Using Honeypots for Security Operations

Jim Barlow

<jbarlow@ncsa.uiuc.edu>

Head of Security Operations and Incident Response

National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign

Outline

- Honeypots and why did we start using them?
- Details on incident involved with
- Setting one up and honeypot activity
- What we learned
- Other areas of application
- Future work

Traditional Honeypots

- First used for researching blackhat activity
  - Set up a honeypot, see who breaks in
- Know your enemy papers

Why did we set one up?

- Had incident where we wanted to get specific intruder on our honeypot to monitor
- Persistent intruder
  - Generally intruders move to greener pastures when discovered

What did we want to find?

- Where are they coming from?
- Where are they going?
- What tools are they using?
- What exploits are being used?
- Motive?

More details on incident

- Miscreants were using trojaned ssh clients to compromise accounts
- Would then attempt local exploits
- Large number of compromised accounts and machines
- Tended to use same system to launch attacks for days or weeks
- Can we get them to use our system?

Setting up honeypot

- If we build it, will he come?
  - Can be a hard problem, how to get specific intruder onto our honeypot?
- Bait and Switch honeypots
  - http://baitnswitch.sourceforge.net/
- US DoD – Net Force Maneuver
- We decided to use Sebek from honeynet.org
- Used their own tool against themselves
  - Use trojaned ssh client to log into honeypot

First honeypot activity

- **Fed account into their “collector” using tojaned ssh client (on compromised machine).**
- **Intruders logged into our honeypot within 2 minutes**
- **There were no local vulnerabilities on honeypot**
- **Session 1 output**

What did this tell us?

- Actively using and monitoring passwords collected
- Specific commands they used
  - Some of what they initially look for
- ssh host sh -i
- IP address attacking from

Honeypot round 2

- Second account fed took three hours to log into system
- Session 2 output
- Different command syntax
  - Does that tell us anything?
- Few more hits over next couple days

Additional hits on second hp

- Spent more time on system around a week later
- Some interesting information
  - Looking for exported filesystems
  - Targeting our teragrid cluster
  - Download and use of nfsshell tool
- Session 3 output

Third times a charm?

- Fed account on third honeypot system
  - Knew format of password collector and could feed accounts at random
- Compromised machine on our network using scan and sploit.
  - We were able to see everything they did on the compromised system.
  - Lots of interesting items discovered
- Session 4 output

Other interesting sessions

- Started giving them boxes that could be rooted
  - Would they start using the machine more?
- After getting root
  - Didn't install standard rootkit
  - Installed mod_rootme package
    - Started web server as root
    - OpenSSL led to additional compromise

