IDENTIFYING BRUTE FORCE HOST ACCESS ATTEMPTS

Joe McManus
Aaron Shelmire
CMU 95-855
December 8th 2008

GOALS

- Identify Brute force host access attempts
- Create scripts to find this behavior in flow data using SiLK
- Study common username password services
  - 22/SSH
  - 23/Telnet
  - 143,220,585,993/IMAP/IMAPS

TYPES OF ATTACKS

- Many attacks are initiated by port scan.
- Two main types of attacks
  - Dictionary Attacks
  - Brute Force Attacks

DICTIONARY ATTACKS

- Attempts well known usernames and passwords
  - i.e. jsmith/jsmith
- Tries entire “dictionary” database for passwords
- Tries service usernames
  - i.e oracle/tiger
  - root/toor

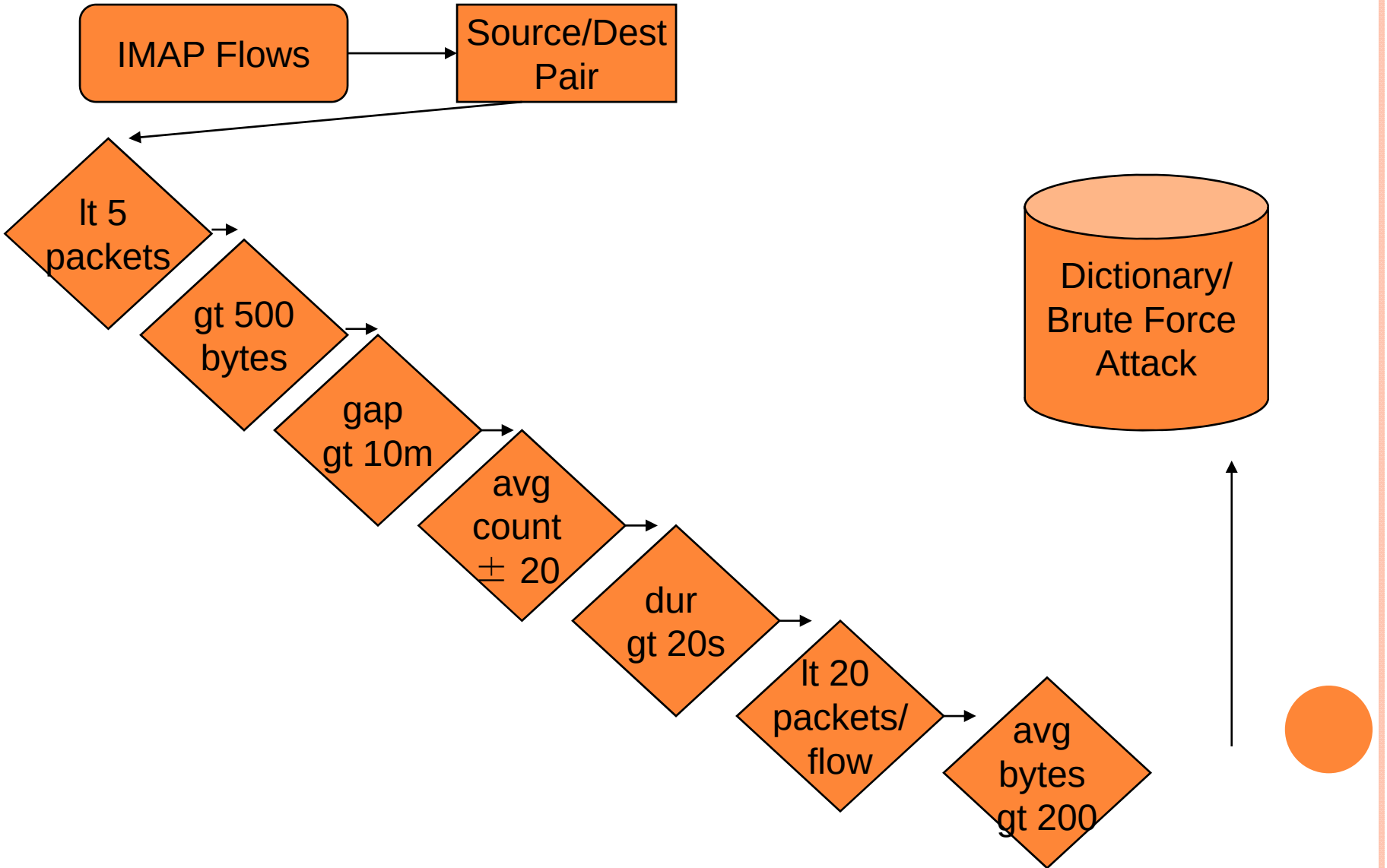
BRUTE FORCE ATTACKS

- Also uses well known usernames and passwords
- Will try many combinations, in an attempt to guess all possible combinations
- In flow analysis both types of attacks look similar.

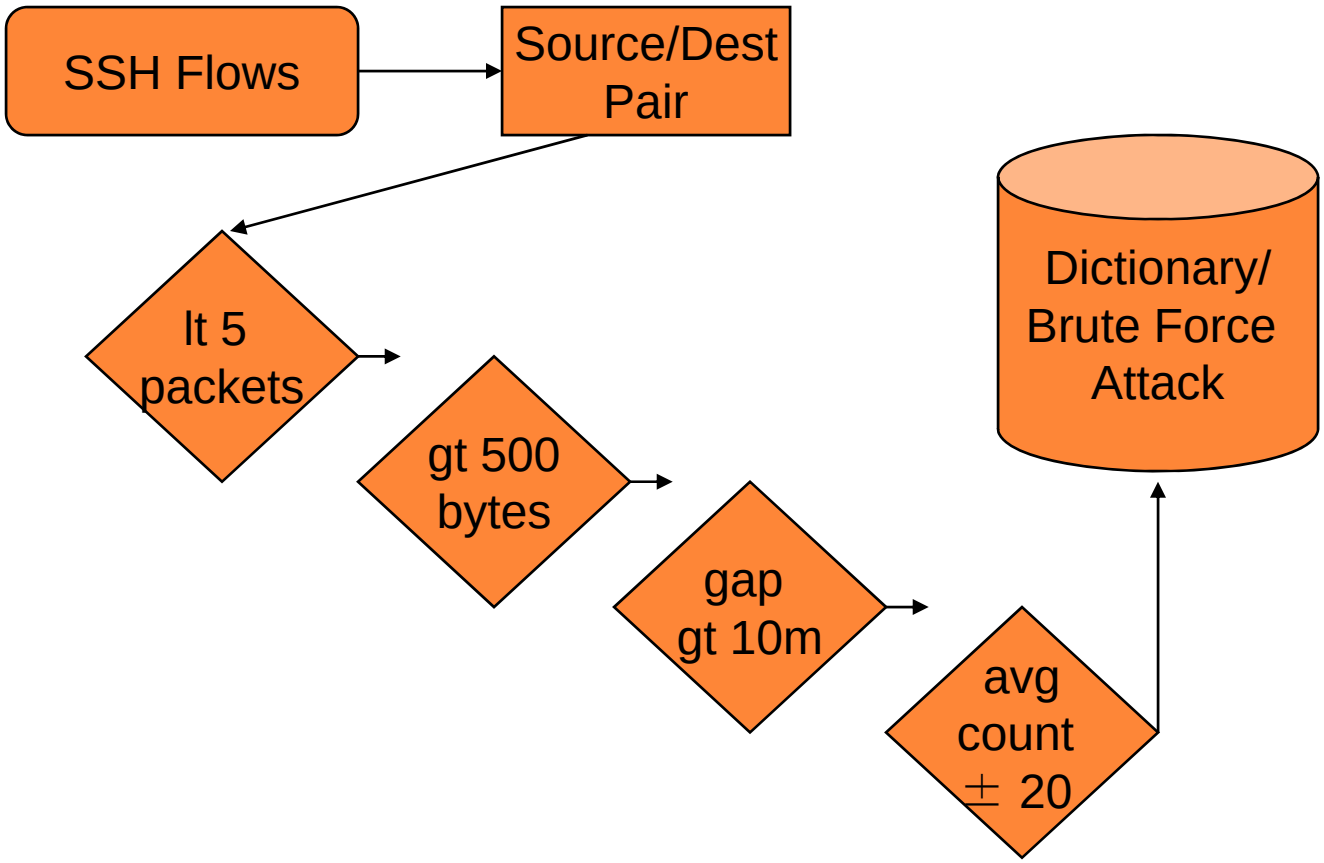
Attack Characteristics

- Automated
  - Uniform data rate
  - Packet size roughly similar
  - Many flows
  - Duration of a few minutes

