ray@rootcon:~$ cd /tmp/presentation

Adaptive Jumpoff Server Design for Implementing Honeypots

ray@rootcon:~$ whoami

Ray Divinagracia Torres

- BS Computer Science, UP Diliman (*Magna Cum Laude*, Batch 2014)
- MS Computer Science, UP Diliman (2015 - present)
- CTF: Age of Extinction -- Hack in the Box, Kuala Lumpur Malaysia (Oct 2014)
- CISA Exam Passer (June 2015)

ray@rootcon:~$ cat honeypots_definition.txt

What are honeypots?

- A security resource whose value lies in being probed, attacked, or compromised (Spitzner, 2002)

ray@rootcon:~$ cat honeypots_definition.txt

What are honeypots?

- A security resource whose value lies in being probed, attacked, or compromised (Spitzner, 2002)
- Highly flexible -- can be used to achieve different goals

ray@rootcon:~$ cat honeywords.txt

What are honeywords?

- Improves the functionalities of honey-accounts (planted user accounts that trigger an alarm when used by an adversary)

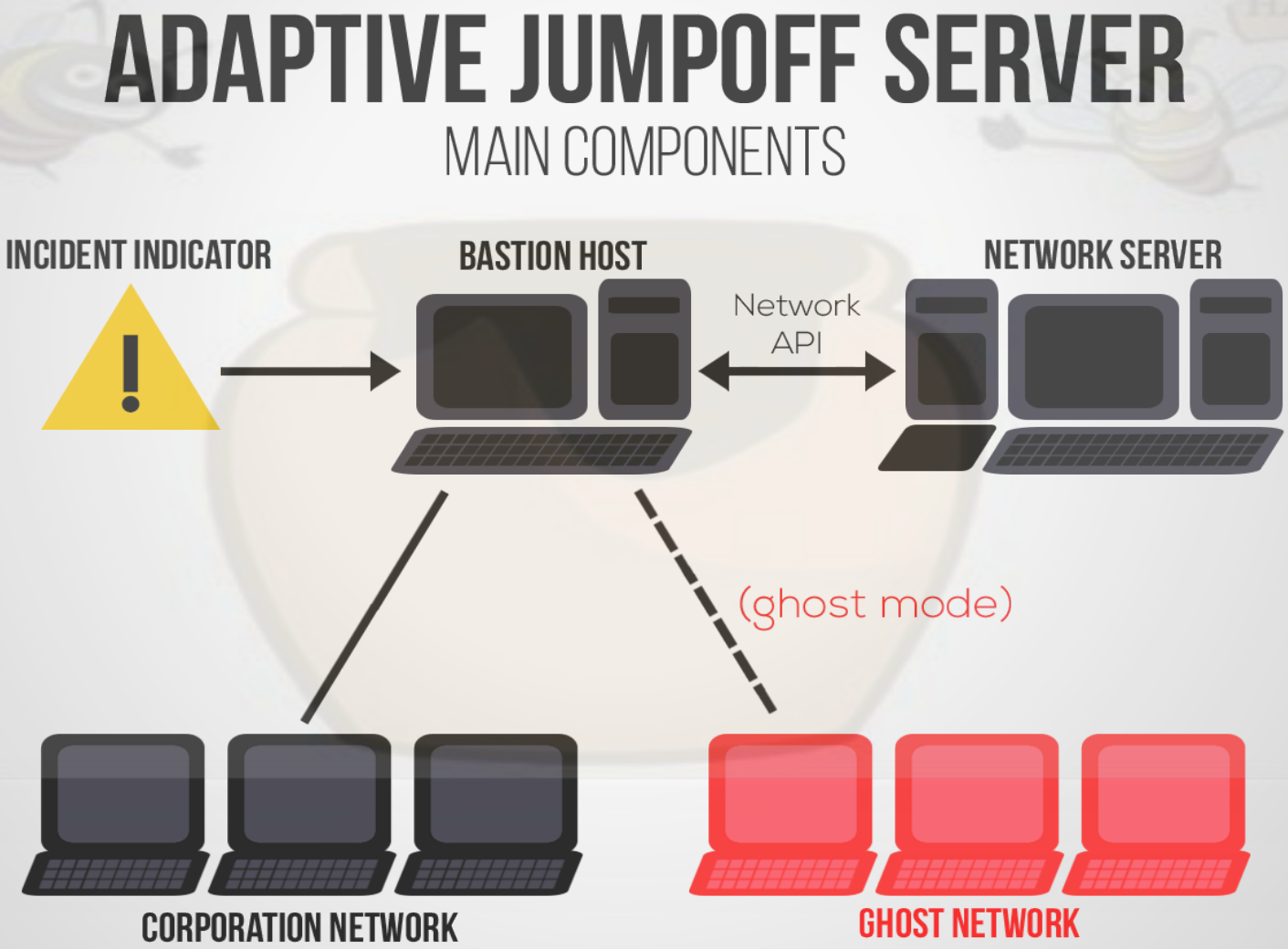
ray@rootcon:~$ cat honeywords.txt

What are honeywords?

