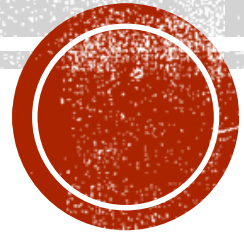
SOFTWARE DEFINED VIRTUAL NETWORKING SECURITY

CHAPTER 4 NETWORK SECURITY PRELIMINARIES



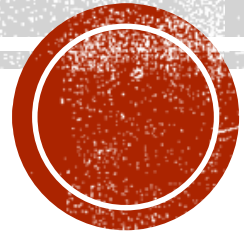
Dijiang Huang, Ankur Chowdhary, and Sandeep Pisharody

OUTLINE

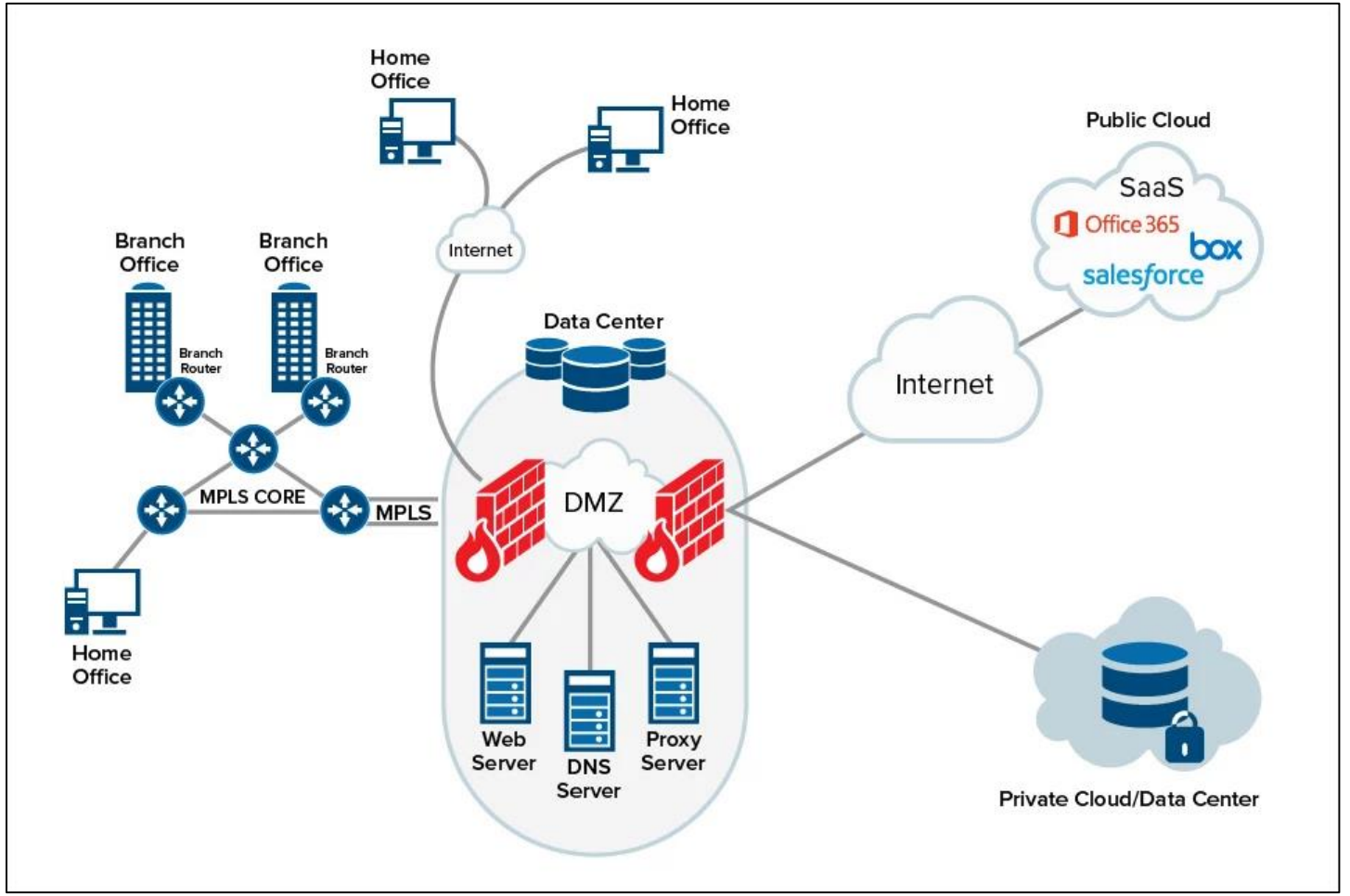
- Computer Network Security Basics
- Network Reconnaissance
- Preventive Techniques
- Detection and Monitoring
- Security Auditing, Host-based Intrusion Detection, Issues with HIDS

COMPUTER NETWORK SECURITY BASICS

Threat Vectors, SIEM, Risk and Attack, Defense-in-depth, Cyber Kill Chain



ENTERPRISE NETWORK



THREAT VECTORS

Network - Perimeter of the network usually protected by the Firewall.

User – Social Engineering and Social Networking to gather information about users, tricking them into opening pathway for attack.

Email – Phishing attempts and malicious attachments target email threat vector.

THREAT VECTORS

Web Applications – Inadequately protected web applications being targeted by SQL Injection and Cross Site Scripting (XSS) attacks.

Remote Access – A host/device trying to access secured and unauthorized segments of the network.

Mobile – Smartphones, tablets, and other mobile devices can be used for malware propagation, attacking corporate network.

SECURITY ADMIN GOALS

Identifying who might be attacking.

How the attack occurs?

Which incident patterns affect your industry more than others

Setting in Motion security policy to mitigate threats.

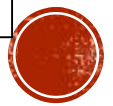
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

The product capabilities of gathering, analyzing and presenting information from network and security devices

Vulnerability management and policy-compliance tools

Operating-system, database and application logs

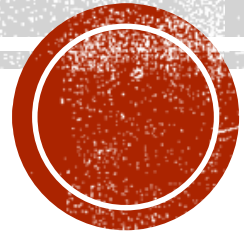
External threat data



SIEM COMPONENTS

- Data Collection – Log Management
- Dashboards – Activities and Patterns
- Alerting – Automated analysis of correlated events
- Compliance – reports adhering to government and security standards
- Retention – Correlation with historical data
- Forensic Analysis – Search over data based on different incident criteria.

NETWORK RECONNAISSANCE



Network Mapping, Port Scanning and Penetration Testing

RECONNAISSANCE TOOLS

- Nmap
- Nikto
- Zenmap
- Nessus

NMAP INSTALLATION

- $ sudo yum install nmap (Redhat/Fedora)
- $ sudo apt-get install nmap (Ubuntu/Debian)

NMAP PING SCAN

- Checking the devices on your network responding to ping scan.

```
Host is up (0.0016s latency).
MAC Address: FA:16:3E:DE:5D:82 (Unknown)
Nmap scan report for 172.16.16.6
Host is up (0.0016s latency).
MAC Address: FA:16:3E:C4:3E:E2 (Unknown)
Nmap scan report for 172.16.16.7
Host is up (0.0017s latency).
MAC Address: FA:16:3E:07:06:9D (Unknown)
Nmap scan report for 172.16.16.10
Host is up (0.0016s latency).
MAC Address: FA:16:3E:1B:46:53 (Unknown)
Nmap scan report for 172.16.16.13
Host is up (0.0051s latency).
MAC Address: FA:16:3E:26:34:E9 (Unknown)
Nmap scan report for 172.16.16.17
Host is up (0.0028s latency).
MAC Address: FA:16:3E:2F:6C:C6 (Unknown)
Nmap scan report for 172.16.16.19
Host is up (0.0016s latency).
```


NMAP TCP PORT SCANNING

- sudo nmap -p 1-65535 -sV -sS -T4 target

```
centos@host-172-16-16-11 ~]$ sudo nmap -p 1-65535 -sV -sS -T4 172.16.16.7

Starting Nmap 6.40 ( http://nmap.org ) at 2018-09-07 10:42 MST
Nmap scan report for 172.16.16.7
Host is up (0.00053s latency).
Not shown: 65525 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
MAC Address: FA:16:3E:07:06:9D (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.59 seconds
```


NMAP OS DETECTION + TRACEROUTE

- nmap -v -sS -A -T4 172.16.16.7

```
Host is up.
Nmap done: 256 IP addresses (11 hosts up) scanned in 1.80 seconds
[centos@host-172-16-16-11 ~]$
[centos@host-172-16-16-11 ~]$ sudo nmap -p 1-65535 -sV -sS -T4 172.16.16.7

Starting Nmap 6.40 ( http://nmap.org ) at 2018-09-07 10:42 MST
Nmap scan report for 172.16.16.7
Host is up (0.00053s latency).
Not shown: 65525 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
MAC Address: FA:16:3E:07:06:9D (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

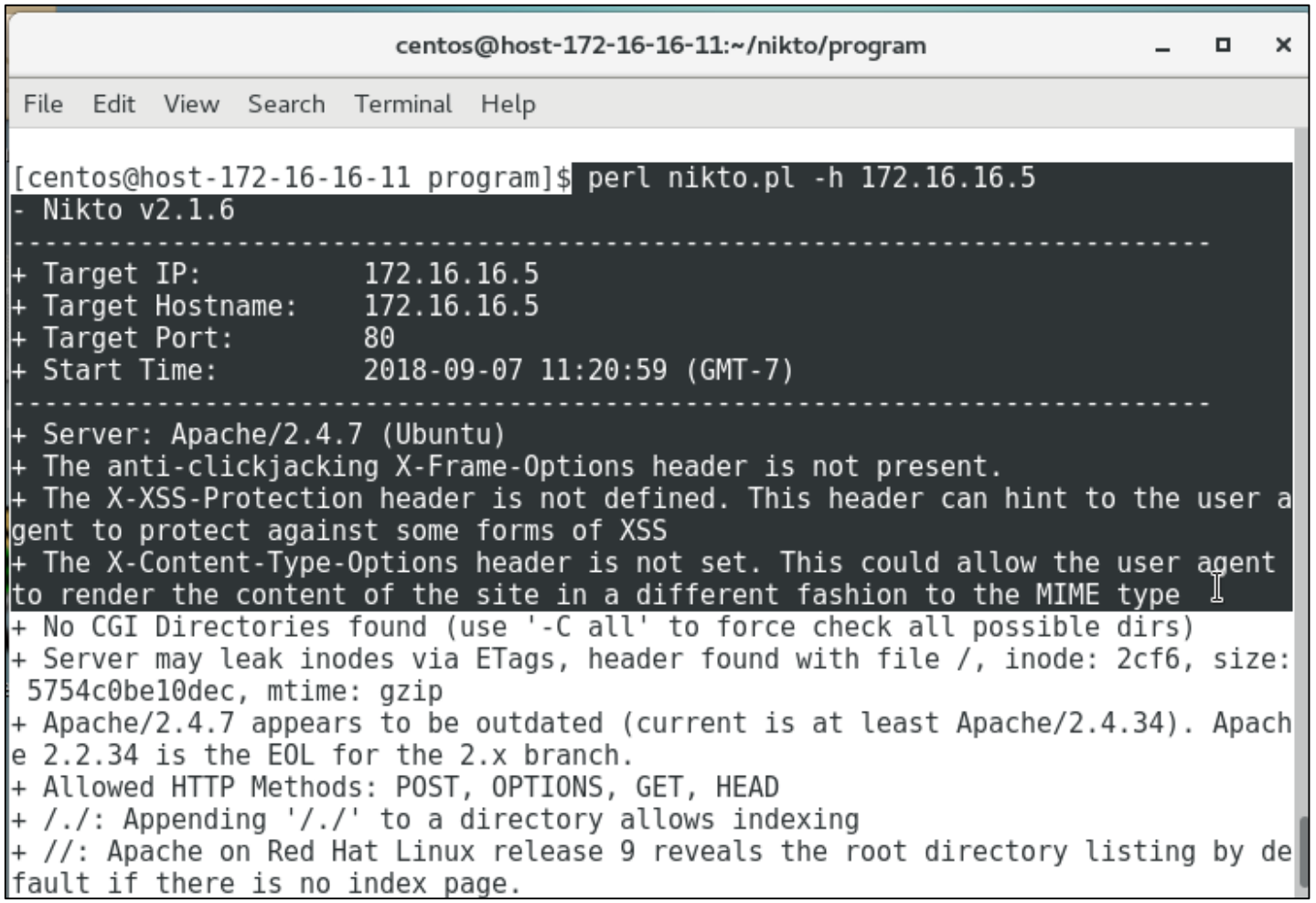

NIKTO

- Web application and CGI scanner
- $ sudo yum install git perl perl-Net-SSLeay openssl
- $ sudo git clone https://github.com/sullo/nikto.git
- $ cd nikto/program
- $ perl nikto.pl -h

NIKTO