IMAP Analysis



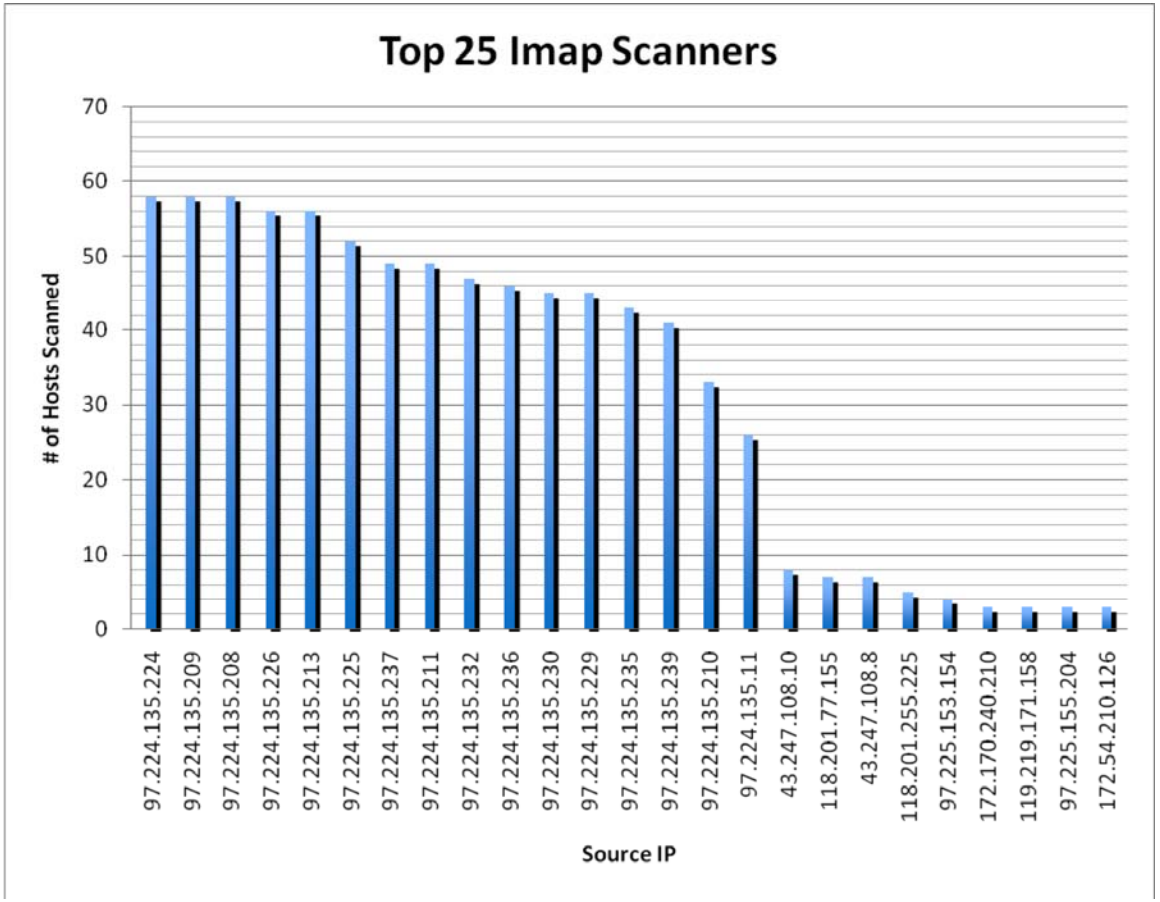
SSH Analysis



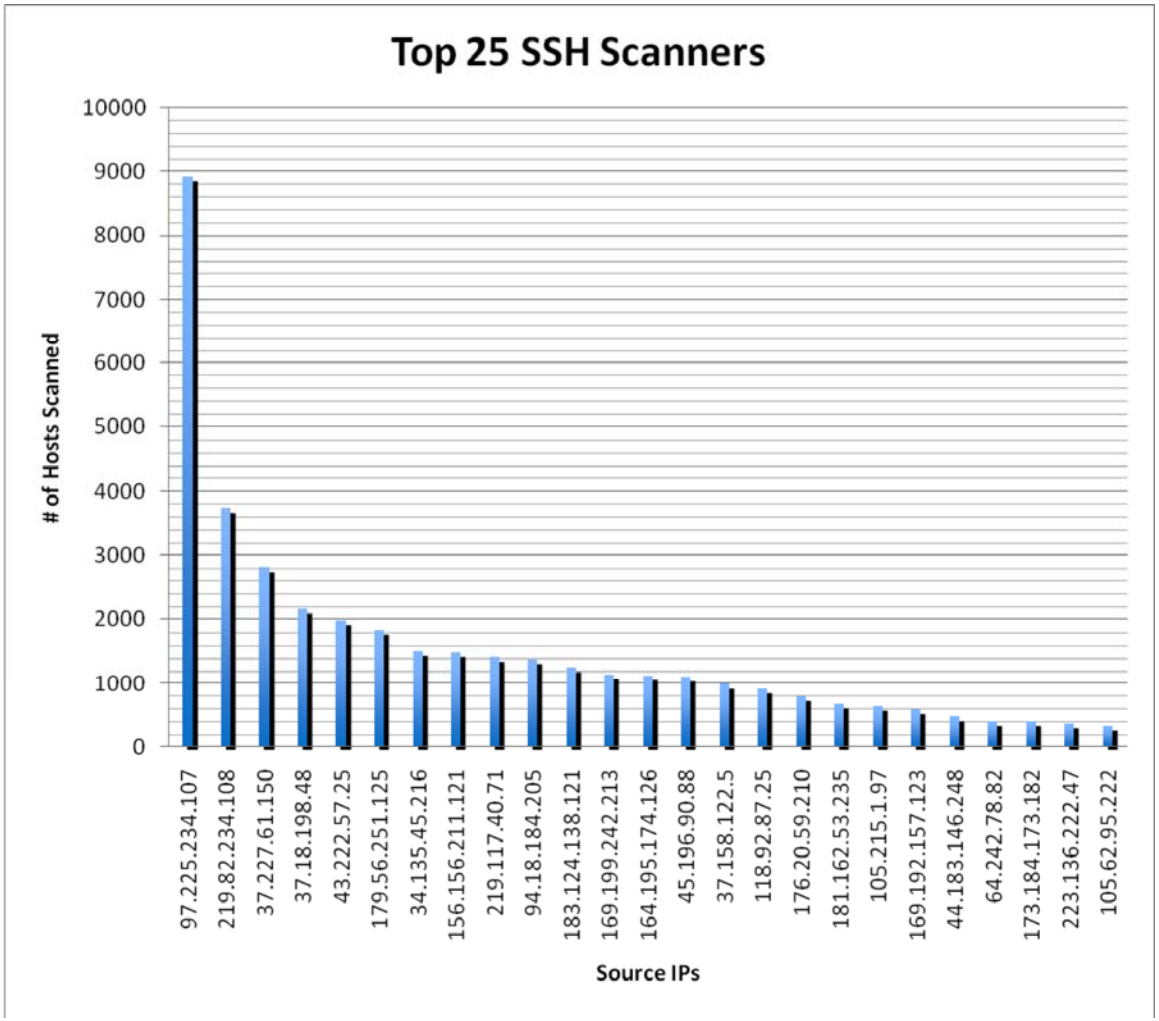
Suspicious Scanning Traffic

- We looked at the minimum amount of traffic that scanning a port would create for each protocol.
- If a machine responded back more than the minimum per flow it would be marked as suspicious.
- A flexible bash script wrapping around the SiLK tool suite.
- Ineffective as it is a simple test only looking at minimum amount of bytes per flow.
- Only ties scanner to traffic, many times scanning and attempts are from two different Ips.