- Improves the functionalities of honey-accounts (planted user accounts that trigger an alarm when used by an adversary)

- honeywords is a term coined by Ari Juels and Ronald Rivest that refers to accounts (either real or honey-accounts) having multiple possible passwords, where only one of which is genuine

ray@rootcon:~$ eog design_architexture.jpg



ray@rootcon:~$ cat incident_indicator.txt

- Use of a honey-account with or without honeywords as a point of entry

ray@rootcon:~$ cat incident_indicator.txt

- Use of a honey-account with or without honeywords as a point of entry

- ideally this is the trigger for an incident state

ray@rootcon:~$ cat bastion_host.txt

- an “ideally” hardened jumpoff server

ray@rootcon:~$ cat bastion_host.txt

- an “ideally” hardened jumpoff server
- uses the idea of it being “hardened” to camouflage itself from being a honeypot

ray@rootcon:~$ cat bastion_host.txt

- an “ideally” hardened jumpoff server
- uses the idea of it being “hardened” to camouflage itself from being a honeypot
- functions as a legitimate jumpoff server until the incident state is triggered

ray@rootcon:~$ cat network_server.txt

- server that handles the network configuration of the BH

ray@rootcon:~$ cat network_server.txt

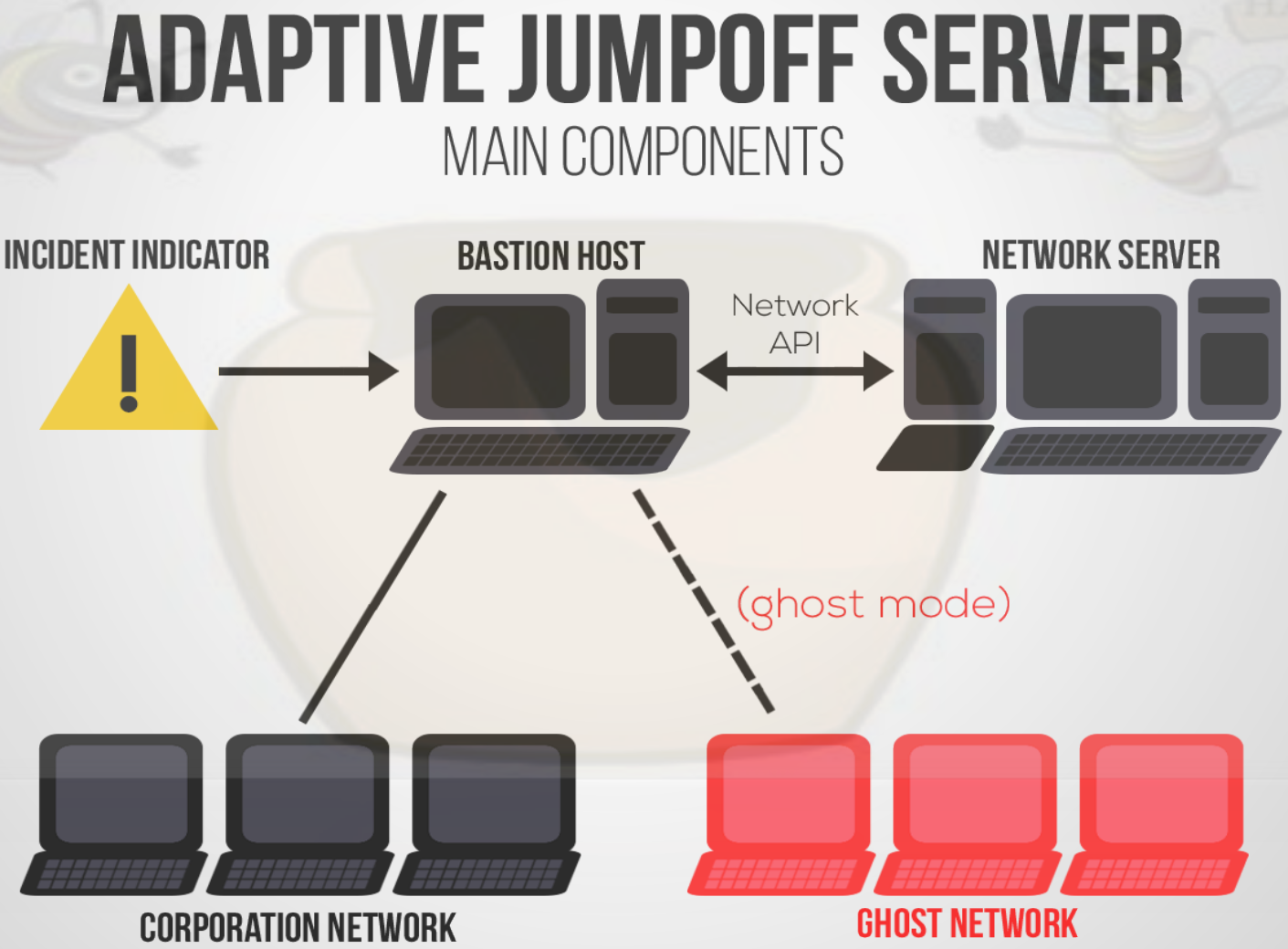
- server that handles the network configuration of the BH
- communicates with the BH through a network API