```
[centos@host-172-16-16-11 program]$ ls
databases  docs  nikto.conf  nikto.pl  plugins  replay.pl  templates
[centos@host-172-16-16-11 program]$ perl nikto.pl -h
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:p
ass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /direct
ory
```


NIKTO


centos@host-172-16-16-11:~/nikto/program
File Edit View Search Terminal Help
[centos@host-172-16-16-11 program]$ perl nikto.pl -h 172.16.16.5
- Nikto v2.1.6

+ Target IP: 172.16.16.5
+ Target Hostname: 172.16.16.5
+ Target Port: 80
+ Start Time: 2018-09-07 11:20:59 (GMT-7)

+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent
to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2cf6, size:
5754c0be10dec, mtime: gzip
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.34). Apach
e 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ /./: Appending '/./' to a directory allows indexing
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by de
fault if there is no index page.

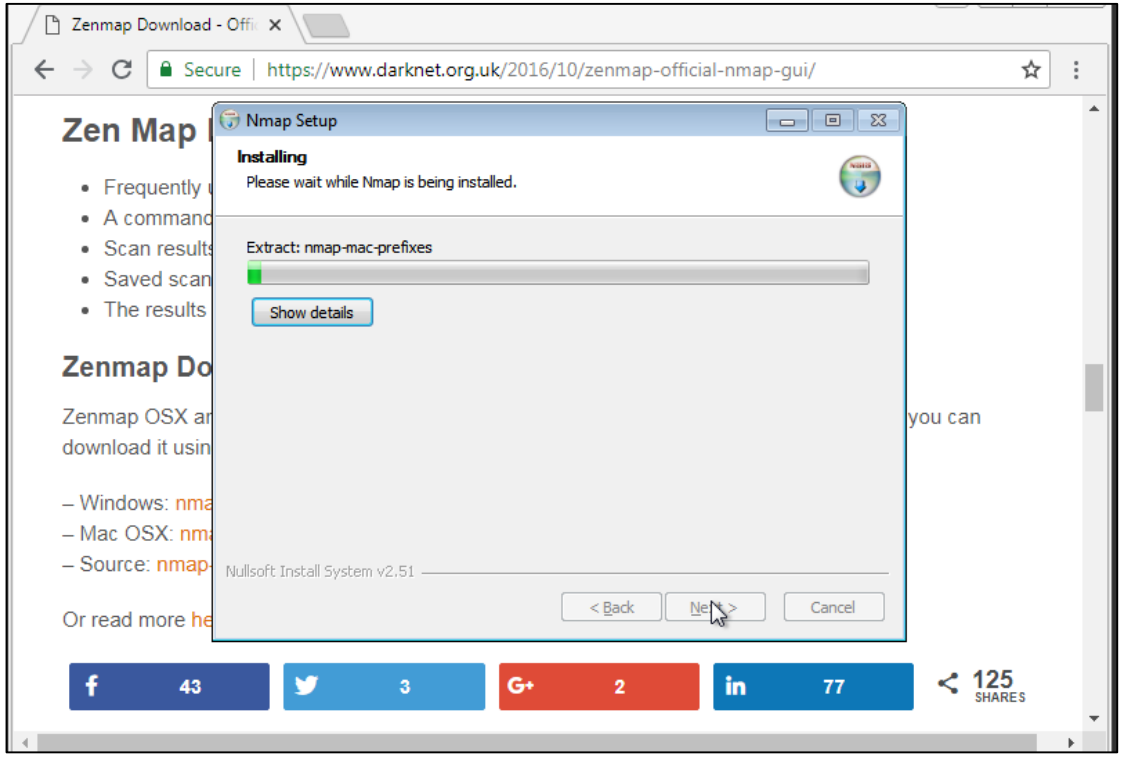
NIKTO SCANNING A WEBSITE

- Scanning a vulnerable website

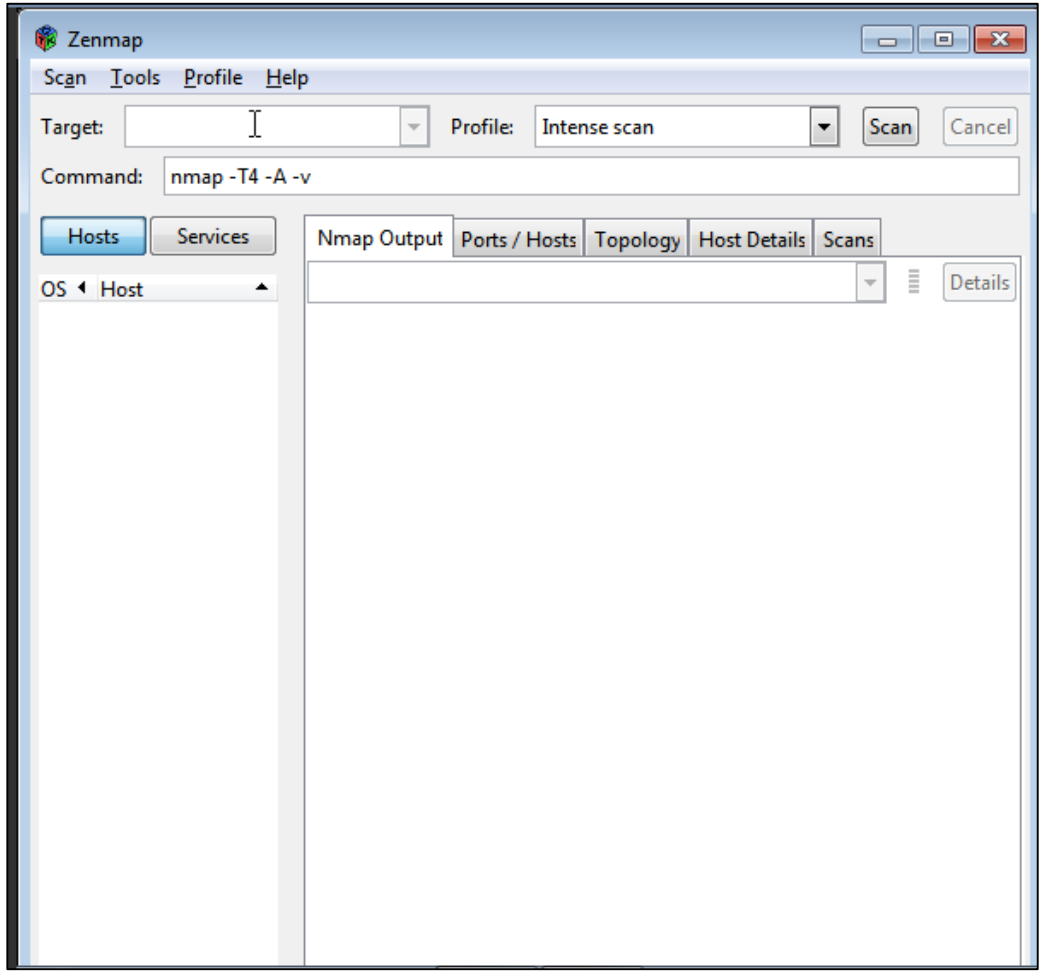
```
[centos@host-172-16-16-11 program]$ perl nikto.pl -h  https://www.thothlab.com
- Nikto v2.1.6
---------------------------------------------------------------------------
- Target IP:          206.207.50.38
- Target Hostname:    www.thothlab.com
- Target Port:        443
---------------------------------------------------------------------------
- SSL Info:        Subject:  /OU=Domain Control Validated/OU=EssentialSSL Wildca
rd/CN=*.thothlab.com
                   Altnames: *.thothlab.com, thothlab.com
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA L
imited/CN=COMODO RSA Domain Validation Secure Server CA
- Start Time:         2018-09-07 11:25:25 (GMT-7)
---------------------------------------------------------------------------
- Server: No banner retrieved
- The anti-clickjacking X-Frame-Options header is not present.
- The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
- The site uses SSL and the Strict-Transport-Security HTTP header is not defined

