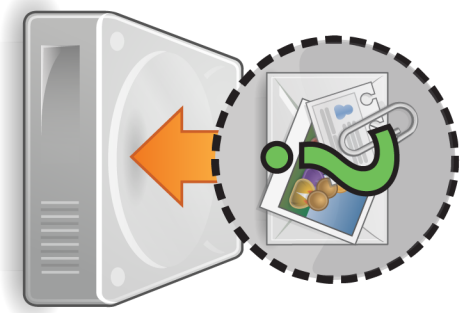
customer
database

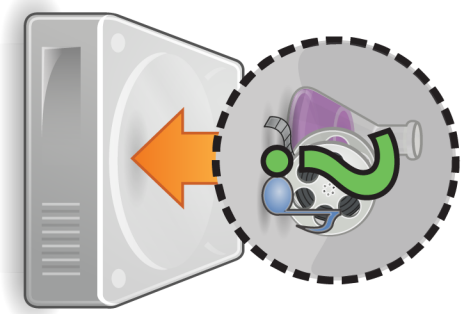

[patch 2]
[patch 3]
[patch 4]
[patch 5]
[you got d0x3d!]
[d0x3d!]
infocon 5
infocon 4
infocon 3
infocon 2
infocon 1

[digital asset drives]

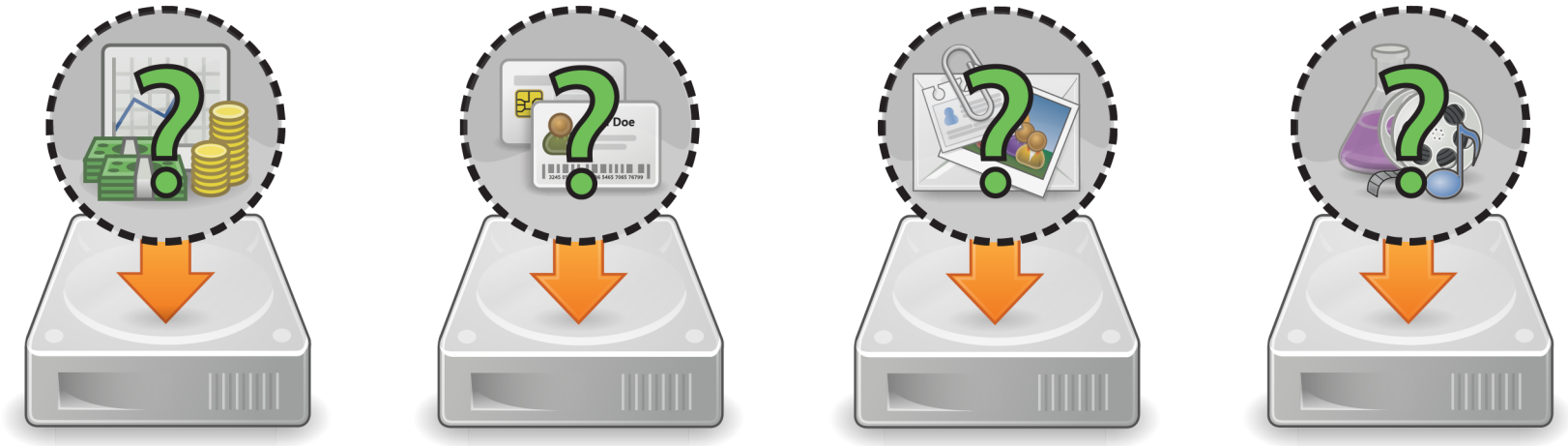








[digital asset drives]



financial data

authentication credentials

personally identifiable information

intellectual property