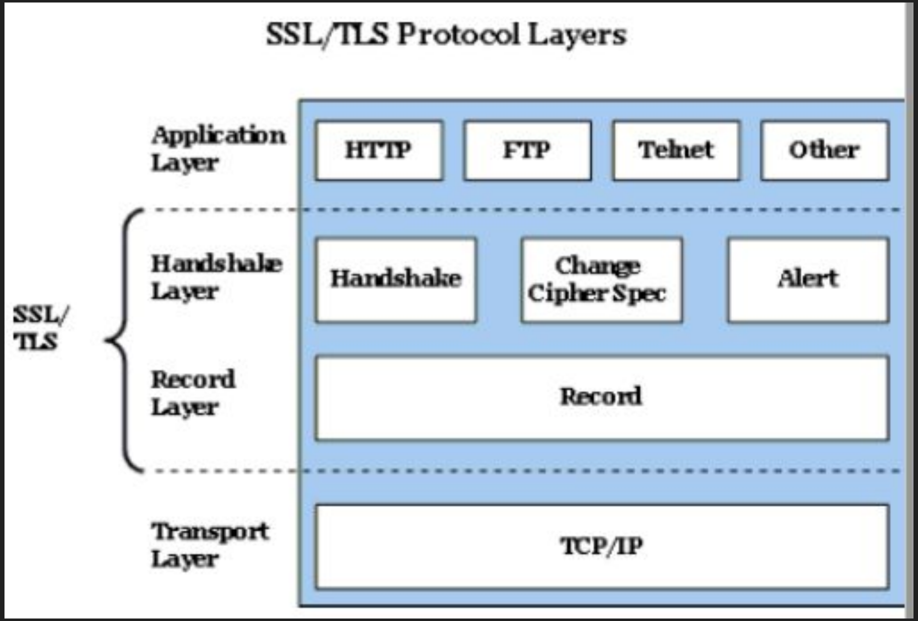
HTTP/HTTPS & Intrusion Detection System (IDS)

Ankur Chowdhary
DevilSec

SSL Protocol

Handshake Protocol: negotiation of security algorithms, server, and optionally client authentication.

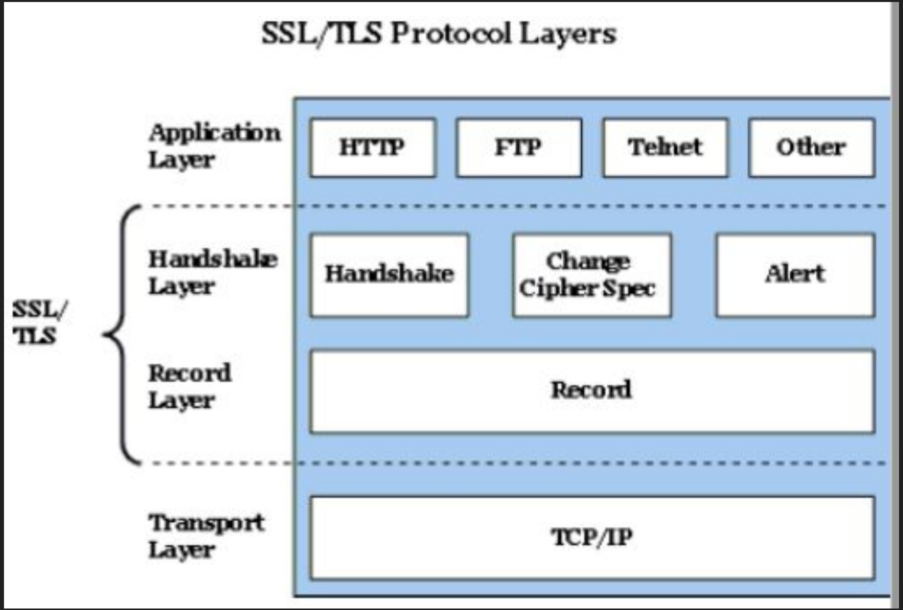
Record Protocol: fragmentation, compression, encryption. Using secret key to provide authentication and integrity protection.



SSL Protocol

Handshake Protocol: Fatal errors and warnings.

