Create a Security Profile Using New Wireshark Features
Laura Chappell
Founder, Wireshark University
Founder, Chappell University

What is a “Security Profile”?
A customized Wireshark configuration built to identify unusual traffic.

RECONS
probandoprobandomoz
.Bot DNS query response styles
.exe/zip/jar
.attachments
.Unusual HTTP response codes
.MZ...This program cannot be run in DYN mode
.Browsing to China/Russia

Visit www.wiresharkbook.com for pcapng trace files and more
Security Profile Elements

- Protocol preference settings
- Coloring rules
- Display filters
- Filter expression buttons

Basic 4-Step Process

1. Create a new profile
2. Add your “suspect traffic” coloring rules (use a name/color convention)
3. Create Filter Expressions to display sets of traffic based on their group name
4. When you open trace files, click the Filter Expression to view the desired traffic
COLOR Coding is Key

- Coloring Rules – what color palette shall you use to identify…
  - Recons [WHITE on dark orange (#FF4F00)]
  - Known breaches [WHITE on dark orange (#FF4F00)]
  - Hits to suspect websites [WHITE on dark orange (#FF4F00)]
  - Uploads/downloads of .exe files [WHITE on dark red]
  - Errors “of concern” [BLACK on orange]
  - Tools in use [BLACK on #FF4FFF]
  - Just notes to yourself [WHITE on dark green]

A Note to the Developers…

- Filter Expressions saved in a separate file (not in preferences) – easier to share/distribute without sending too much unnecessary stuff
- More color names known – possible to define color names in a table and pull from a drop down?
- Fix the custom column display problem (column for coloring rule name not applying properly – custom column problem?)
Proper Naming is a MUST

- Naming Rules – what preceding pattern will help filter out packets that match a certain coloring rule?
  - Recons
  - Known breaches
  - Hits to suspect websites
  - Errors “of concern” (S- other errors are T-)
  - Uploads/downloads of .exe files
  - Tools in use
  - Just notes to yourself

Let’s Build a New Security Profile

- Select Edit | Configuration Profile or right-click on the Profile column on the Status Bar
Get Your Regex On!

- $ end of line
- ^ beginning of line
- (?i) case insensitive
- . any character (except newline \n)
- \ escape out special characters

Example:
frame matches “(?i)probando”

ASKTOOLBAR.DLL MALWARE

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET MALWARE ASKTOOLBAR.DLL Reporting";
flow:established,to_server; content:"GET"; nocase;
http_method; content:"/toolbarv/askBarCfg?"; nocase;
http_uri; content:"v="; nocase; http_uri; content:"e=";
http_uri; nocase;

Visit www.wiresharkbook.com for pcapng trace files and more
Let’s Add Some Color -

- Illegal ICMP Echo Requests (tool detection)
- LOIC (by Anonymous)
- Questionable ICMP Types 13, 15, 17
- HTTP GET Requests for .exe or .zip files
- Connecting to a .ru or .cn HTTP server
- Duplicate IP Addresses Detected

Finally - the Core Filter Expression Buttons!

\[\text{frame.coloring\_rule\_name matches "^S-"}\]
All packets that match any security coloring rule names

\[\text{frame.coloring\_rule\_name matches "^T-"}\]
All packets that match any troubleshooting coloring rule names

\[\text{frame.coloring\_rule\_name matches "^ST-"}\]
All packets that match any tool detection coloring rule names

\[\text{frame.coloring\_rule\_name matches "^N-"}\]
All packets that match the notes coloring rule names
 Bonus…

- **Infected Host?**
  - `http.accept_language == "ru" ||
  - `http.accept_language == "zh-cn"`