Session Five – Blue team Ops/log analysis

This session sees us investigate a possible compromise of a web server through analysis of log files.

Log files provide one of the most effective ways to keep a record of what has happened on a system. Being able to use these files effectively and sift through them to find items of interest is a core skill for blue team ops.

Each main part of the puzzle is on a new page to prevent spoliers from reading ahead.

Part 0 – Setting up a Linux environment

- The command line tools that come included in Linux OSs make them ideal for dealing with file manipulation tasks. For this task it is recommended that you use a Linux environment (the Mac terminal may also work). This can be achieved on a Windows machine through VM software such as VirtualBox
- For those without access to the above for this practical, a copy of the files is stored on the CyberBulls activity server at 35.176.93.174 under /home/guest/logs
- This can be accessed over ssh via the Putty program.

Part 1 – Command Line Tools Refresher

A basic grasp of command line skills is required in order to efficiently navigate large logfiles. Key commands are mentioned below

- Grep – this command is used to filter a file for lines containing a given string.
    - Using the –v flag will inverse this and filter out any lines containing the given string

    - e.g. cat file.txt | grep something | grep –v nothing | less
- Less – this command presents a piped output in a scrollable view
- Tail – this command displays the last few lines of a file
    - e.g. cat file.txt | tail –n 100 | less for the last 100 lines

Part 2 – Key log files

The log files recovered from the compromised web server contain a variety of logs from different sources. Look up the role of the following logs – these will be important when trying to find the compromise

- Auth.log
- Daemon.log
- Dpkg.log

Part 3 - Solving the problem

Now that you are up to speed on log analysis, head to https://www.honeynet.org/challenges/2010_5_log_mysteries and work through the questions on the compromise. This can either be approached through manually investigating the logs on the command line, using a script to complete the task or by downloading log analysis tools. Some hints are included below.

- The auth.log file is key to finding failed log in attempts which would be part of a brute force attack. Can you find the attacker IPs through this and then search for a valid logon from that IP?
- Once a rough timestamp for the attack is established, grep or tail can be used to filter for lines around the area of that timestamp. These are likely to be of interest.

- Think about the type of tasks that an attacker might wish to do after gaining access. Looking through the logs for evidence of adding users, opening up the firewall or installing new software could be a good place to start.

Part 4 – Extensions

Once a general idea of the compromise and a rough timeline has been worked out, try to automate the task of finding timestamps and IPs of brute force attackers if you have not done so already.

The log files contain multiple examples of bad security practices and sys admin on the system. See what examples you can find of this – what would you do to fix it?