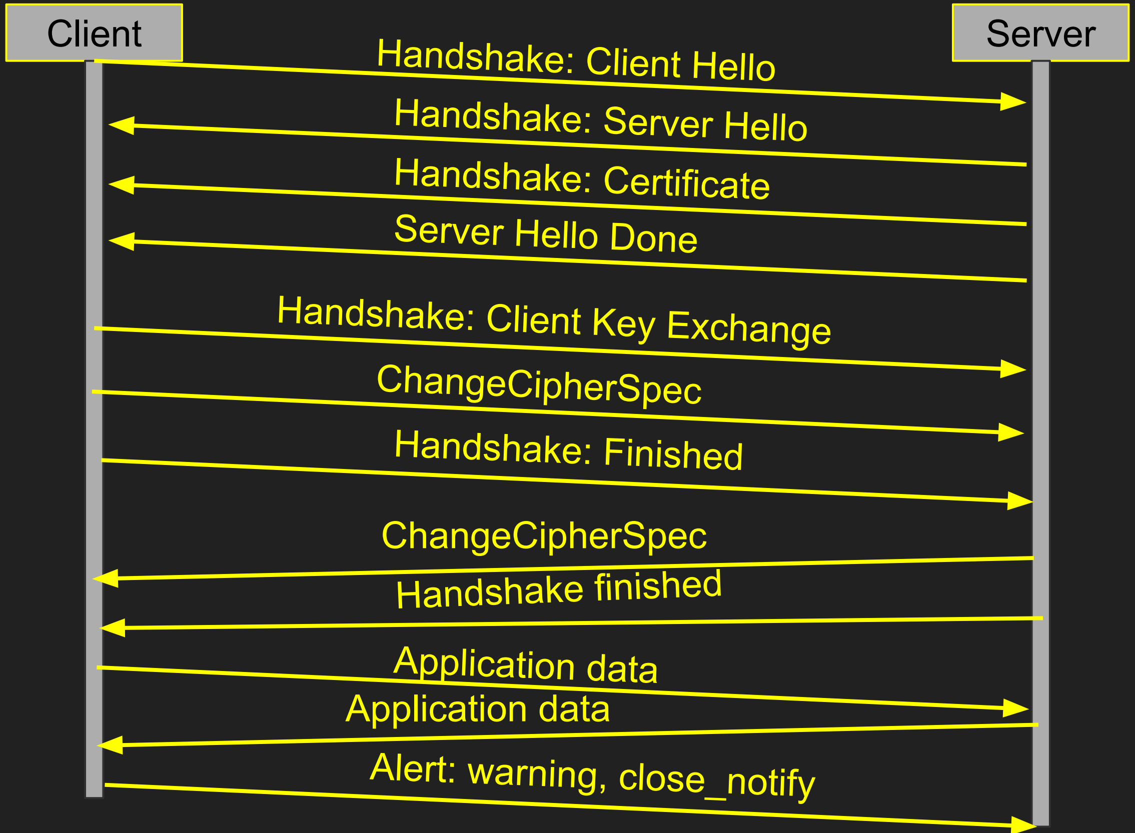
Change Cipher Spec: Single message that indicates the end of SSL handshake.



SSL Packages

- SSL protocol handles encrypted communication and mutual authentication between browsers and Web server.
- apache: contains httpd daemon and related utilities
- mod_ssl: includes mod_ssl module, which provides strong cryptography for Apache Web server via the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocol.
- openssl: contains OpenSSL toolkit. Implements SSL and TLS protocols and also includes a general purpose cryptographic library.
- Certificate Authority (CA): provides authentication for secure Web server. Certificate can be self-signed or issued by CA.

SSL Communication



LET’S MAKE A HTTPS WEBSITE

Inject: Install and configure apache in https mode (10 pts)

Top 5 Players

Intrusion Detection System (IDS)

IDS is software, hardware or combination of both used to detect intruder activity.

Snort is an open source IDS

- It is a multi-mode packet analysis tool
- Sniffer (Passive and Active Sniffer)
- Port mirror sniffer, GW sniffer
- Packet Logger
- Data Analysis tool
- Network Intrusion Detection System

IDS Categorization

Network IDS (NIDS)

1. Listens and analyzes traffic in a network
2. Capture data package
3. Compare with database signatures (signature-based)
4. Operates in promiscuous mode

Host-based IDS (HIDS)