- The site uses SSL and Expect-CT header is not present.
```


ZENMAP

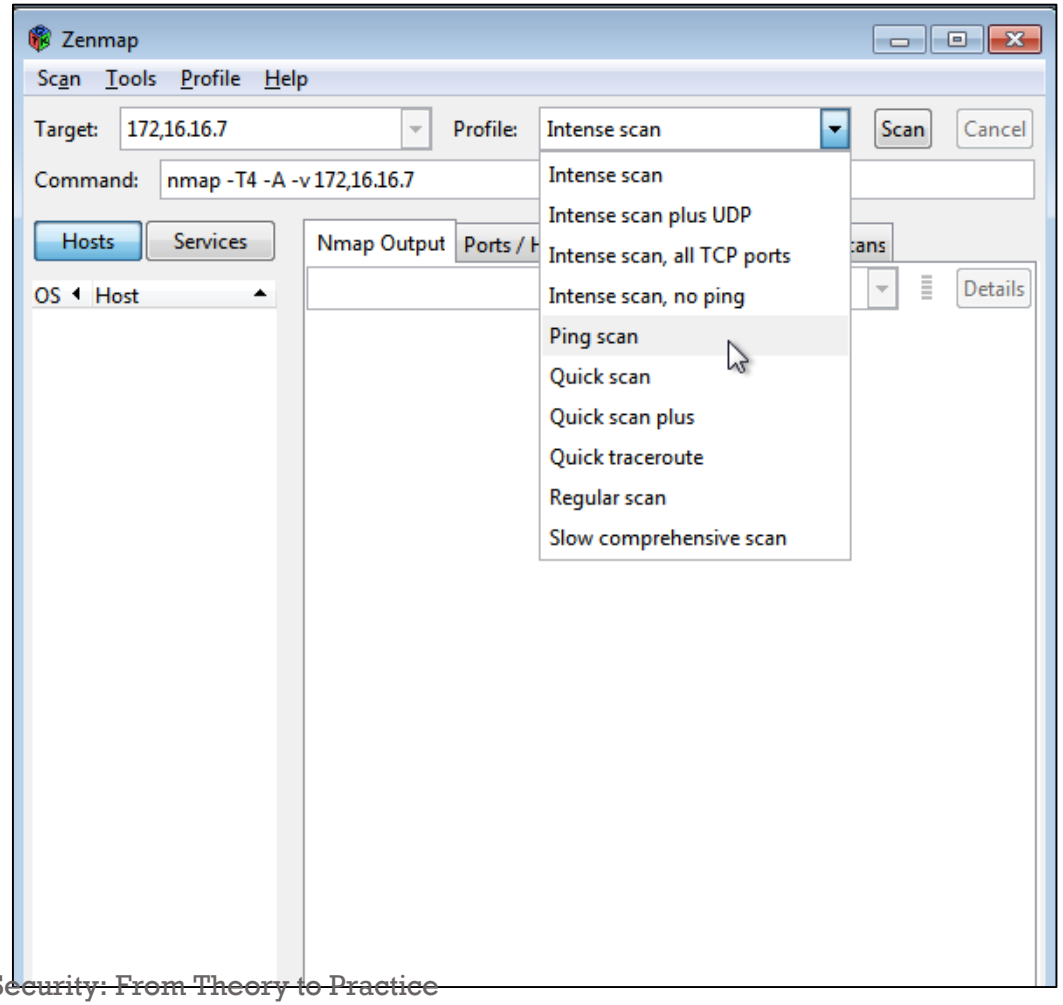
- Download and install, set up will ask for installation of WinPCAP, so make sure you allow permission to install WinPCAP.



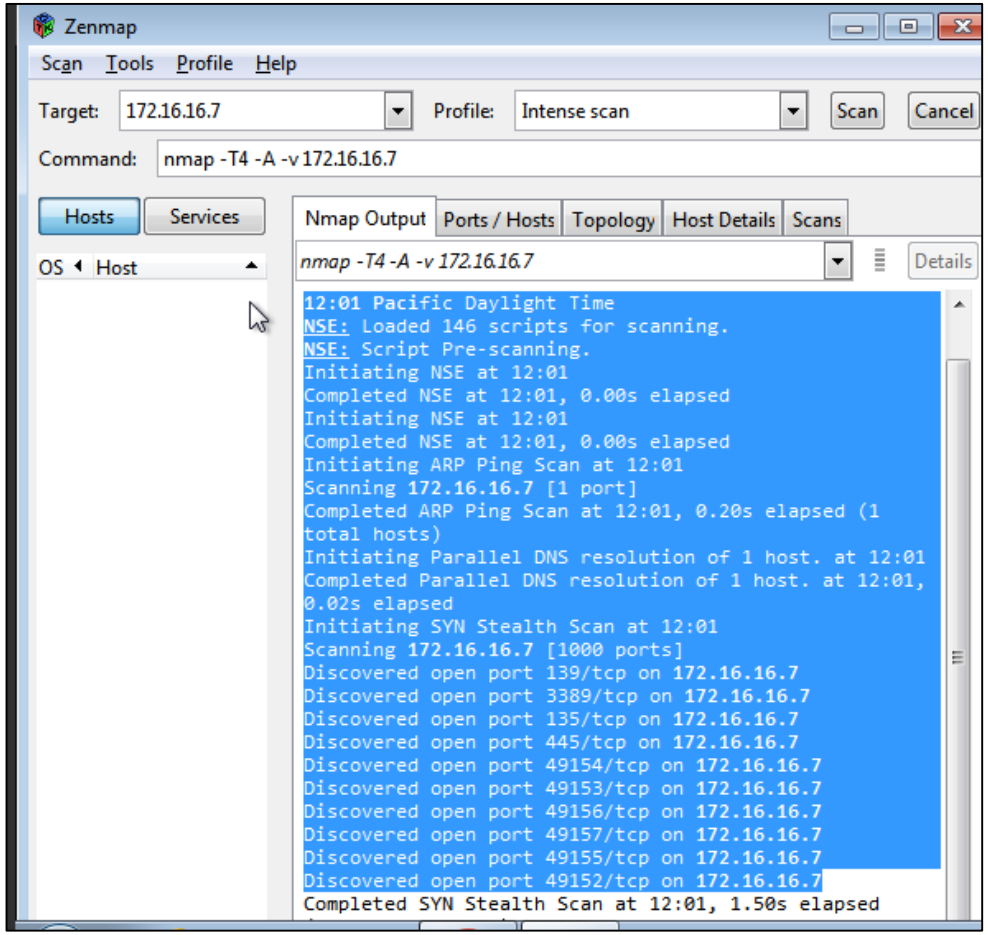
ZENMAP GUI


Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details

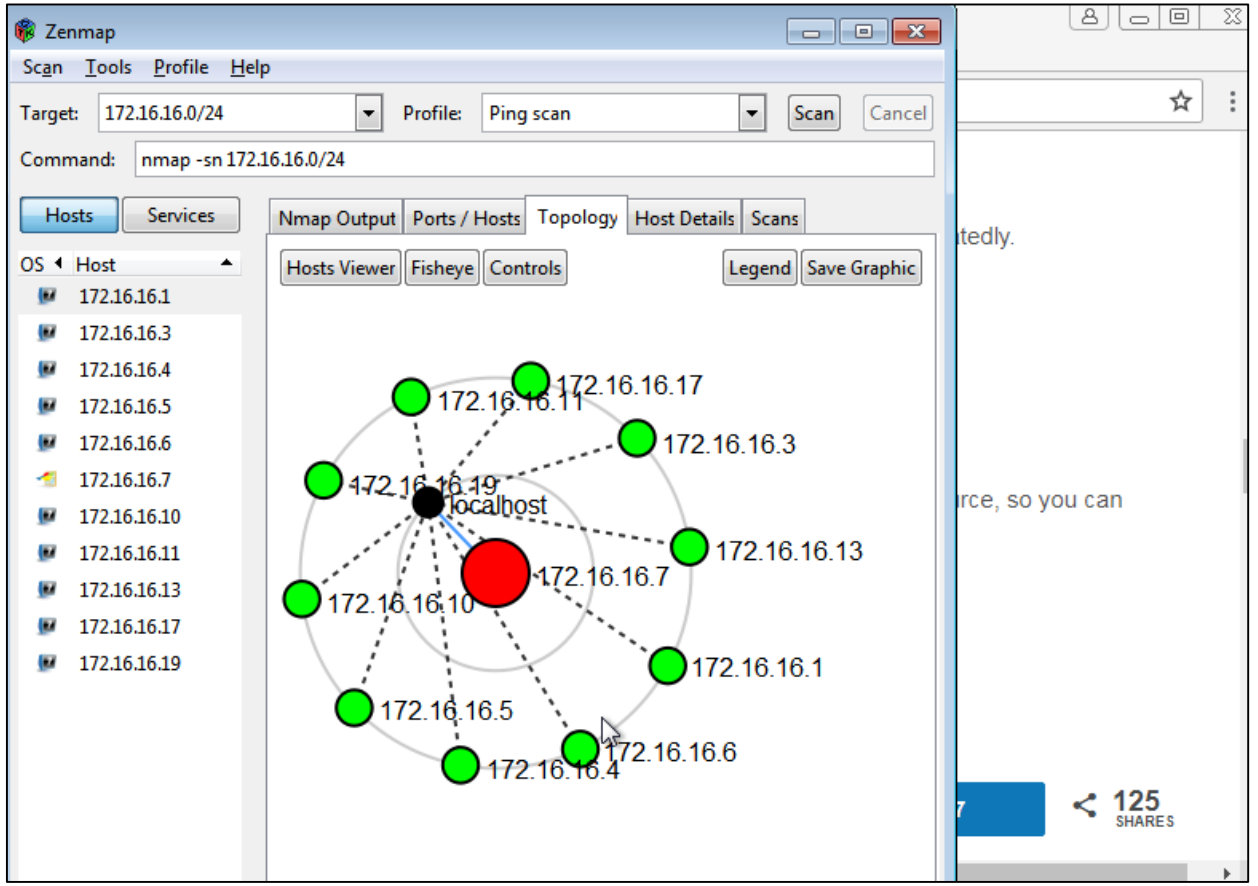
ZENMAP SCANNING



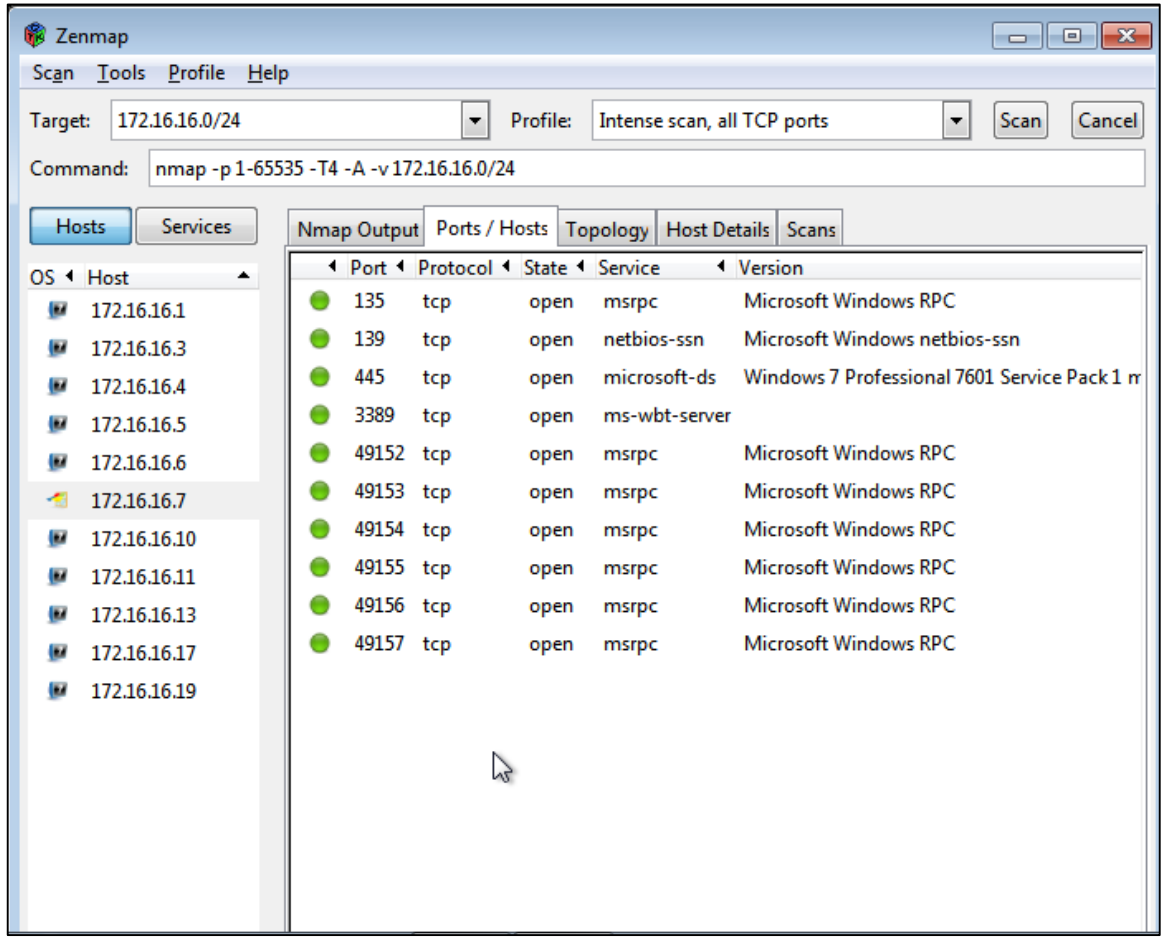
ZENMAP SCANNING



ZENMAP PING SCAN AND TOPOLOGY VISUALIZATION



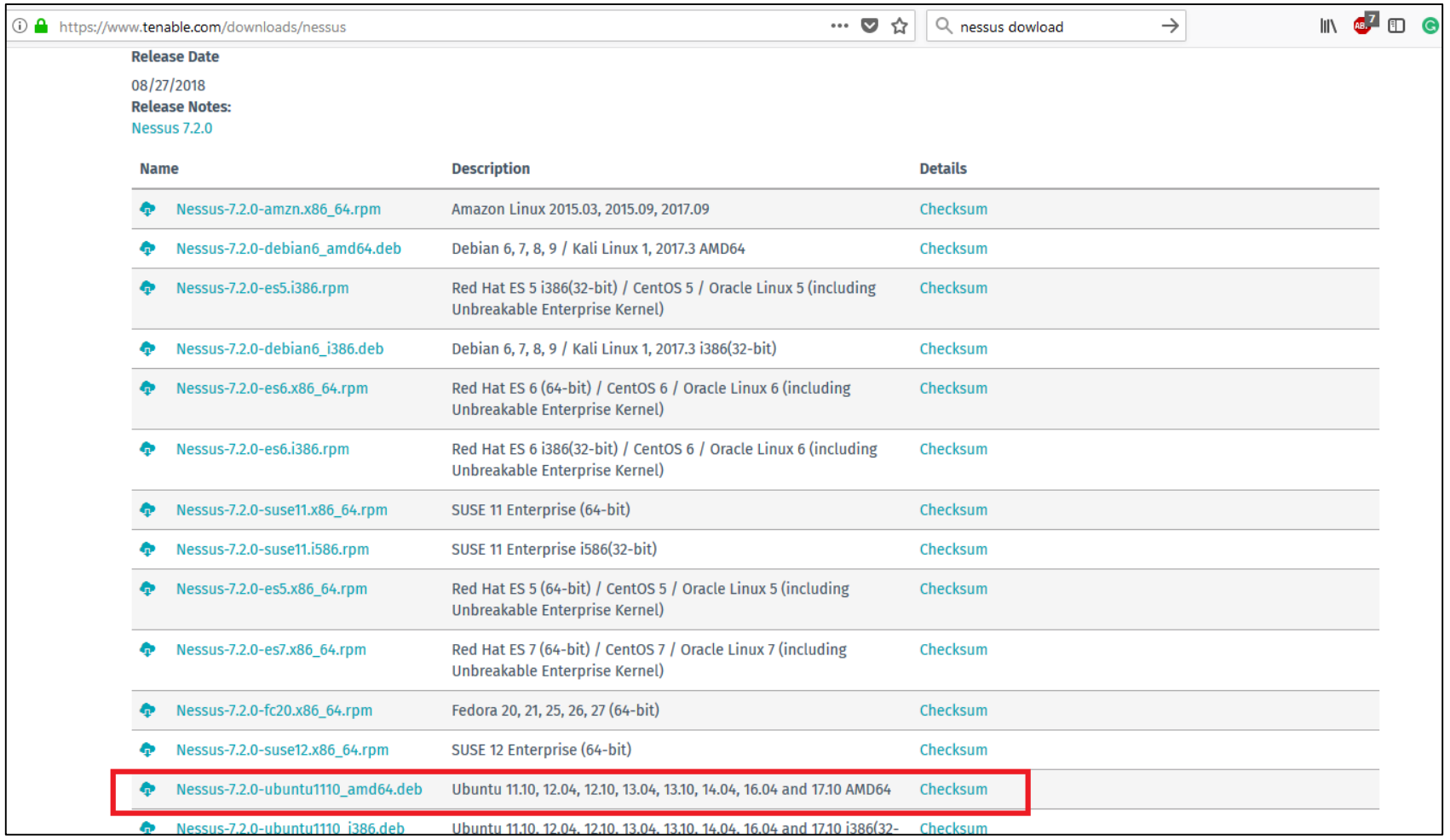
ZENMAP TCP PORT SCAN



NESSUS COMMERCIAL VULNERABILITY SCANNER

- Download Nessus from tenable website
- https://www.tenable.com/downloads/nessus

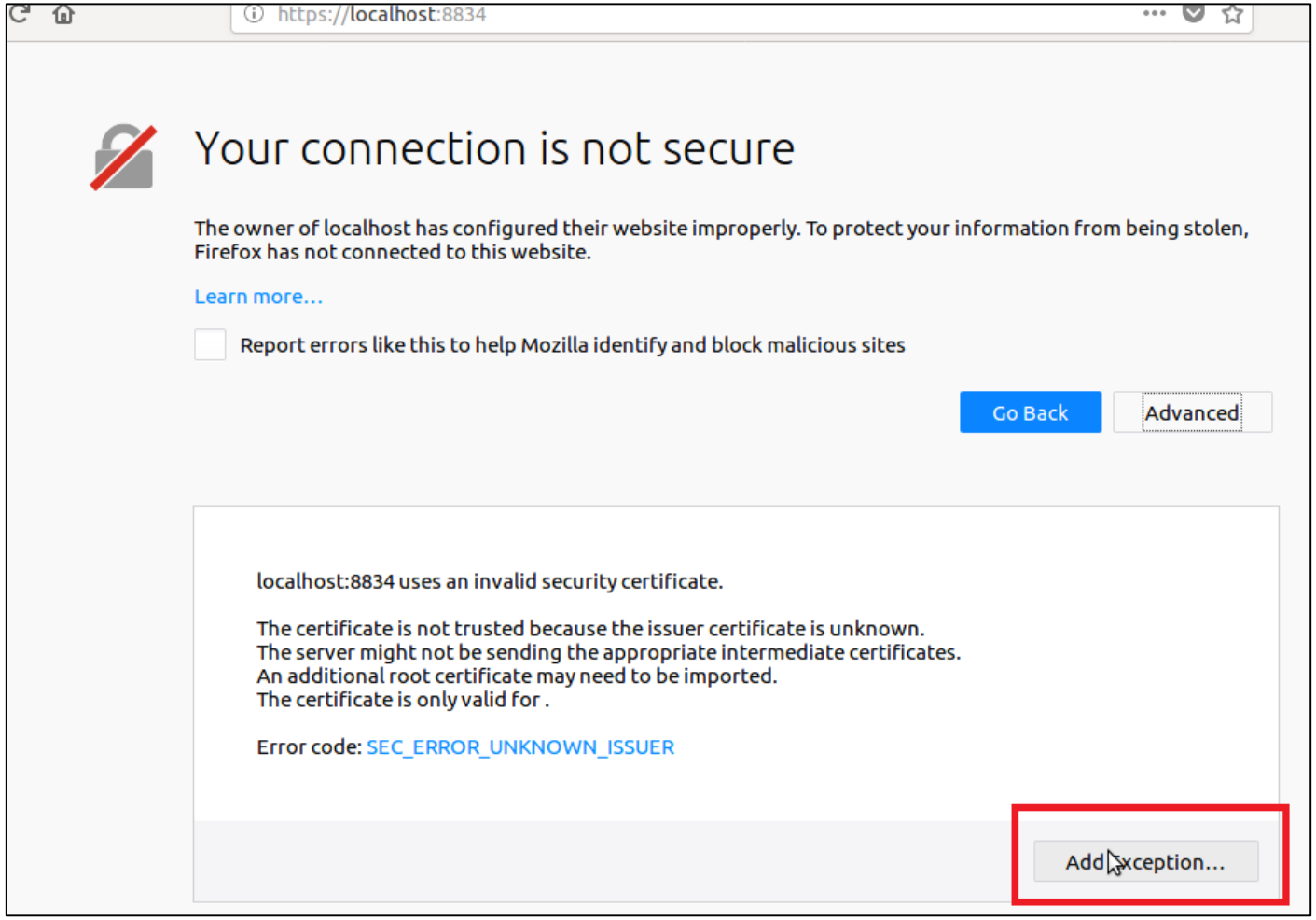
NESSUS


https://www.tenable.com/downloads/nessus
nessus dowload
Release Date
08/27/2018
Release Notes:
Nessus 7.2.0
Name
Description
Details
Nessus-7.2.0-amzn.x86_64.rpm
Amazon Linux 2015.03, 2015.09, 2017.09
Checksum
Nessus-7.2.0-debian6_amd64.deb
Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64
Checksum
Nessus-7.2.0-es5.i386.rpm
Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)
Checksum
Nessus-7.2.0-debian6_i386.deb
Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)
Checksum
Nessus-7.2.0-es6.x86_64.rpm
Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)
Checksum
Nessus-7.2.0-es6.i386.rpm
Red Hat ES 6 i386(32-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)
Checksum
Nessus-7.2.0-suse11.x86_64.rpm
SUSE 11 Enterprise (64-bit)
Checksum
Nessus-7.2.0-suse11.i586.rpm
SUSE 11 Enterprise i586(32-bit)
Checksum
Nessus-7.2.0-es5.x86_64.rpm
Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)
Checksum
Nessus-7.2.0-es7.x86_64.rpm
Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)
Checksum
Nessus-7.2.0-fc20.x86_64.rpm
Fedora 20, 21, 25, 26, 27 (64-bit)
Checksum
Nessus-7.2.0-suse12.x86_64.rpm
SUSE 12 Enterprise (64-bit)
Checksum
Nessus-7.2.0-ubuntu1110_amd64.deb
Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 AMD64
Checksum
Nessus-7.2.0-ubuntu1110_i386.deb
Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04 and 17.10 i386(32-
Checksum

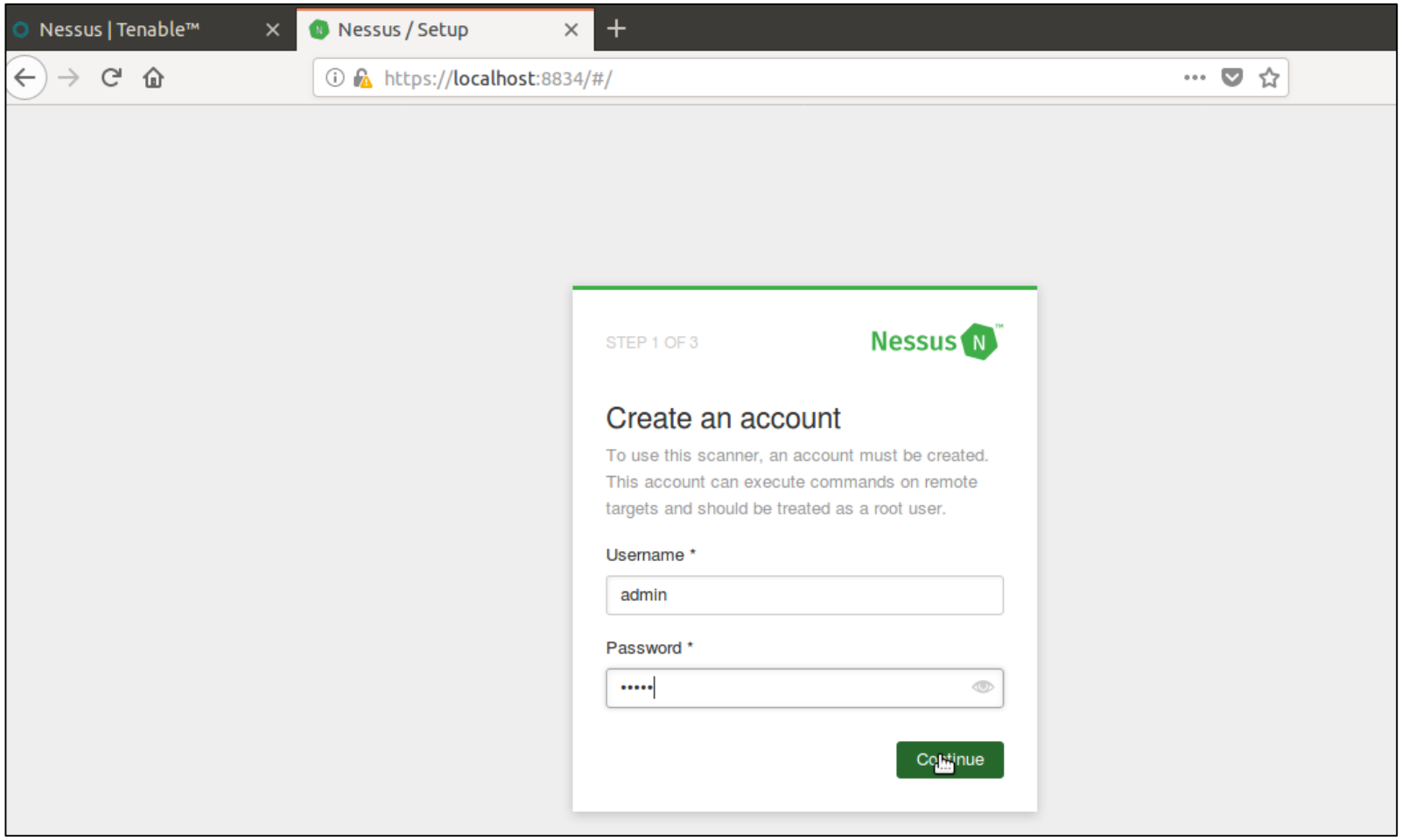
NESSUS SERVICE LINUX