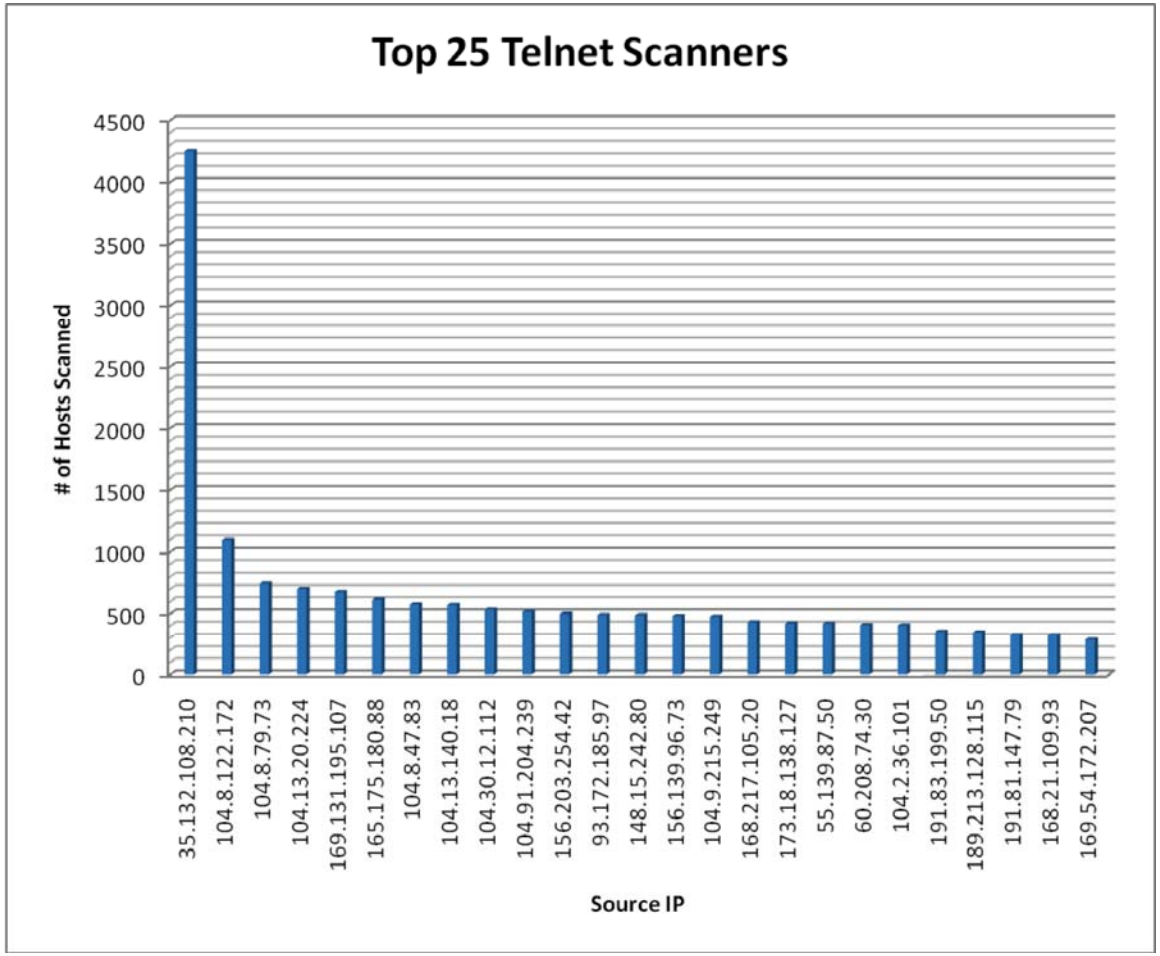
IMAP Scanners



SSH Scanners



TELNET Scanners



CONCLUSION

- We studied three types of traffic. However only SSH showed any compromised hosts.
- SSH also is the most scanned port in our data
  - Firewalls should be used to lock down SSH access
  - Open source tools should be used that block access based on scanning/brute force behavior
  - Leveraging netflow data should be done for full situational awareness.

WHERE DO WE GO FROM HERE?

- Automate detection process to run in a close to real time manner to block Brute Force behavior.
- Automate detection tools to plug in to IP Tables to block traffic in a close to real time manner.
- Flag compromised hosts and study the behavior to determine characteristic behavior of compromised hosts.