1. Installed as an agent on the host
2. Listens and analyzes system logs

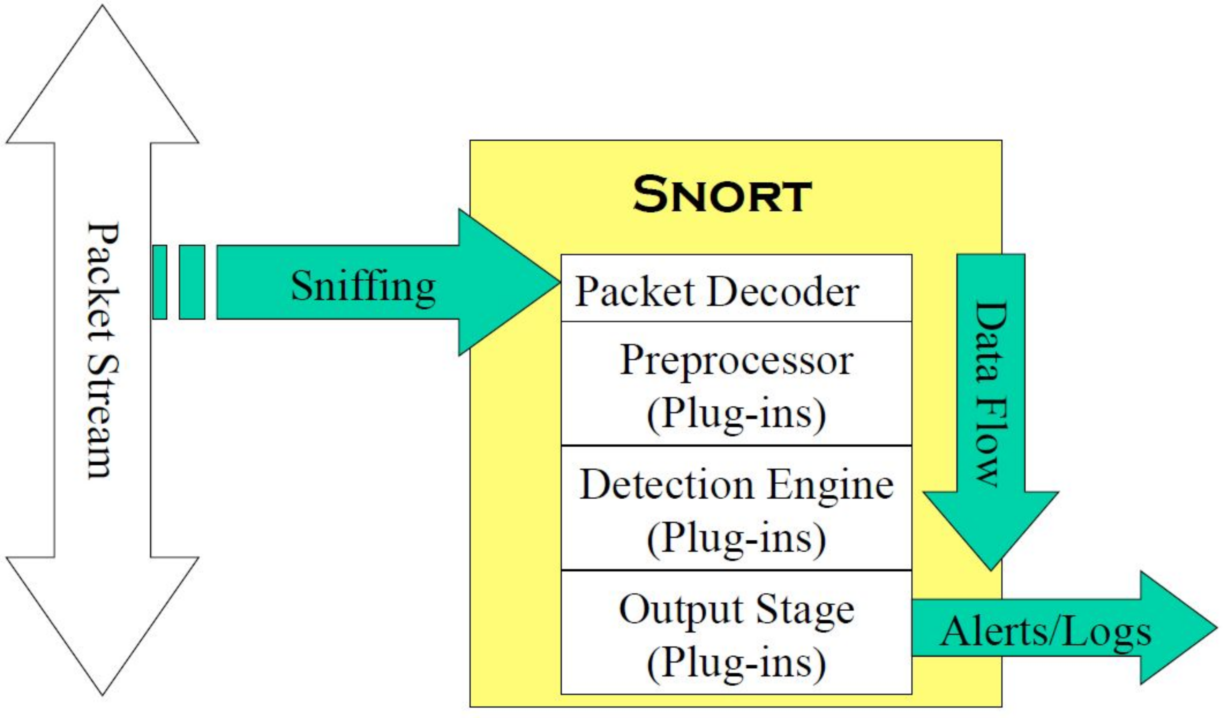
Snort Requirements

- WinPCAP - WinPcap is a packet capturing library in Windows
- Barnyard - Barnyard is an output system for Snort. Snort creates a special binary output format called **unified2**. Barnyard reads this file, and then re-sends the data to a database backend.
- Libpcap - pcap (packet capture) consists of an application. programming interface (API) for capturing network traffic.
- PCRE - regular expression C library inspired by Perl's external interface. PCRE library is incorporated into a number of prominent open-source programs such as the Apache HTTP Server, the PHP and R scripting languages, and Snort.

Snort Requirements

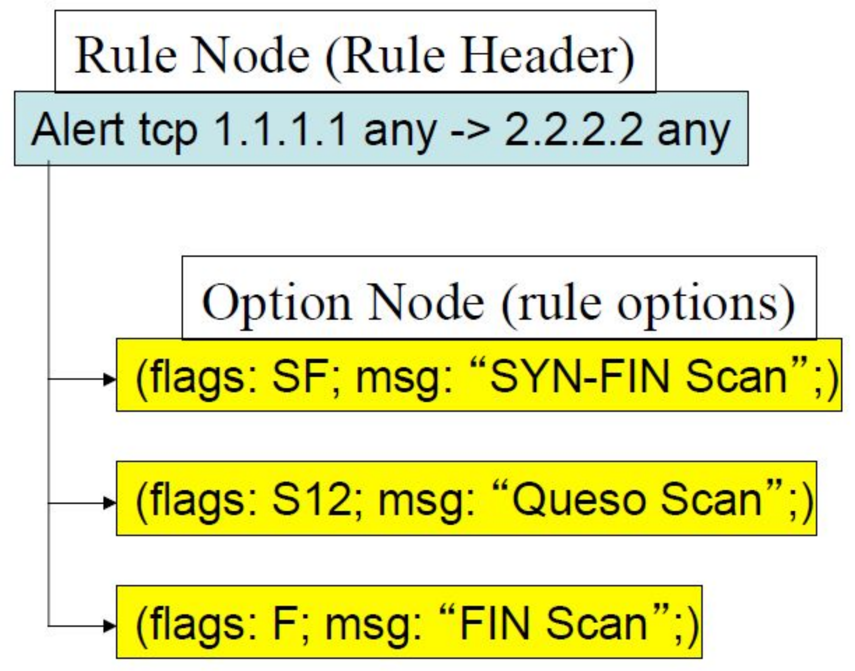
- Libdnet - Libdnet is a generic networking API that provides access to several protocols.
- DAQ - DAQ is the Data-Acquisition API that replaces direct calls into packet capture libraries like PCAP,PFPACKET, NFQ, IPFW with an abstraction layer that make it easy to add additional software or hardware packet capture implementations.
- Barnyard2 - Output process plug-ins.