ray@rootcon:~$ cat network_architecture.txt

Normal Setup VS Ghost Setup

- normal setup is the production network that the jumpoff server sees
- ghost setup is the honeypot network (or honeynet)

ray@rootcon:~$ eog design_architexture.jpg



ray@rootcon:~$ cat process_flow.txt

1. Honey-account (with or without honeywords) is used. (Incident Indicator is triggered)

ray@rootcon:~$ cat process_flow.txt

1. Honey-account (with or without honeywords) is used. (Incident Indicator is triggered)

2. BH notifies NS about the Incident

ray@rootcon:~$ cat process_flow.txt

3. NS acks, changes BH's VLAN config from normal to ghost network

    a. BH continues to log all movements by the adversary and send them to NS

    b. During the incident, if a sudo login is made, NS is notified to shutdown the connection. This is called the isolation state

    c. During the isolation state, connection from the BH is ended. Only the Ghost network will be actively logging the movement of the attacker (probes, ssh attempts, etc)

ray@rootcon:~$ cat state_transition.txt

1. Use pre-configured shell for honey account or account with honeyword

ray@rootcon:~$ cat state_transition.txt

1. Use pre-configured shell for honey account or account with honeyword

2. Accounts in /etc/passwd & /etc/shadow will be replaced by false accounts --> also replace auth logs and account names on other logs

    a. Delete all private data by the organization

```
ray@rootcon:~$ screen ; reptyr ($pgrep \
demo_honeyd)
```

DEMO

```
ray@rootcon:~$ screen ; reptyr ($pgrep \
demo_kippo)
```

kippo

SSH Honeypot

DEMO

ray@rootcon:~$ cat considerations.txt

- Hardening method for BH and NS

ray@rootcon:~$ cat considerations.txt

- Hardening method for BH and NS
- What logs to replace

ray@rootcon:~$ cat considerations.txt

- Hardening method for BH and NS
- What logs to replace
- What other things to replace during state transition -- dependent on network setup of the organization

ray@rootcon:~$ cat considerations.txt

- Hardening method for BH and NS
- What logs to replace
- What other things to replace during state transition -- dependent on network setup of the organization
- Memory resident data

ray@rootcon:~$ cat advantages.txt

- Prevention of further compromise

ray@rootcon:~$ cat advantages.txt

- Prevention of further compromise
- Detection of insider attacks

ray@rootcon:~$ cat advantages.txt

- Prevention of further compromise
- Detection of insider attacks
- Analysis

ray@rootcon:~$ cat cons_risks.txt

- Cost of additional resources (for setup and monitoring)

ray@rootcon:~$ cat cons_risks.txt

- Cost of additional resources (for setup and monitoring)
- Compromise of legitimate production or corporate servers

ray@rootcon:~$ tail presentation

Questions?

References

Book/Paper Sources:

- Honeypots: Tracking Hackers by Lance Spitzner (2002)
- Honeywords: Making Password-Cracking Detectable by Ari Juels and Ronald L. Rivest

Image Sources:

http://1.bp.blogspot.com/-sxx0mXXKSrk/UdfA_sG0pxI/AAAAAAAAAR0/yZgXyh6kUww/s1600/honey-pot-and-bees-on-background-of-honeyconb-hackers_group_of_india.jpg

https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcRXn4JteNxaAZtCaGgsoq9rbyfdU48Ij1pdRBqBozLqb_oJeiRJ

https://wikidownload.com/Download/incident-icon.jpg

http://www.yell.com/static/image/f84efa56-854a-49f7-a7ce-7d57f0785be4_image_jpeg?t=tr/w:550/h:412/m:FitPad

https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcTG9u9I1mXKaYBpQ6EAzKl9gFHhaqBoaBzufjHVHtzPH5B1qfOp

http://www.cliparthut.com/clip-arts/488/process-clip-art-488802.jpg

http://www.honeyd.org/images/honeyd-logo.gif

https://avatars0.githubusercontent.com/u/952610?v=3&s=400

http://www.honeynet.tn/saher/3.png

https://encrypted-tbn3.gstatic.com/images?q=tbn:ANd9GcT_fwi-LzcqZvOXayW20cGwCrEh7KWHVPzGDH2aADI4L9doFXaA