```
ubuntu@ubuntu:~/Downloads$ ls
Nessus-7.2.0-ubuntu1110_amd64.deb  Nessus-7.2.0-ubuntu1110_amd64.deb.part
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i Nessus-7.2.0-ubuntu1110_amd64.deb
[sudo] password for ubuntu:
Selecting previously unselected package nessus.
(Reading database ... 208854 files and directories currently installed.)
Preparing to unpack Nessus-7.2.0-ubuntu1110_amd64.deb ...
Unpacking nessus (7.2.0) ...
Setting up nessus (7.2.0) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /etc/init.d/nessusd start
 - Then go to https://ubuntu:8834/ to configure your scanner

Processing triggers for ureadahead (0.100.0-16) ...
ubuntu@ubuntu:~/Downloads$ sudo service nessusd start
Starting Nessus : .
ubuntu@ubuntu:~/Downloads$
```

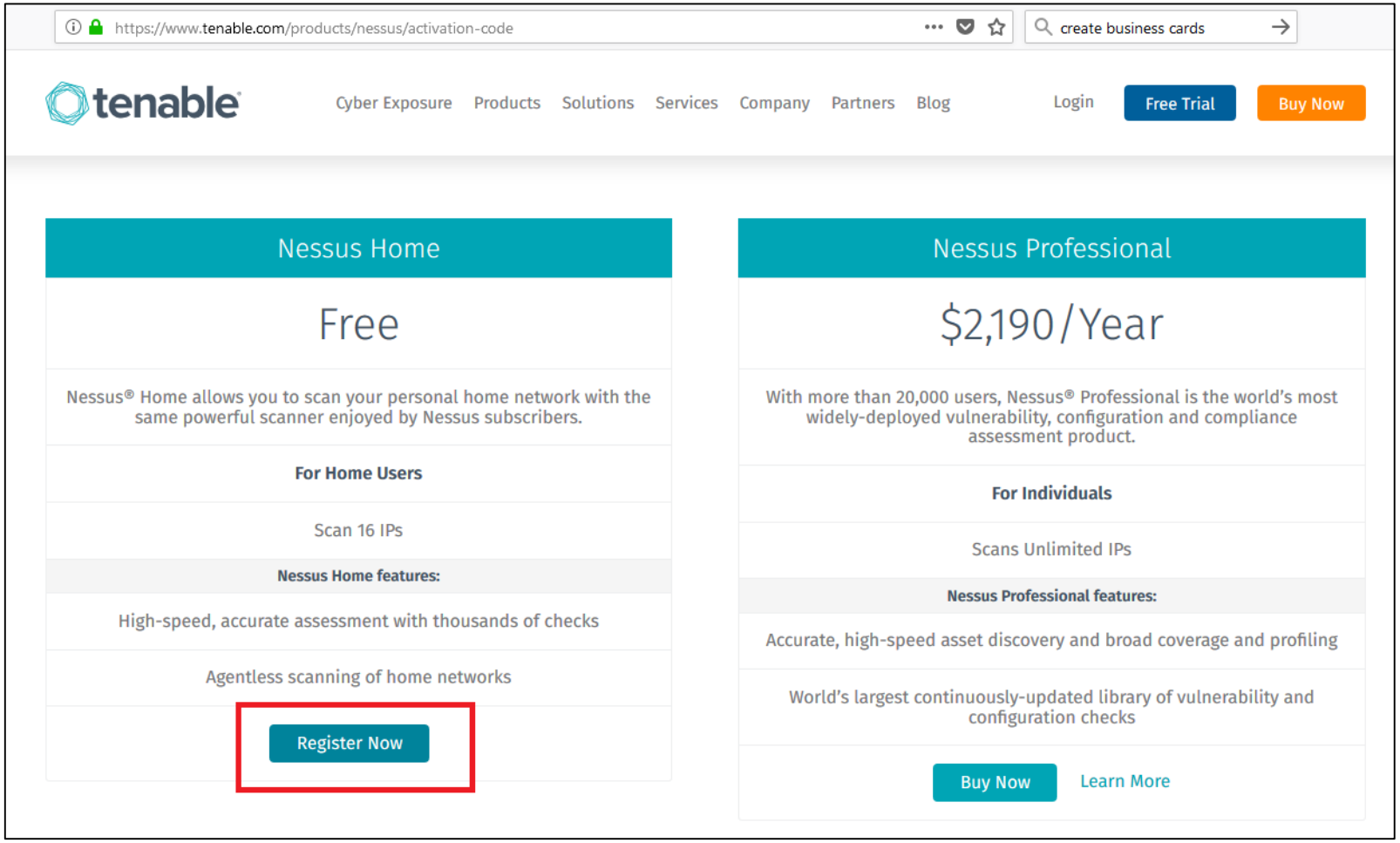

NESSUS GUI


https://localhost:8834
Your connection is not secure
The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Report errors like this to help Mozilla identify and block malicious sites
Go Back
Advanced
localhost:8834 uses an invalid security certificate.
The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.
The certificate is only valid for .
Error code: SEC_ERROR_UNKNOWN_ISSUER
Add Exception...

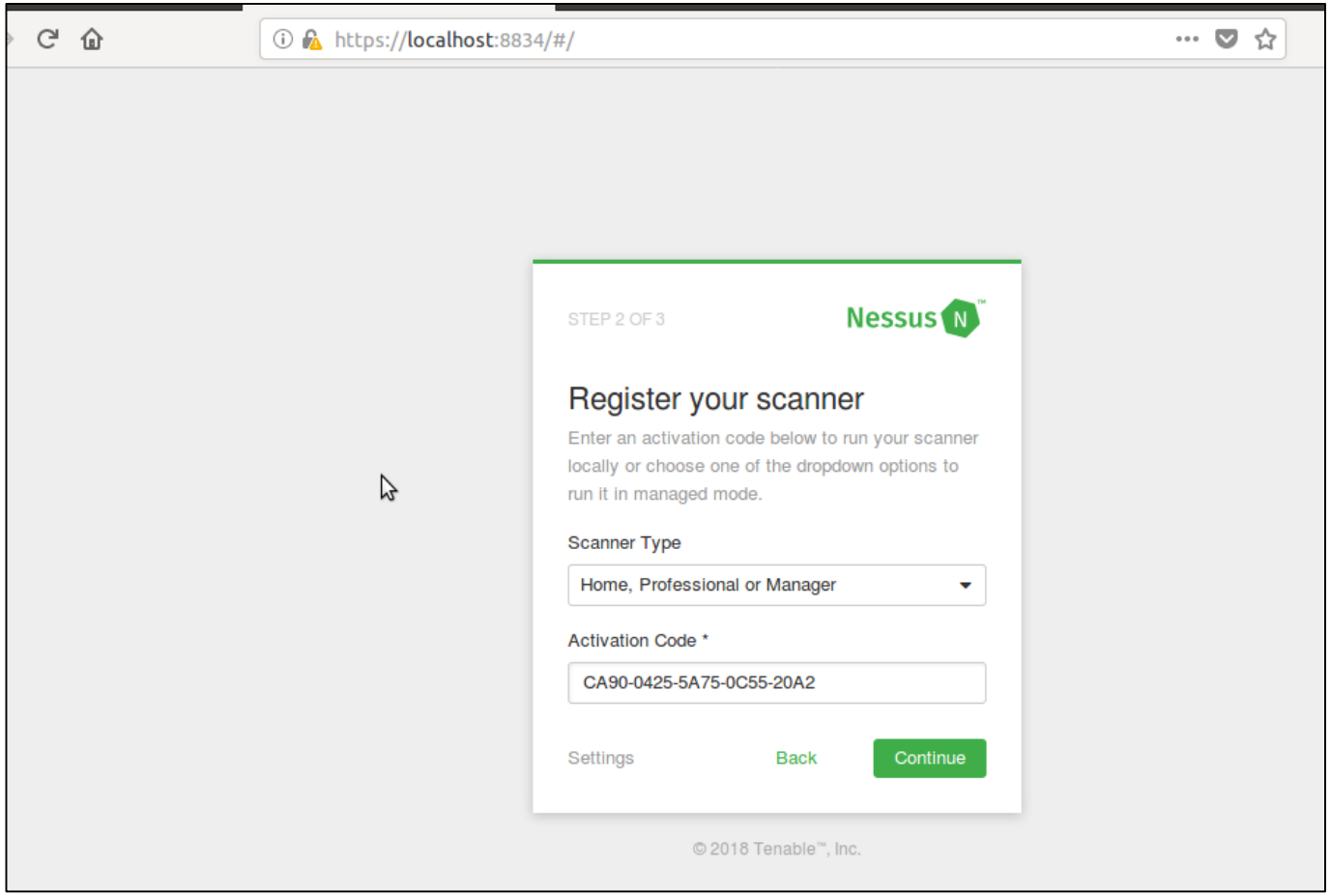
NESSUS ADMIN PORTAL



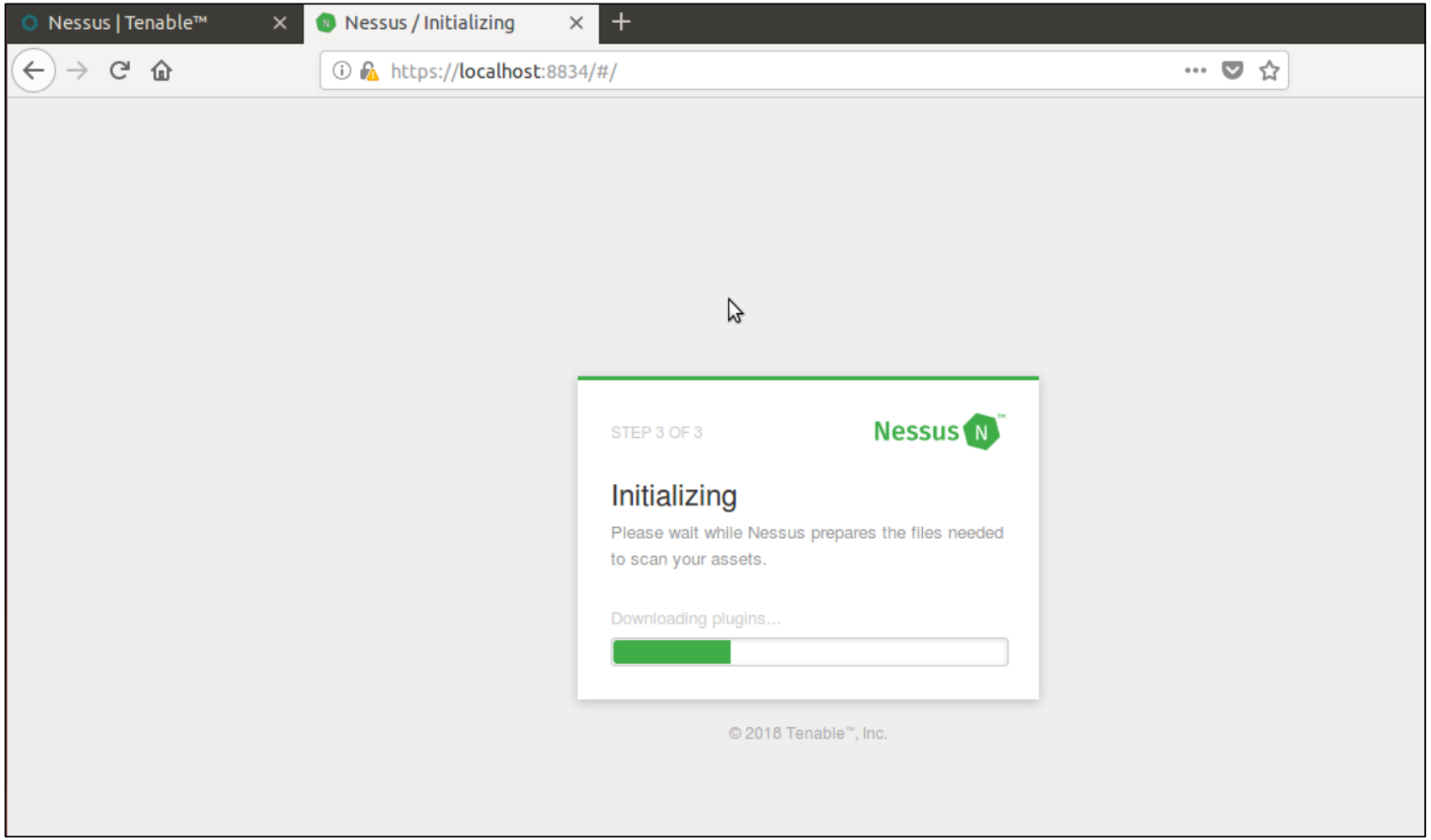
NESSUS ACTIVATION CODE



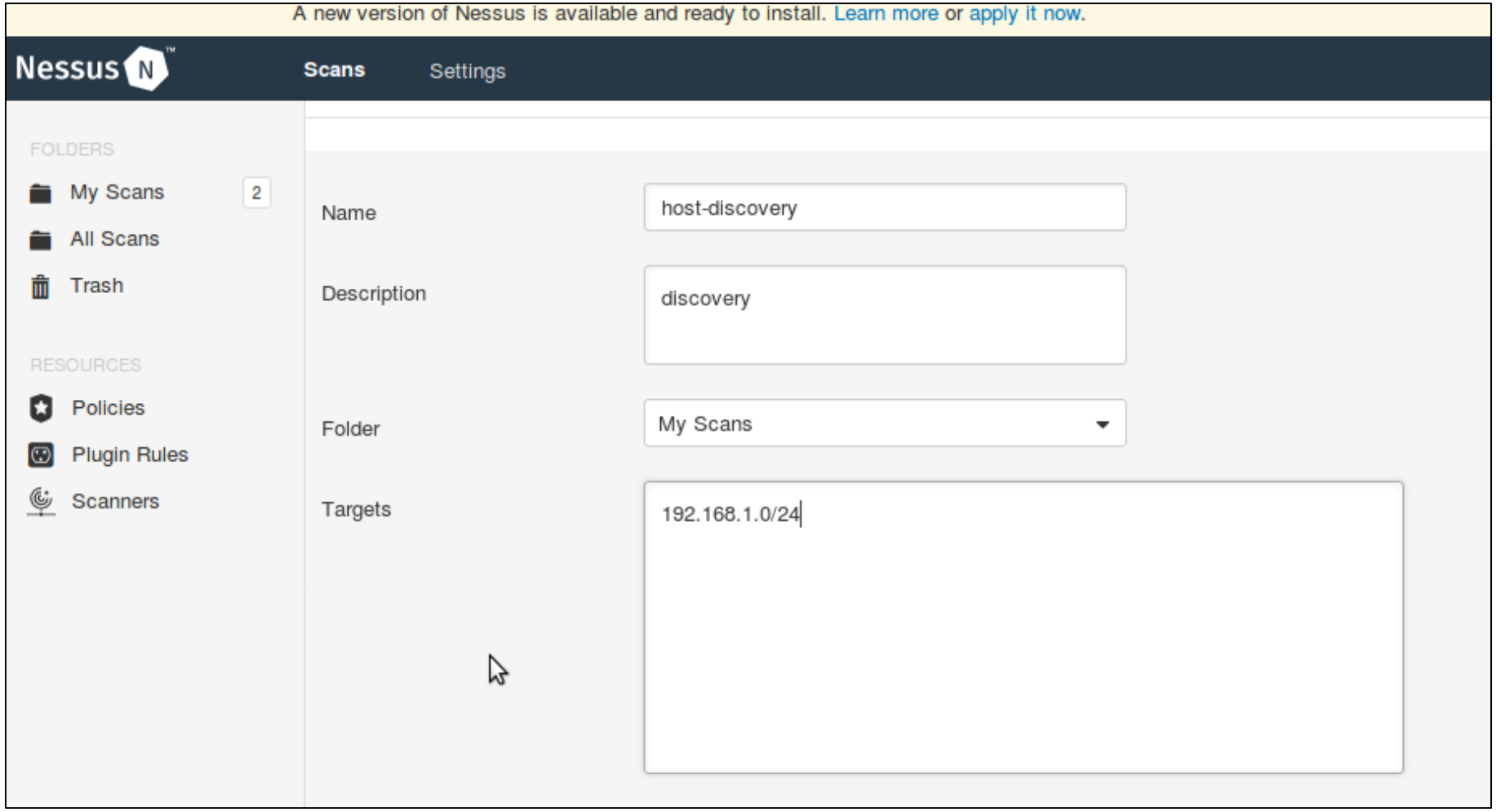
NESSUS INITIALIZATION…TAKES SOME TIME