Snort Data Flow



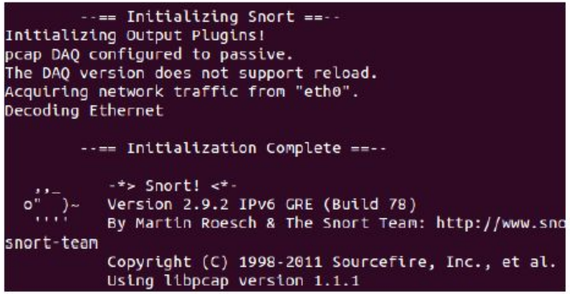
Snort Rule Sets

1. Activation: alert and turn on dynamic rule.
2. Dynamic: log the traffic when called by above activation rule.
3. Alert: generate alert and log traffic.
4. Pass: ignore traffic.
5. Log: log the traffic, don't alert.


Rule Node (Rule Header)
Alert tcp 1.1.1.1 any -> 2.2.2.2 any
Option Node (rule options)
(flags: SF; msg: “SYN-FIN Scan”;)
(flags: S12; msg: “Queso Scan”;)
(flags: F; msg: “FIN Scan”;)

Snort Related Software Packages

Snort (intrusion detection system)

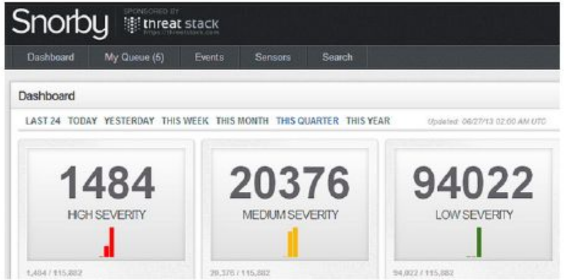


```
        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "eth0".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.2 IPv6 GRE (Build 78)
   ''''    By Martin Roesch & The Snort Team: http://www.sno
snort-team
           Copyright (C) 1998-2011 Sourcefire, Inc., et al.
           Using libpcap version 1.1.1
```

Snorby (reporting system)

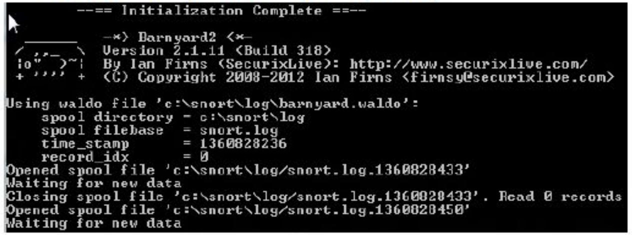


1484 HIGH SEVERITY 1,484 / 115,882

20376 MEDIUM SEVERITY 20,376 / 115,882

94022 LOW SEVERITY 94,022 / 115,882

Banyard2 (output plug-ins)

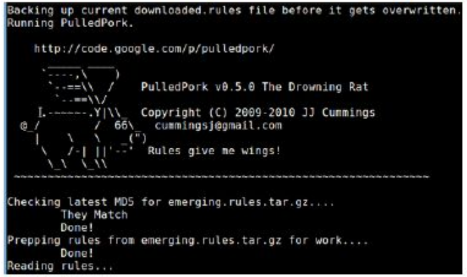


```
        --== Initialization Complete ==--

  _______    -*> Barnyard2 <*-
 / ,,_   \   Version 2.1.11 (Build 318)
 |o"  )~|    By Ian Firns (SecurixLive): http://www.securixlive.com/
 + '''' +    (C) Copyright 2008-2012 Ian Firns <firnsy@securixlive.com>

Using waldo file 'c:\snort\log\barnyard.waldo':
    spool directory = c:\snort\log
    spool filebase  = snort.log
    time_stamp      = 1360828236
    record_idx      = 0
Opened spool file 'c:\snort\log/snort.log.1360828433'
Waiting for new data
Closing spool file 'c:\snort\log/snort.log.1360828433'. Read 0 records
Opened spool file 'c:\snort\log/snort.log.1360828450'
Waiting for new data
```

PulledPork (rules management)



```
Backing up current downloaded.rules file before it gets overwritten.
Running PulledPork.

    http://code.google.com/p/pulledpork/
      _____ ____
     `----,\    )
      `--==\\  /     PulledPork v0.5.0 The Drowning Rat
       `--==\\/
     .-~~~~-.Y|\\_   Copyright (C) 2009-2010 JJ Cummings
  @_/        /  66\_   cummingsj@gmail.com
    |    \   \   _(")
     \   /-| ||'--'  Rules give me wings!
      \_\  \_\\
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Checking latest MD5 for emerging.rules.tar.gz....
        They Match
        Done!
Prepping rules from emerging.rules.tar.gz for work....
        Done!
Reading rules...
```

LET’S INSTALL AND TEST SNORT IDS

Inject: Install and configure Snort NIDS (20 pts)

Top 5 Players