The Reconstruction of Isengard

The Design, Implementation, and Testing of a Bastion Host

Alex Hurd and Eric Richter

Clarkson Open Source Institute

April 23, 2014

Topics

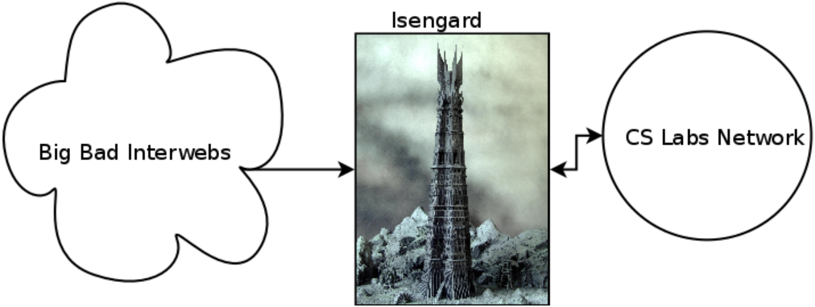
- Bastion Host
  - About
  - Setup
  - Passwords
- CS Lab Network Reconfiguration
  - Implemented Security Policies
  - Network Monitoring/Firewall/Routing “HyperCube”

Bastion Host

Bastion Host

What is a Bastion Host?

- Bridge between internal network and outside world
- Elevated security



Bastion Host (cont.)

Why is a Bastion Host important?

- Extra security (Obviously!)
- Monitoring/Accountability
- First layer of attacks from the outside

What goes behind the Bastion Host? (i.e. what goes through it?)

- All external SSH Traffic. This includes:
  - Internal Services
  - Web Hosts
  - Student Projects
  - ...and so on

Building the Bastion Host

Setup

- Virtual Machine
- OpenBSD 5.4 x86_64

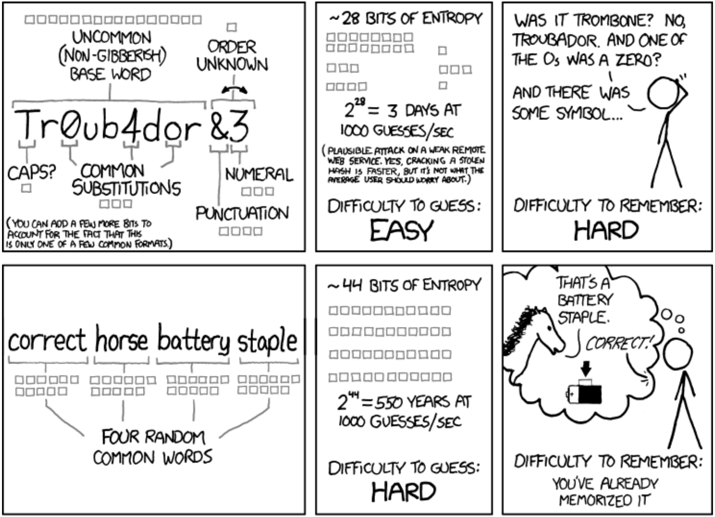
Configuration

- SSH on port 1122
- Sudo actually reports incidents
- Password complexity requirements
- Send logs to Storage

```
robm@homebox ~$ sudo su
Password:
robm is not in the sudoers file.
This incident will be reported.
robm@homebox ~$ █
```

HEY — WHO DOES SUDO REPORT THESE "INCIDENTS" TO?
YOU KNOW, I'VE NEVER CHECKED.
NICE
NAUGHTY

Password Complexity


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Password Complexity

Implement a "Minimum Entropy Requirement"

Several ways to meet (but not limited to):

- Around twelve characters (letters, numbers, symbols)
- Non-dictionary words OR
- Lengthy combination of words (a la xkcd)
- Generated Passwords (e.g. Pass, KeyPass)

Network Reconfiguration

Network Reconfiguration (cont.)

128.153.144 $\Longrightarrow$ Inaccessible from Outside

- COSI/ITL Lab Machines
- Wireless Network (dd-wrt)
- Open Ethernet Ports

128.153.145 $\Longrightarrow$ SSH through Isengard

- Internal Services

128.153.146 $\Longrightarrow$ SSH from Clarkson, everything else open

- Web Hosts
- Student Projects

Network Reconfiguration (cont.)

Security Policies

- Europa & Juno: Enforce SSH traffic only from Isengard
- Titan: Enforce SSH traffic from only Clarkson's Network (including Isengard)

"HyperCube"

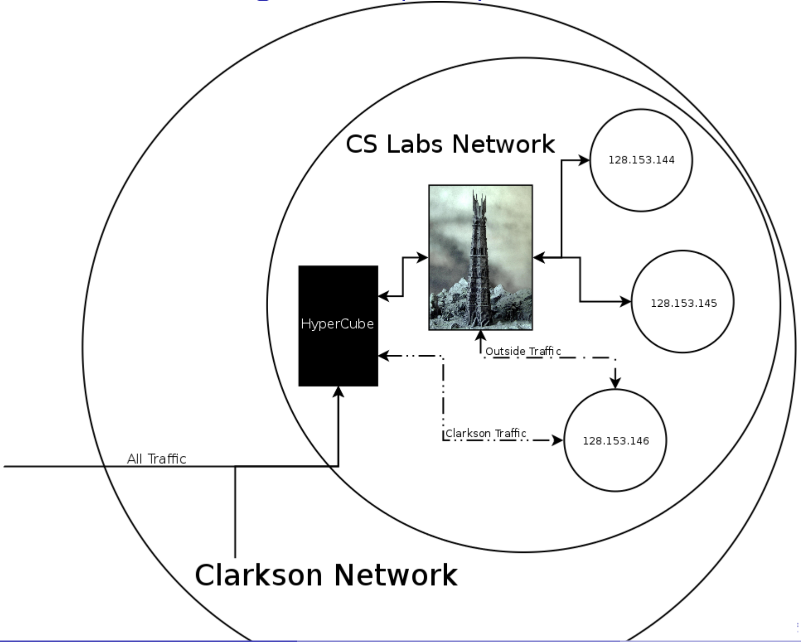
What is the Network Monitoring/Firewalling/Routing Box?

- Intermediary between ALL traffic in and out of the network
- Traffic monitoring
- Act as a stateful firewall
- Have the capabilities to perform deep pack inspection

Why is this "HyperCube" important?

- More security
- Pinpoint network abnormalities
- Provide usage statistics

Network Reconfiguration (tl;dr)



Questions?