..STILL INITIALIZING



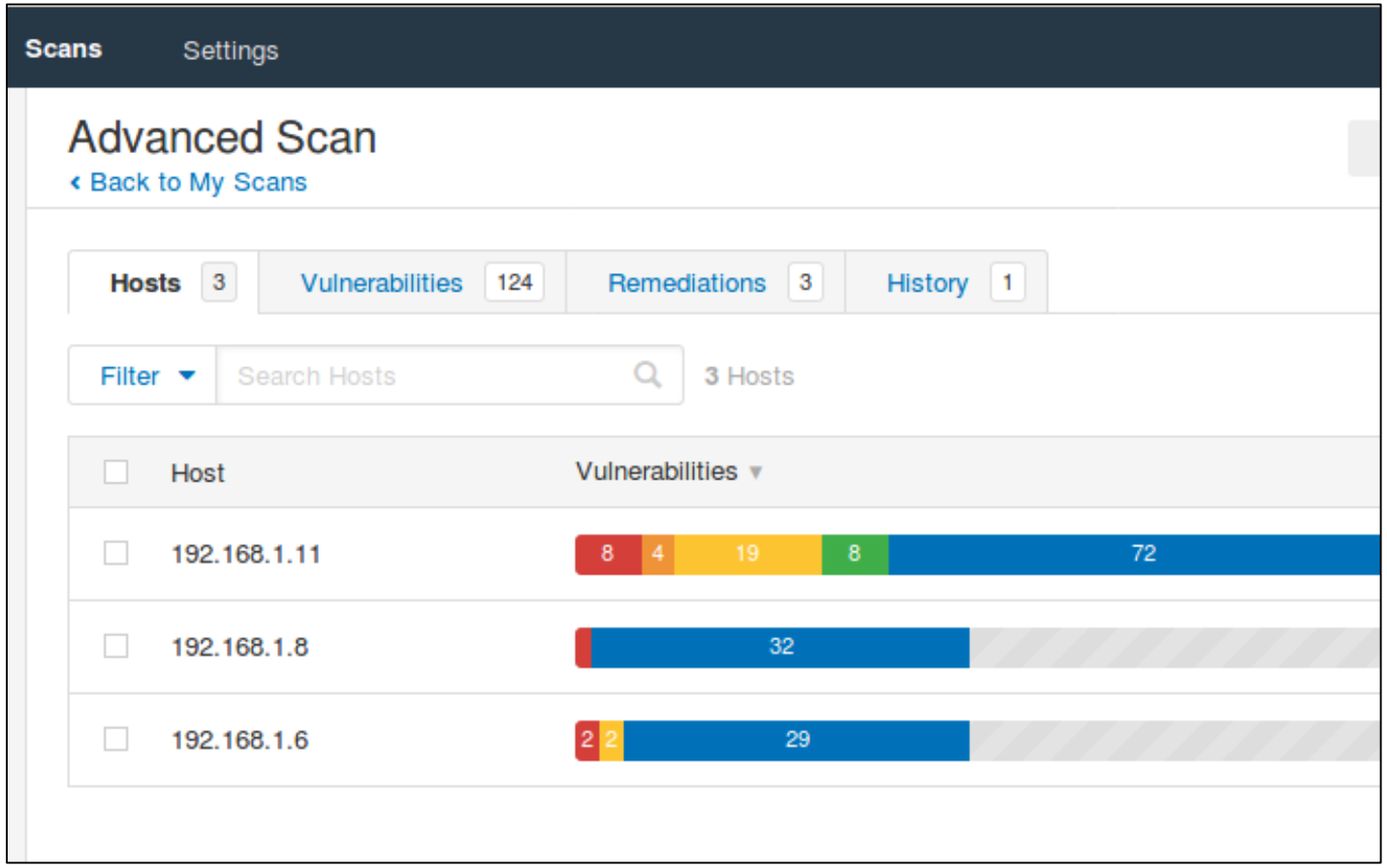
NESSUS CREATE A NEW SCAN



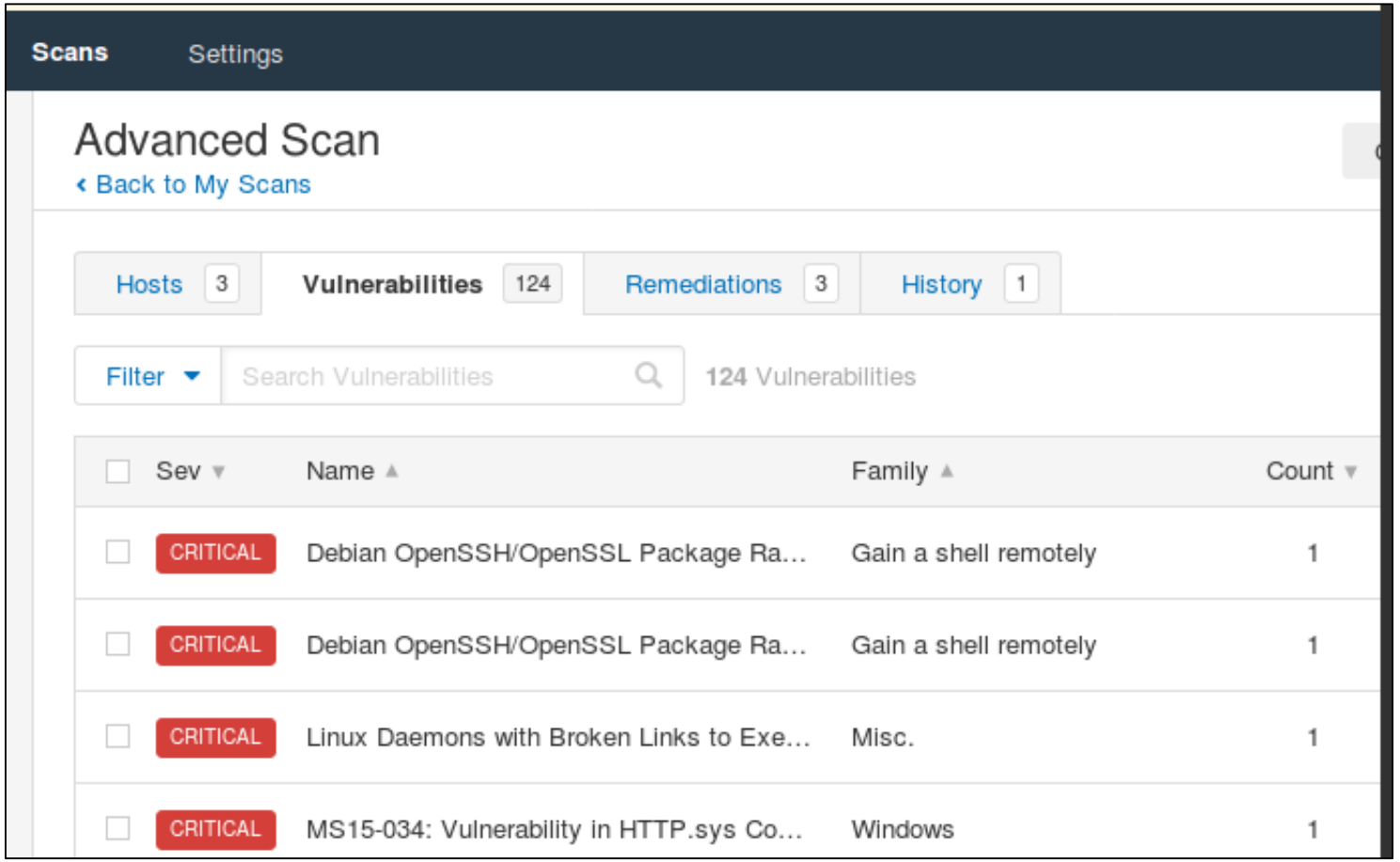
NESSUS LAUNCH A SCAN

Schedule	Last Modified
On Demand	**Today at 2:56 PM**
On Demand	July 20 at 5:06 AM
On Demand	**July 19 at 5:44 AM**
On Demand	**July 19 at 4:34 AM**
On Demand	N/A

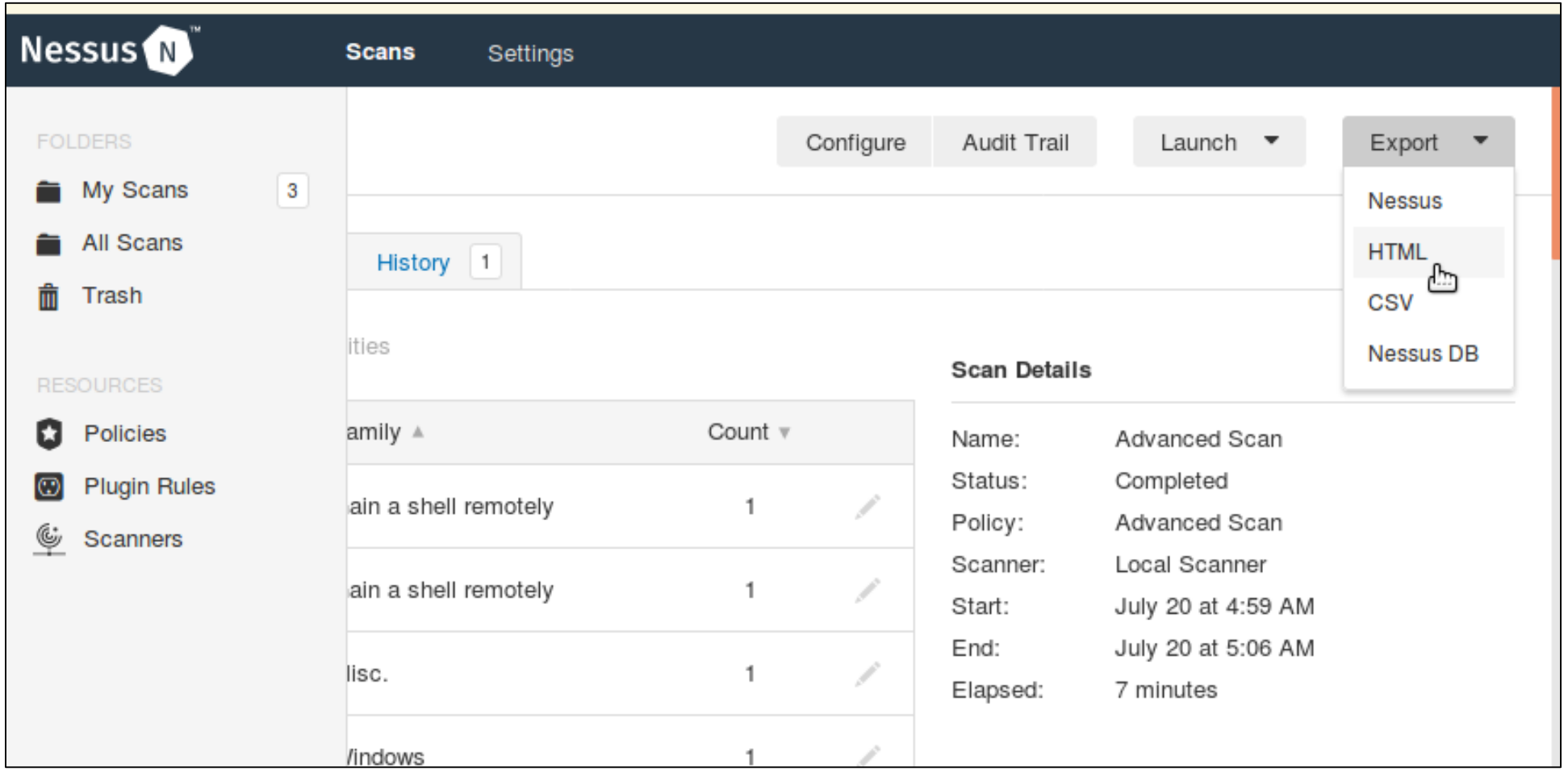
NESSUS CHECK SCAN RESULTS AND VULNERABILITIES



NESSUS CHECK SCAN RESULTS AND VULNERABILITIES



NESSUS EXPORT SCAN RESULTS



SNORT NIDS PRE-REQUISITES

- Ensure to update and upgrade your system
  - sudo apt-get update
  - sudo apt-get upgrade
- Install required dependencies:
  - apt-get install openssh-server ethtool build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev

SNORT NIDS INSTALLATION

- Make a directory: sudo mkdir ~/snort_src
- Go to the created directory: cd snort_src
- Install Data Acquisition library (DAQ) to make abstract calls to packet capture libraries:
  - sudo wget https://snort.org/downloads/snort/daq-2.0.6.tar.gz
  - sudo tar -xvfz daq-2.0.6.tar.gz
  - cd daq-2.0.06
  - Run the configuration script using:
    - ./configure && make && sudo make install

SNORT NIDS MODE

- Update shared libraries using:
  - sudo ldconfig
  - Snort on Ubuntu gets installed to /usr/local/bin/snort directory, it is good practice to create a symbolic link to /usr/sbin/snort using:
    - sudo ln –s /usr/local/bin/snort /usr/sbin/snort

VERIFY SNORT INSTALLATION

