Logging: Supplement

# Notes & References

Table 10-1. Default logging system(s), by Linux distribution

|  |  |
| --- | --- |
| CentOS 5 | syslog |
| CentOS 6 | rsyslog |
| CentOS 7 | rsyslog and journalctl |
| Mint 11-17 | rsyslog |
| Min 18, 18.1 | rsyslog and journalctl |
| OpenSuSE 11.4, 12.1, 12.2 | rsyslog |
| OpenSuSE 12.3, 13.1 | rsyslog and journalctl |
| OpenSuSE 13.2, 42.1, 42.2, 42.3 | journalctl |
| Ubuntu 11.04-14.10 | rsyslog |
| Ubuntu 15.04-17.10 | rsyslog and journalctl |

Table 10-2. Default Syslog Daemon by Linux Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| CentOS 5.6 | syslogd 1.4.1 | Mint 17.3 | rsyslog 7.4.4 |
| CentOS 5.7 | syslogd 1.4.1 | Mint 18 | rsyslog 8.16.0 |
| CentOS 5.8 | syslogd 1.4.1 | Mint 18.1 | rsyslog 8.16.0 |
| CentOS 5.9 | syslogd 1.4.1 | Mint 18.2 | rsyslog 8.16.0 |
| CentOS 5.10 | syslogd 1.4.1 | Mint 18.3 | rsyslog 8.16.0 |
| CentOS 5.11 | syslogd 1.4.1 | OpenSuSE 11.4 | rsyslogd 5.6.3 |
| CentOS 6.0 | rsyslogd 4.6.2 | OpenSuSE 12.1 | rsyslogd 5.8.5 |
| CentOS 6.1 | rsyslogd 4.6.2 | OpenSuSE 12.2 | rsyslogd 5.8.11 |
| CentOS 6.2 | rsyslogd 4.6.2 | OpenSuSE 12.3 | rsyslogd 7.2.5 |
| CentOS 6.3 | rsyslogd 5.8.10 | OpenSuSE 13.1 | rsyslogd 7.4.4 |
| CentOS 6.4 | rsyslogd 5.8.10 | OpenSuSE 13.2 | rsyslog 8.4.2-1.1 |
| CentOS 6.5 | rsyslogd 5.8.10 | OpenSuSE 42.1 | rsyslog 8.4.0-4 |
| CentOS 6.6 | rsyslogd 5.8.10 | OpenSuSE 42.2 | rsyslog 8.4.0-3 |
| CentOS 6.7 | rsyslogd 5.8.10 | OpenSuSE 42.3 | rsyslogd 8.24.0 |
| CentOS 6.8 | rsyslogd 5.8.10 | Ubuntu 11.04 | rsyslogd 4.6.4 |
| CentOS 7.0-1406 | rsyslog 7.4.7-6 | Ubuntu 11.10 | rsyslogd 5.8.1 |
| CentOS 7.1-1503 | rsyslog 7.4.7-7 | Ubuntu 12.04 | rsyslogd 5.8.6 |
| CentOS 7.2-1511 | rsyslog 7.4.7-12 | Ubuntu 12.10 | rsyslogd 5.8.6 |
| CentOS 7.3-1611 | rsyslog 7.4.7-16 | Ubuntu 13.04 | rsyslogd 5.8.11 |
| CentOS 7.4-1708 | rsyslog 8.24.0 | Ubuntu 13.10 | rsyslogd 5.8.11 |
| Mint 11 | rsyslogd 4.6.4 | Ubuntu 14.04 | rsyslog 7.4.4 |
| Mint 12 | rsyslogd 5.8.11 | Ubuntu 14.10 | rsyslog 7.4.4 |
| Mint 13 | rsyslogd 5.8.6 | Ubuntu 15.04 | rsyslog 7.4.4 |
| Mint 14 | rsyslogd 5.8.6 | Ubuntu 15.10 | rsyslog 8.12 |
| Mint 15 | rsyslogd 5.8.11 | Ubuntu 16.04 | rsyslog 8.16 |
| Mint 16 | rsyslogd 5.8.11 | Ubuntu 16.10 | rsyslog 8.16 |
| Mint 17 | rsyslog 7.4.4 | Ubuntu 17.04 | rsyslog 8.16 |
| Mint 17.1 | rsyslog 7.4.4 | Ubuntu 17.10 | rsyslog 8.16 |
| Mint 17.2 | rsyslog 7.4.4 |  |  |

Exercises

1. Run the Firefox XCS Code Execution attack against an Ubuntu 12.04 x64 system. Escalate privileges to root using CVE-2013-2094. Show that the exploit leaves no trace in either /var/log/syslog or /var/log/auth.log.
2. Use tail with the -f option to follow Linux logs continuously.
3. Configure a Linux logging server. Read <http://www.rsyslog.com/article60/> and configure the server to create separate log files for each sending host.
4. A Linux administrator can modify the Bash configuration file to modify the command prompt so that whenever a prompt is issued, the history file is checked and the most recently executed command is logged using the logger command. Do so.
5. Write a PowerShell script to search the security logs to find all instances where a member was added to a security-enabled global group.
6. Exploit a Windows system, escalating privileges to SYSTEM. Run the clearev command from within Meterpreter to clear the Application, Security, and System logs on the target.
7. Use the PowerShell cmdlet Write-EventLog to generate a custom log entry. Can it be used to add entries to the security log? Can it be used to spoof log entries?
8. Print out the last 5 entries from the Windows security log in plain text with the command

C:\Windows\system32>wevtutil qe Security /c:5 /f:Text

1. Windows log subscriptions use HTTP on TCP/5985. Run a Wireshark packet capture, collecting the HTTP traffic between the hosts. Can the log data be extracted from the packets? What about the authentication credentials?
2. Group policy can be used to run scripts when a user logs on. Write a script to check to see if Sysmon is installed on the system. If it is installed the script should update the configuration file. If it is not installed, then the script should install Sysmon with a specified configuration file.