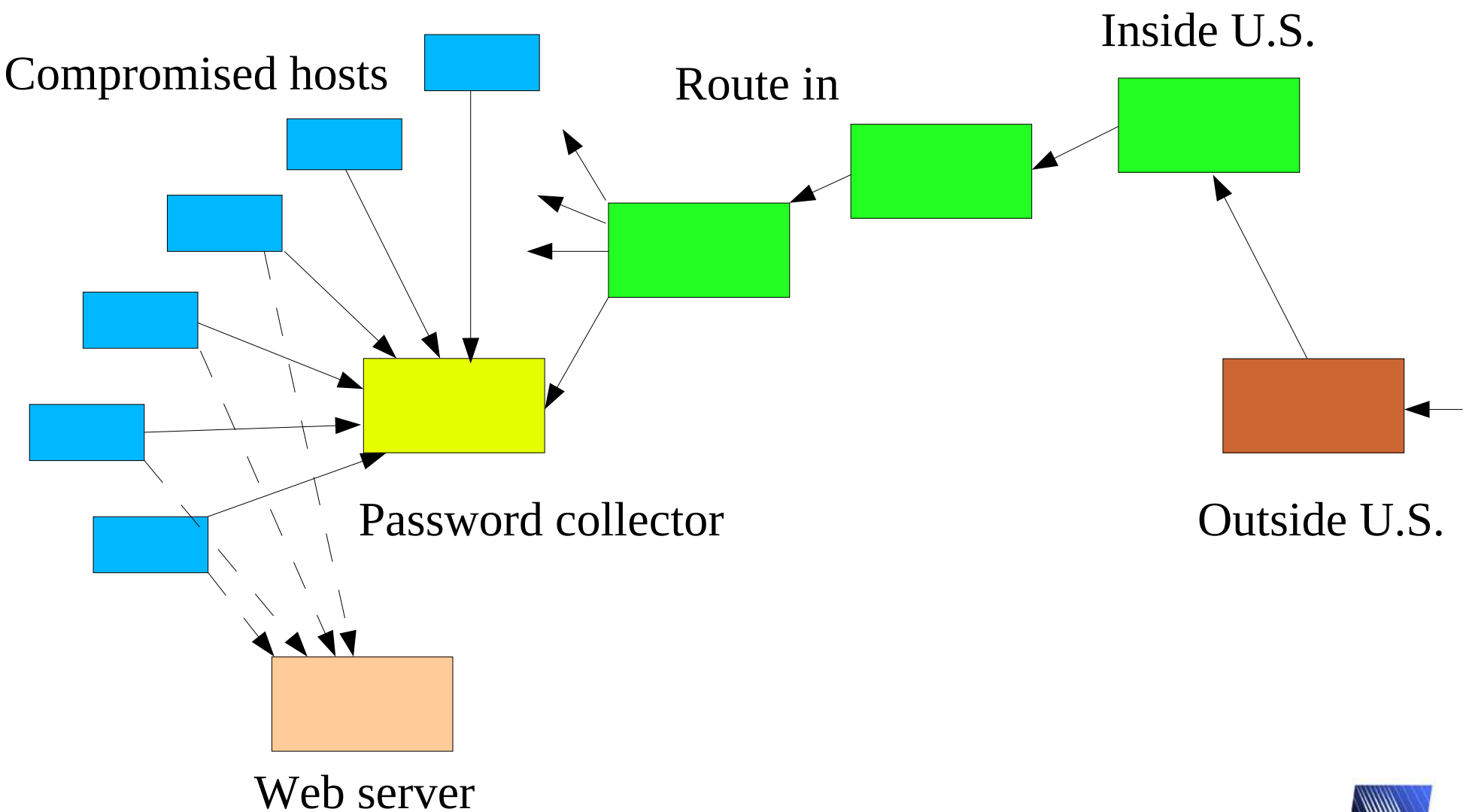
How did this all help us?

- Categorize vulnerabilities being exploited
- Identify IP address attacking from
- Get tools being used
  - How and where they were getting them from
    - ie. uuencoding – thought safe
- Share all this with trusted community
  - Also created “info file” that could be shared with newly affected sites

What else did this tell us about the miscreant?

- Strange habit of logging in, out, and back in again
  - Why? More than one person?
- Once on machine logs onto localhost
  - Changes last login entry
- Seems all attacks were done manually
- Occasional special characters typed
  - Foreign character set?
- Maybe possible to analyze commands to determine if more than one person
- Eventually hp not needed (at times)

Attack network



Other areas we are using honeypots

- SSH brute force logger
  - Logging usernames and passwords for last 9 mo.
  - Create account with one of these common ones and watch what they do
  - Wash/rinse/repeat
    - Categorize attackers?
- X server honeypot
- Remote site with similar name
  - ncsa.teragrid.org vs. ncsa.org

Other uses of honeypots/honeytokens

- Honeytokens/web bugs
  - Bugged email
  - Web page/email archive
    - How long till it's mined off of google?
- Online forensics from honeypot
  - Needed to access remote machine
  - Log in from ssh password collector
  - Thought compromised host was blocked at border

Future Work

- **Distributed honeynet**
  - **Same username at multiple sites (known_hosts attack)**

Questions?

Gracias

jbarlow@ncsa.uiuc.edu