```
adel@adel-vm:~$ snort -V

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.9.0 GRE (Build 56)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.7.4
           Using PCRE version: 8.38 2015-11-23
           Using ZLIB version: 1.2.8
```


SNORT CONFIGURATION

- To run Snort on Ubuntu safely without root access, you should create a new unprivileged user and a new user group for the daemon to run under:
  - sudo groupadd snort
  - sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort

SNORT CONFIGURATION

- Before configuring Snort, you will need to create a directory structure for Snort.
  - sudo mkdir /etc/snort
  - sudo mkdir /etc/snort/preproc_rules
  - sudo mkdir /etc/snort/rules
  - sudo mkdir /var/log/snort
  - sudo mkdir /usr/local/lib/snort_dynamicrules

SNORT CONFIGURATION

- Create new files for white and black lists as well as local rules:
  - sudo touch /etc/snort/rules/white_list.rules
  - sudo touch /etc/snort/rules/black_list.rules
  - sudo touch /etc/snort/rules/local.rules

SNORT CONFIGURATION

- Next, set proper permission to the following directories:
  - Chmod –R 5775 /etc/snort/
  - Chmod –R 5775 /var/log/snort/
  - Chmod –R 5775 /usr/local/lib/snort
  - Chmod –R 5775 /usr/local/lib/snort_dynamicrules/

SNORT CONFIGURATION

- Now, you need to copy snort configuration files from snort source to new created directories:
  - Go to ~/snort_src/snort-2.9.9.0/etc
  - sudo cp *.conf* /etc/snort
  - sudo cp *.map /etc/snort
  - sudo cp *.dtd /etc/snort
  - cd ~/snort_src/snort-2.9.8.2/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/
  - sudo cp * /usr/local/lib/snort_dynamicpreprocessor/

SNORT CONFIGURATION

- Edit snort configuration file (snort.conf) located in /etc/snort/
- For testing purpose you do not need all rulesets, so run the following command to comment out all of them:
  - sudo sed -i "s/include \$RULE_PATH/#include \$RULE_PATH/" /etc/snort/snort.conf
  - sudo vim /etc/snort/snort.conf

SNORT CONFIGURATION

- Go to line 104 and change the following:
  - var RULE_PATH ../rules ➔ var RULE_PATH /etc/snort/rules
  - var SO_RULE_PATH ../so_rules ➔ SO_RULE_PATH /etc/snort/so_rules
  - var PREPROC_RULE_PATH ../preproc_rules ➔ var PREPROC_RULE_PATH /etc/snort/preproc_rules
  - var WHITE_LIST_PATH ../rules ➔ var WHITE_LIST_PATH /etc/snort/rules/iplists
  - var BLACK_LIST_PATH ../rules ➔ var BLACK_LIST_PATH /etc/snort/rules/iplists
- To enable local rules and test snort, go to line 545 and uncomment local.rules
  - Include $RULE_PATH/local.rules

TESTING SNORT CONFIGURATION

- Test the configuration file using:
  - sudo snort -T -i ens160 -c /etc/snort/snort.conf
- You should see output like this:
  - Snort successfully validated the configuration!
  - Snort exiting

SNORT ADDING CUSTOM RULES

- Now edit local.rules file
  - sudo vim /etc/snort/rules/local.rules
- Add this rule:
  - alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)
  - This rule means generate an alert on icmp packets originated from any source and any port to the home_net on any port. HOME_NET can be changed to include home_net ip.

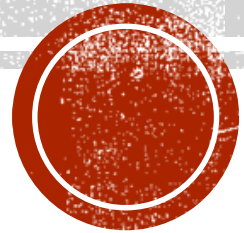
SNORT TESTING CUSTOM RULE

- Now, for testing, you have to ping from a VM on your network and make snot listening on the right interface:
  - sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0
    - Check your interface that you want snort to listen on!!, use ifconfig to define the interface

SNORT TESTING CUSTOM RULE

- Now, ping from one machine to anorher to see the snort alerts!
- On your terminal (console) you can see the alerts. You can refer to snort manual to see other options on how to log alerts.
- Go check saved logs /var/log/snort/snort.log.<timestamp>

DETECTION AND LOGGING



Intrusion Detection, Logging

INCIDENT AND EVENT LOGGING

LOG SOURCES

- Server and Workstation OS Log
- Application Logs – Web Server, Database Server
- Security Tool Logs - AV, HIDS, NIDS
- Outbound proxy logs, end-user application logs
- Firewall Logs

LOG LOCATIONS

- Linux - /var/log
- Windows – System, Security, Application Event Logs
- Network Devices – Syslog, proprietary locations and formats

WINDOWS EVENTS AND INCIDENTS

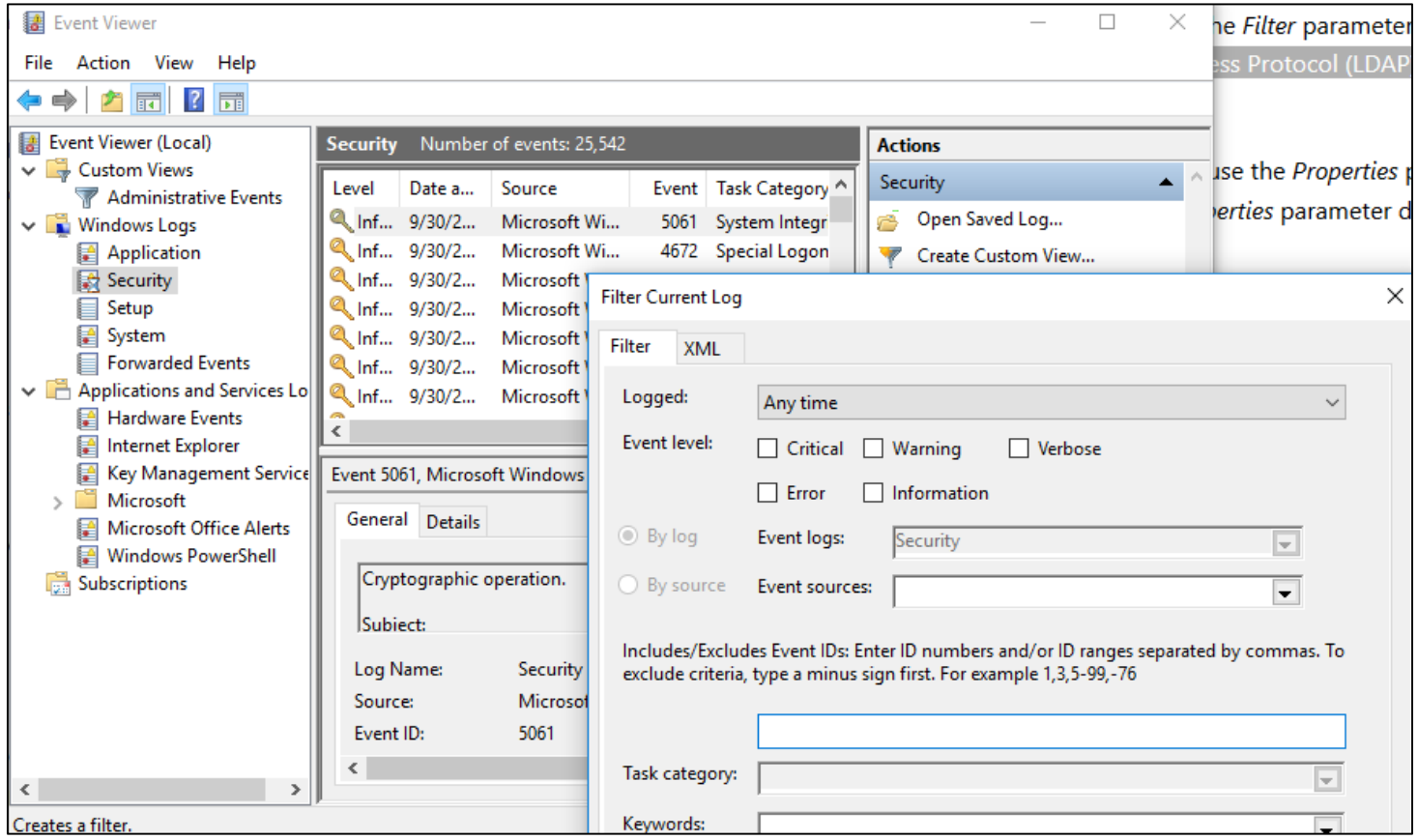
- User Log-on, Log-Off
- User Account Changes
- Password Changes
- Service Started/ Stopped/ Errors
- Registry entries modified
- Object Access Attempts
- Audit, Event Logs Cleared

WINDOWS EVENTS AND INCIDENTS

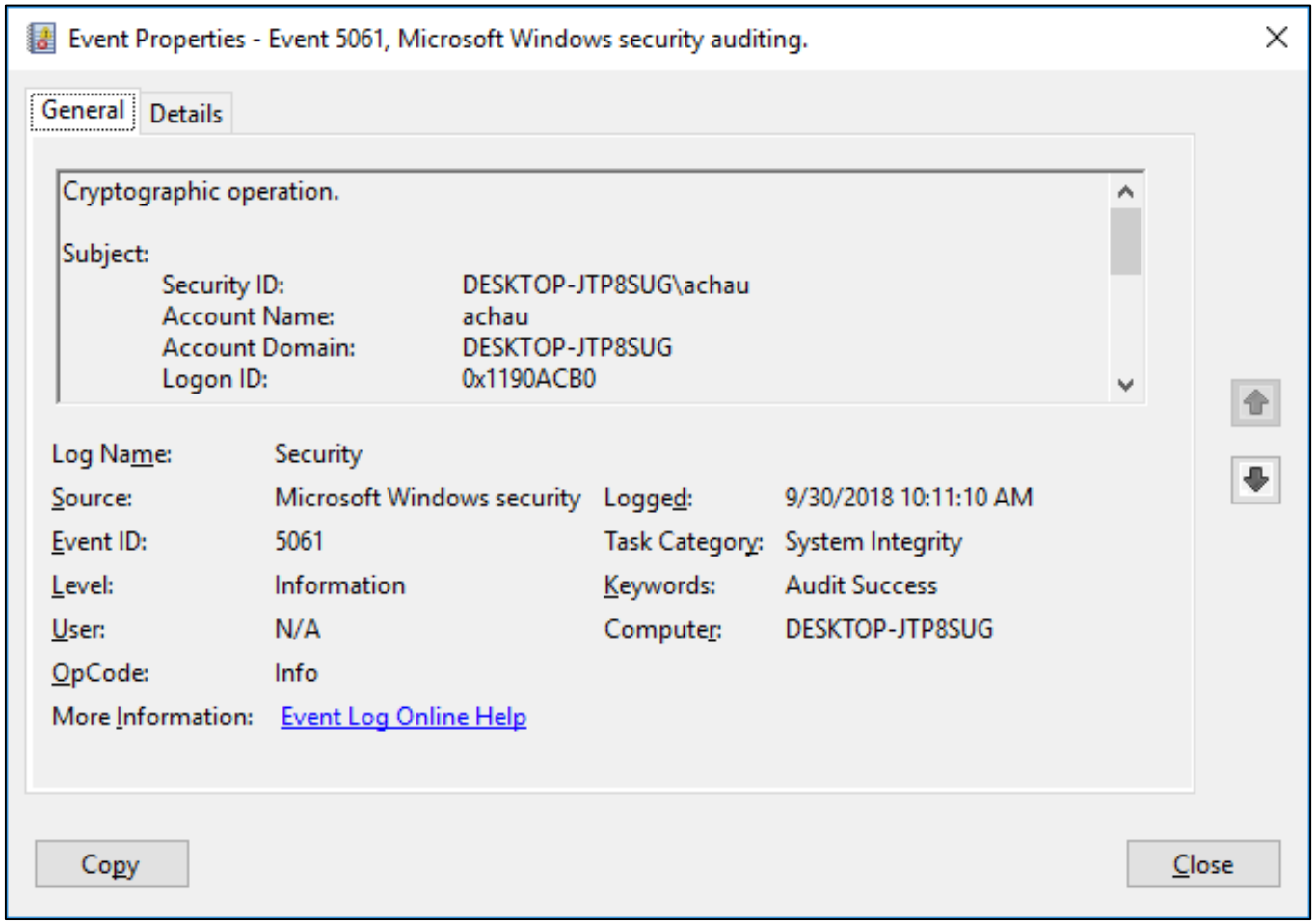
Windows Activity	Source	Event ID
App Crash	Application	1001
Application Error	Application	1000
New process Created	Security	4688
Service Installed on the System	Security	4697
Successful Logon	Security	528, 540
Failed Logon	Security	529-537

WINDOWS EVENT VIEWER

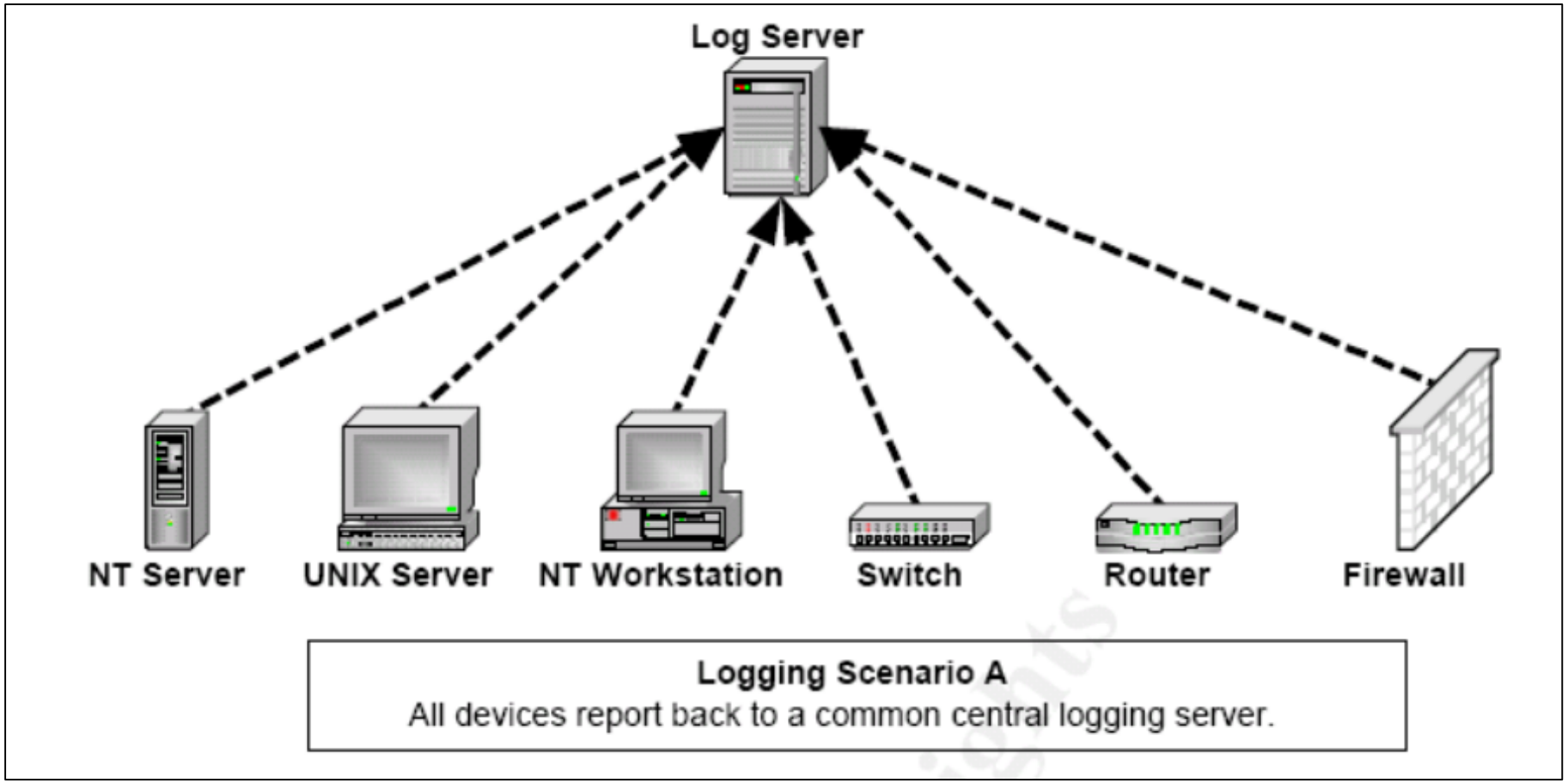
- Shows windows application logs and system messages.
- Useful tool for security assessment and troubleshooting.



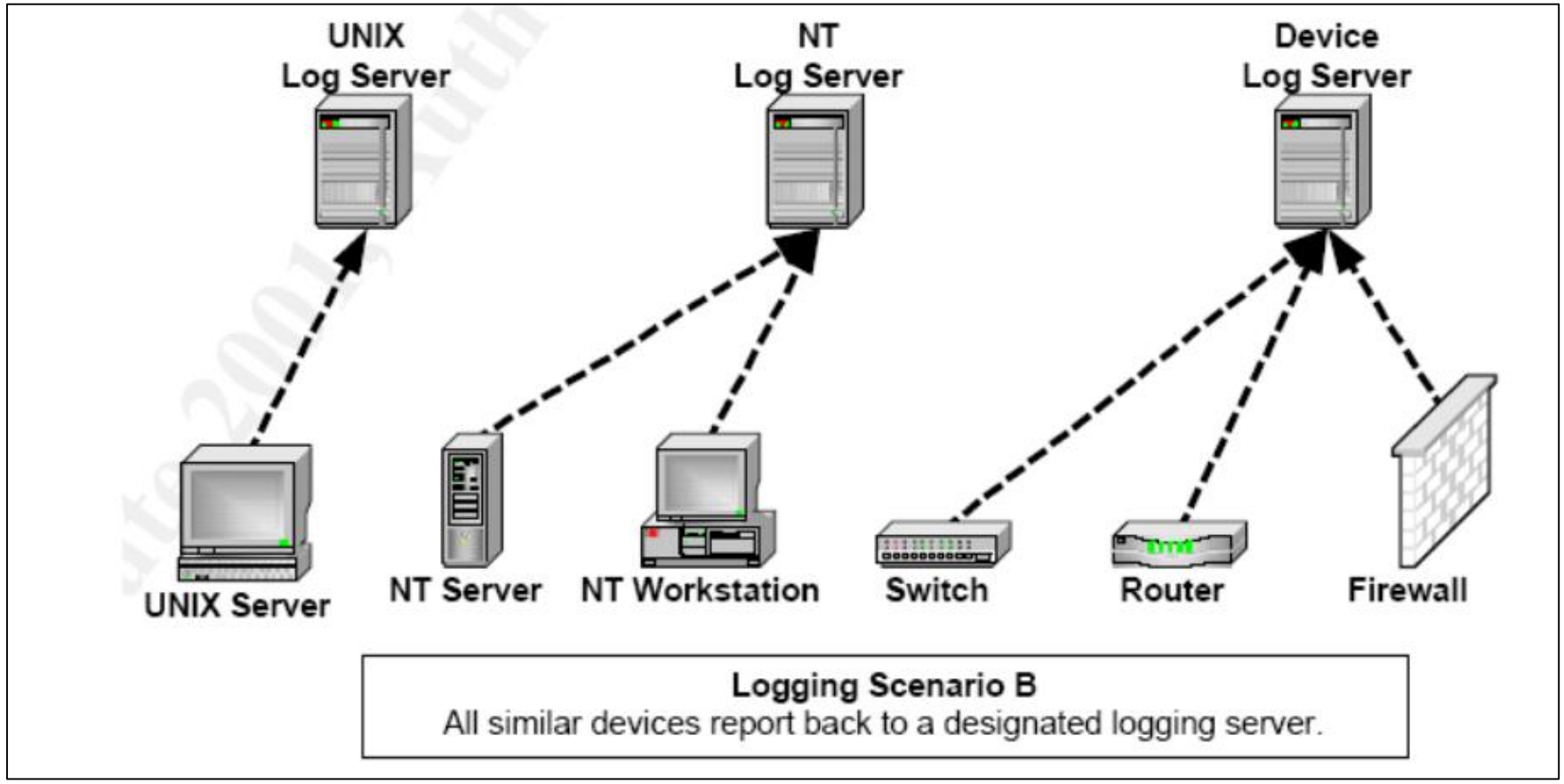
WINDOWS EVENT VIEWER



LOGGING MECHANISM – CENTRALIZED LOGGING



LOGGING MECHANISM – DISTRIBUTED LOGGING



SYSLOG

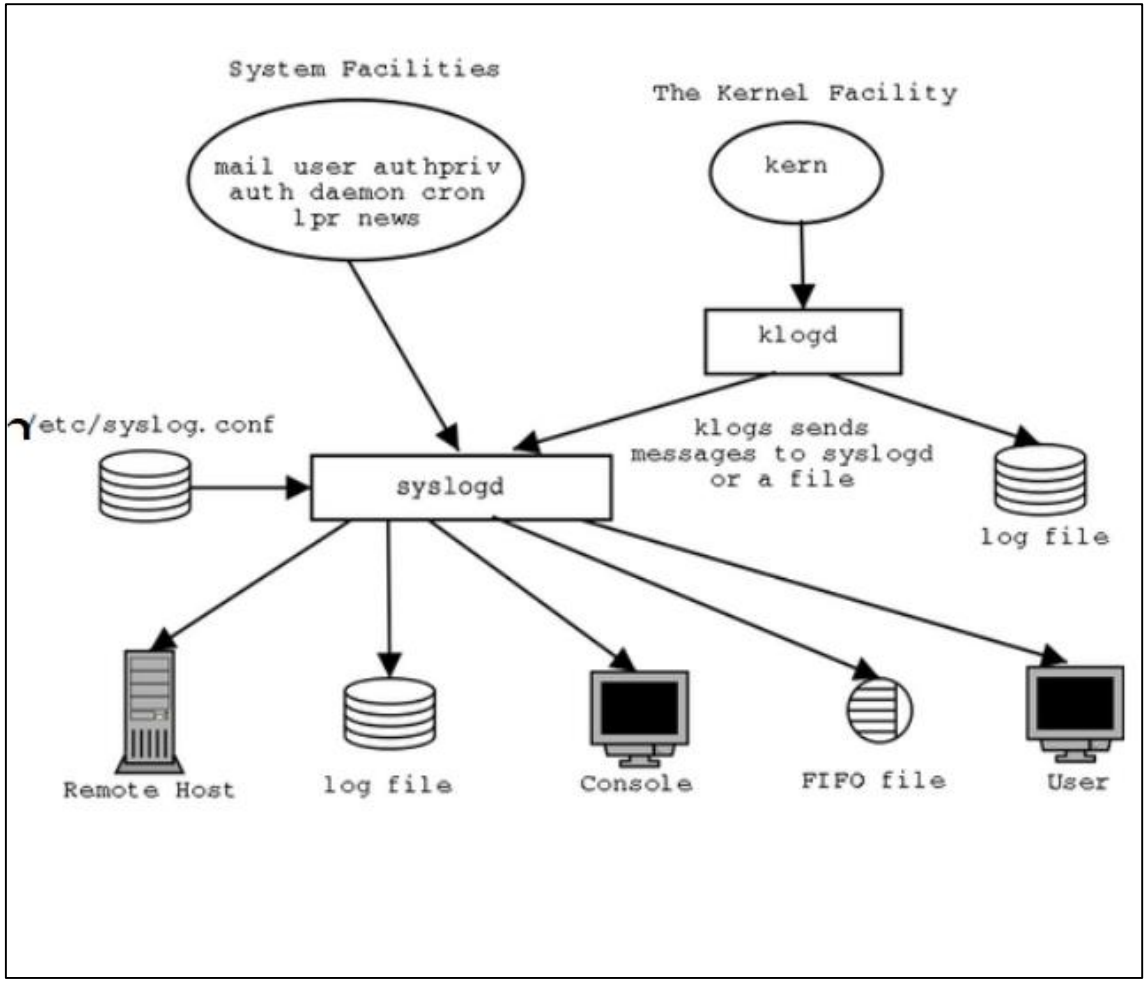
- Syslog is a utility for tracking and logging all manner of system messages from the merely informational to the extremely critical.
- Each msg sent to the syslog server has two descriptive labels:
- Function Facility for the application that generated it, e.g., mail, cron, auth (security logs).
- Severity Level of the message.

SYSLOG SECURITY LEVELS

Severity Level	Keyword for	Keyword for Cisco Router	Description
0	emerg	emergencies	System unusable
1	alert	alerts	Immediate action required
2	crit	critical	Critical condition
3	err	errors	Error conditions
4	warning	warnings	Warning conditions
5	notice	notifications	Normal but significant
6	info	informational	Informational messages
7	debug	debugging	Debugging messages

SYSLOG

- **syslogd** collects the logs from various agents in a centralized manner.
- Logging is configured in /etc/syslog.conf files containing names and locations for your system log files.
- **klogd** takes care of kernel log messages



SAMPLE SYSLOG CONFIGURATION FILE

