Release Notes for Open-AudIT v1.8.4

Released 2015-11-11

Open-AudIT 1.8.4 is mostly a bug fix release with a major item resolved - Windows 2012R2 now works with Scheduled Tasks in Open-AudIT Enterprise. Yay! We also resolved a bug whereby every SNMP audit would create new network cards and ip addresses, regardless of what was in the database.

I'd suggest you go to menu -> Admin -> Database -> Database maintenance and clean out anything you don't need.

Open-AudIT Enterprise - Improve - Add minutes to Task Schedule.

Open-AudIT Enterprise - Improve - Added minutes field to task bulk upload .csv file.

Open-AudIT Enterprise - Bug - Fixed broken JSON output for OAE Map.

Open-AudIT Enterprise - Improve - Moved modules menu over to the right side in the menubar.

Open-AudIT Enterprise - Improve - Remove 'at' and replace with 'schtasks' for all task activity on Windows. Windows 2012R2 should now work with Scheduled Tasks in Open-AudIT.

Open-AudIT - New - when running Discovery with debug, the output is no longer buffered and prints to the screen ASAP. Make sure you wait for the page to complete rendering before proceeding (as indicated by your browser).

Open-AudIT - New - Added support for submitting linux audit results using CURL if WGET is not installed.

Open-AudIT - Improve - Revised SQL statements when processing audit results to hopefully make processing a bit faster. Removed the join between the sub-table and the system table where possible.

Open-AudIT - Improve - Added user account add/delete alerts.

Open-AudIT - Improve - Added more details for Linux daemons (services in the GUI).

Open-AudIT - Improve - When discovering a device and SSH is open and we have SSH credentials, test supplied, device specific and default credentials and store.

Open-AudIT - Improve - When discovering a device and SSH is open and we have SSH credentials, retrieve the UUID, hostname and domain to enable matching an existing device in the DB.

Open-AudIT - Improve - When discovering a device and WMI is open and we have WMI credentials, test supplied, device specific and default credentials and store.

Open-AudIT - Improve - When discovering a device and WMI is open and we have WMI credentials, retrieve the UUID, hostname and domain to enable matching an existing device in the DB.

Open-AudIT - Bug - Fixed the audit subnet (Windows) script so results are submitted sequentially. Provided an option called 'sequential' that is enabled by default. See Discovery patch for 1.8.2 (Windows) for more information.

Open-AudIT - New - Provide a config option called 'discovery_ip_exclude' that holds a (space separated) list of ip addresses that we exclude from discovery processing.

Open-AudIT - Bug - Fix duplicate network cards being created and alerts being generated.

Open-AudIT - Improve - Added code to not match when mac address is all 0's.

Open-AudIT - Improve - Remove description from discovery result if SSH or WMI or SNMP working. If SNMP is working, it sets the description, the others do not remove this.

Open-AudIT - New - Added support for RedBack routers in SNMP.

Open-AudIT - Improve - If we can connect using IPMI, SSH or WMI, remove the Nmap provided description.

Open-AudIT - improve - In audit_linux.sh, added flag to self delete script.

Open-AudIT - improve - Revised code in discovery controller. Added functions for SSH, SCP and WMIC. More revision to come, but this is the start of making discovery more modular and reusable.

Open-AudIT - Improve - XML definition improvement for UnClassed Systems report.

Open-AudIT - improve - Report SQL improvement for Duplicate UUID report.

Open-AudIT - Improve - Removed the 'type' from discover subnet scripts as Nmap is just guessing.

Open-AudIT - Improve - When we attempt to find a matching IP, we don't always have a subnet attribute. Allow for missing or 0.0.0.0 subnet value.

Open-AudIT - Improve - Added Windows 10 for an os_family in audit_windows.

Open-AudIT - improve - Patched CodeIgniter escaping form input and breaking when passing to password command line arguments.