NCIS - Bug #9785

FBI blocking fails if IP has two non-terminated MAC end hosts in NCIS.

08/04/2015 02:06 PM - Michael Zalokar

Status:	New	**Start date:**	08/04/2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

It should never happen in practice, but under rare circumstances it is possible for NCIS to have two non-terminated end hosts for one IP address and two MAC addresses.

Case #1) An ARP record is bouncing between two MACs for one IP from a misconfigured system.
Case #2) Two different systems (with their own MAC addresses) are (trying) to use the same IP address.

The current blocking code only assumes that one and only one non-terminated end host can be found and tracebacks if multiple end host records are found.

History

#1 - 08/04/2015 02:14 PM - Michael Zalokar

Comments about the problem put into the code:

~~bash-4.1$ cvs commit tissue_core/RELEASE_NOTES tissue_core/TissueCoreImpl/BlockImpl.py tissue_core/TissueCoreImpl/EventImpl.py tissue_core/TissueEvent/DetectedData.py~~
~~Checking in tissue_core/RELEASE_NOTES;~~
~~/cvs/cd/tissue/tissue_core/RELEASE_NOTES,v <~~ RELEASE_NOTES
new revision: 1.107; previous revision: 1.106
done
Checking in tissue_core/TissueCoreImpl/BlockImpl.py;
/cvs/cd/tissue/tissue_core/TissueCoreImpl/BlockImpl.py,v <-- BlockImpl.py
new revision: 1.41; previous revision: 1.40
done
Checking in tissue_core/TissueCoreImpl/EventImpl.py;
/cvs/cd/tissue/tissue_core/TissueCoreImpl/EventImpl.py,v <-- EventImpl.py
new revision: 1.38; previous revision: 1.37
done
Checking in tissue_core/TissueEvent/DetectedData.py;
/cvs/cd/tissue/tissue_core/TissueEvent/DetectedData.py,v <-- DetectedData.py
new revision: 1.24; previous revision: 1.23
done

~~bash-4.1$ cvs commit ncis_hw_factory/NcisHwFactory/HwFactory.py~~
~~Checking in ncis_hw_factory/NcisHwFactory/HwFactory.py;~~
~~/cvs/cd/ncis/ncis_hw_factory/NcisHwFactory/HwFactory.py,v <~~ HwFactory.py
new revision: 1.23; previous revision: 1.22
done

Files

ncis_error_email.txt	2.95 KB	08/04/2015	Michael Zalokar