Network Traffic Exploration Application

Presented By Grant Vandenberghe
Grant.Vandenberghe@drdc-rddc.gc.ca
(613) 991-6464
Introducing the NTE

The Network Traffic Exploration (NTE) application allows the user to explore network traces and prototype new detection algorithms.

The NTE is useful for security analysts because of its varied and flexible presentation capabilities.
The NTE is a MATLAB application has been developed on top of an open library of packet analysis functions.
Loading and Viewing Packets

One or more traces can be loaded into the NTE and the packets can be selectively viewed.

The user can explore the data from both a packet, session or host-to-host perspective.

Packet Plot (SYNK4 DOS tool)
(The fixed TCP Sequence number can be used to create a firewall filter rule)

Session plot (W32.Gobot.1)
(Netbios traffic should not appear on parallel channels)
Evaluating A Situation

The NTE includes functions to help determine if a set of packets are “suspicous”. Among these are:

- Heuristic Analysis
- Statistical Analysis
- Signature-Based
Automating Analysis and Recording An Investigation

Some events are true while others are false alarms.

The NTE has the ability to create a script on the fly to detect an attack or filter a false alarm.

The script’s capability can be used to log the steps taken in performing an investigation.

```matlab
% Load the the PCAP trace array
% [PKT_DATA,IP_OPT,TCP_OPT,PAYLOAD]=load_pcap_file_plus_ev('C:\DATA \good_bad_2.dmp','....
  'TRACE_NUMBER','','BPF','ip');
% Assign session id numbers and host-2-host id numbers to the trace array
% PKT_IDX=assign_session_number(PKT_DATA,PAYLOAD);
% Create the host to host array
% [H2H_SUM,H2H_LIST]=create_h2h_array(PKT_DATA,PKT_IDX);
% Print a summary of the host to host connections
% [the filter embedded this is the print function also detects the HTTP tunnel].
% [SSN_NUM,H2H_NUM]=print_host_to_host_details(H2H_SUM,H2H_LIST,'ALL',5,...
  'TTL_PKTS=1&SERV_PORT=80&PROTOCOL=6');
% Convert host to host connections back to packets
% [PKT_REF_NUM]=find_pkt_from_h2h(PKT_IDX,H2H_NUM);
% Create SNORT alert
% [S_ALERT,S_CPAYLOAD,S_PAYLOAD]=create_snort_alert_ev(...
  PKT_DATA,PKT_REF_NUM(1),'GID',1,'SID',6969,'VER',1,'MSG', ...
  'Out of Band Covert Tunnel','PRIORITY',1);
% Store the SNORT alert
% save_snort_alert_ev('junk',S_ALERT,S_CPAYLOAD,S_PAYLOAD);
```

This out-of-band HTTP tunnel can be detected by the adjacent script.
Relating This Small Event To The Bigger Picture

Packet events and exchanges can be overlaid onto network diagrams.
DEMONSTRATION

Starting Premise

You are handed a trace containing suspicious traffic.
Starting the NTE
Load Packets Associated with Alert
Assign Session Number To Each Packet In Trace

Summarize each session using 90 different statistical measurements

Summarize The Session Information Exchange
View Summary Of Trace Session Activity
Plot Session Activity

Note the silence is broken in one direction.
Steps Not Shown

Convert Session #1 Into A List of Packets

View Packet In Wireshark

Wireshark cannot decode the protocol

Payload Type Analysis

Payload is binary but not random

Isolate All Packets In Session #1 Running From Client To Server
Plot Payload Bytes Based On Machine Language Opcodes

- **Network Traffic Exploration Tool v3.0**
  - Options: Load Trace, Assign Ser #, Print Packet, Save Trace, Create Short Alert

- **REPORT TYPES**

- **REPORT OPTIONS**

- **PLOT DISASSEMBLY CODE**
  - Input Trace/Payload (Req)
  - Input Payload (Req)
  - Packet Range (Req)
  - Start Byte (Req)

- **Figure 1**
  - Opcode value
  - Opcode Length
  - NOP sled
  - Taxonomy of OpCodes
Search For English Strings In Packets

Meterpreter is part of Metasploit

Banner for windows command shell
The attack session deviates significantly from the norm (in 37 different out of 90 tests)
Closing Remarks

Key benefits of NTE

- Flexible analysis of security events and network based attacks
- Broad range of features (300)
- Scripting capability

For more information about the tool you can contact.

Grant.Vandenberghe@drdc-rddc.gc.ca