PRAEDA

The embedded device data Harvesting tool for the masses

Deral Heiland
deral_heiland@rapid7.com
@Percent_x
Praeda

- Praeda (Latin for *plunder, booty, spoils of war*)
- Command line tool
- Current Praeda version (Written in Perl)
- Embedded device information harvesting tool
  - Enumerate 100+ devices/models
    - Multifunction printers, UPSs, Modems, IP Cameras, NAS,
Praeda Install Linux

- git clone git://github.com/percx/Praeda.git

- Cpan Perl modules:
  - cpan -i LWP::Simple LWP::UserAgent HTML::TagParser URI::Fetch HTTP::Cookies IO::Socket HTML::TableExtract Getopt::Std Net::SSL Net::SNMP NetAddr::IP
Praeda Install Win7

- Install perl
  - http://www.activestate.com

- Git = Git clone git://github.com/percx/Praeda.git

- Zip = https://github.com/percx/Praeda/archive/master.zip

- Cpan Perl modules:
  - sudo cpan -i LWP::Simple LWP::UserAgent HTML::TagParser URI::Fetch HTTP::Cookies IO::Socket HTML::TableExtract Getopt::Std Net::SNMP NetAddr::IP
  - http://www.sisyphusion.tk/ppm/Net-SSLeay.ppd

- Change line 47 in praeda.pl from “use Net::SSL; to use Net::SSLeay;
Praeda Install OSX

- Git clone git://github.com/percx/Praeda.git

- Cpan Perl modules:
  - `sudo cpan -i LWP::Simple LWP::UserAgent HTML::TagParser URI::Fetch HTTP::Cookies IO::Socket HTML::TableExtract Getopt::Std Net::SSL Net::SNMP NetAddr::IP`
  - If after install you have issue with Praeda.pl not running saying a module is missing most likely cause is:
    - multiple version of perl installed
    - path order is messed up
    - Determine version that is being used and install all modules to that version
      - Sample "sudo perl5.16 -MCPAN -e 'install Net::SNMP'"
Praeda

Diagram:

- Import DataFile
- Scan Target List
- Compare target reply with Datafile info and call associated module job

DataFile:
- Database file of all devices and associated job modules

Target List:
- IP List
  - XXX.XXX.XXX.XXX

Modules:
- Empty boxes for modules to process the data.
Praeda

How it works:

- Scan network for embedded systems
- Fingerprint embedded systems
- Run Praeda modules based on fingerprint
- Gather data and log it
How we use it:

- One of the first tools we run on an assessment
- Use data harvested to gain foothold in environment
- Success rate is pretty darn good.
  - 40-50% in harvesting Valid active directory credentials
Praeda

- Demo
  - Functions
  - Examine output data
Question?

Deral Heiland
Deral_heiland@rapid7.com
Twitter: @Percent_X

https://github.com/MooseDojo/praedaspoit
https://github.com/percx/Praeda
END OF THE WORLD AS WE KNOW IT