```
1:  #kern.*                                          /dev/console
2:  # Log anything (except mail) of level info or higher.
3:  # Don't log private authentication messages!
4:  *.info;mail.none;authpriv.none;cron.none        /var/log/messages
5:  # The authpriv file has restricted access.
6:  authpriv.*                                       /var/log/secure
7:  # Log all the mail messages in one place.
8:  mail.*                                    /var/log/maillog
9:  # Log cron stuff
10: cron.*                                           /var/log/cron
11: # Everybody gets emergency messages
12: *.emerg                                          *
13: # Save news errors of level crit and higher in a special file.
14: uucp,news.crit                                   /var/log/spooler
15: # Save boot messages also to boot.log
16: local7.*                                         /var/log/boot.log
17: # To specifiy a single priority rather than all priorities above.
18: *.=debug                                         /var/log/debug.log
```


LOG ROTATION

- Log Files can grow a lot and become useless.
- Logrotate service rotates log files, conserving only compressed logs under a specified age.
- Logrotate is executed by the crond in regular basis and its main configuration file is /etc/logrotate.conf

```
# see "man logrotate" for details
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# drop log rotation information into this directory
include /etc/logrotate.d
```


LOG ROTATION

```
#cron job 1: at 5am, find yesterday's logs, and move them to old_logs
0 5 * * * /usr/bin/find /mnt/*/log/????-??-?? -maxdepth 0 -type d ! -mmin -
300 -exec bash -c 'dir={}; old=${dir/\/log\//\/old_logs\/}; mv ${dir}
${old}' \;

#cron job 2: find any files older than 5 days, 23 hours, and delete them
0 4 * * * /usr/bin/find /mnt/*/old_logs/????-??-?? -maxdepth 0 -type d ! -
mmin -8580 -exec rm -rf {} \;
```


CONFIGURING THE REMOTE SYSLOG SERVER

- Edit */etc/rsyslog.conf*
- Restart the service- service rsyslog restart
- Add iptables rule if required *iptables –A INPUT –m state –state NEW –m tcp –p tcp --dport 514 –j ACCEPT*
- Restart iptables service.

Server

```
$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
"/etc/rsyslog.conf" [readonly] 61L, 1316C                    4,1
```

Client

```
daemon.*;mail.*;\
        news.err;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       |/dev/xconsole

*.* @192.168.0.4:514
```


DEFENSE AGAINST LOG AND ACCOUNTING FILE ATTACKS

- Active Logging
- Set proper permissions
- Keep a separate log server
- Encrypt the log files - Core Labs tools at http://www.core-sdi.com/english/freesoft.html
- Make Log files append only; $ chattr +a [logname]
- Protecting log files with write-once media, such as CD-ROM

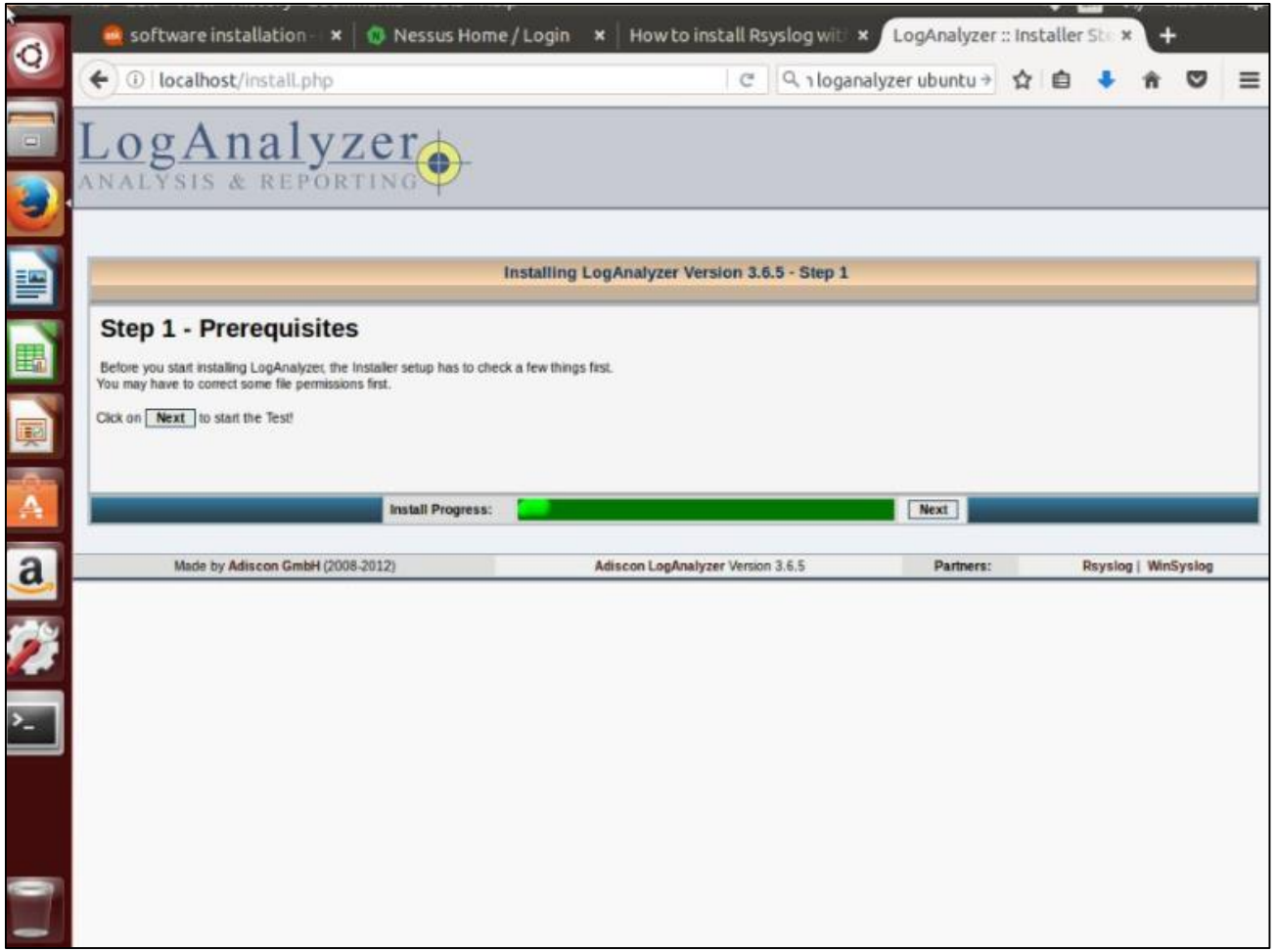
LOG MANAGEMENT SERVERS

- Log Analyzer
- Splunk
- Graylog
- ELK Stack

LOG ANALYZER

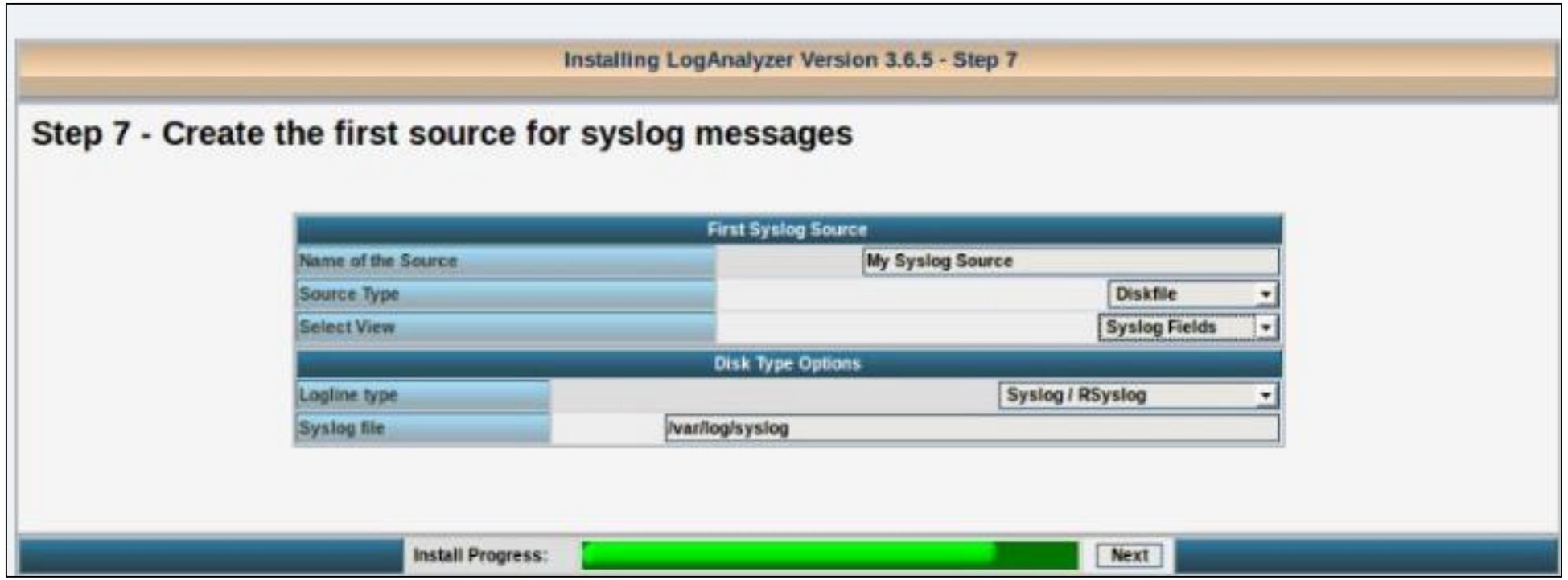
- Logs are saved in a mysql database.
- Configured with rsyslog server and LAMP stack.
- Provides visualization and log configuration options.
- Provides basic search and filtering capability.
- Doesn't have a rich query interface for performing analytics.

LOG ANALYZER

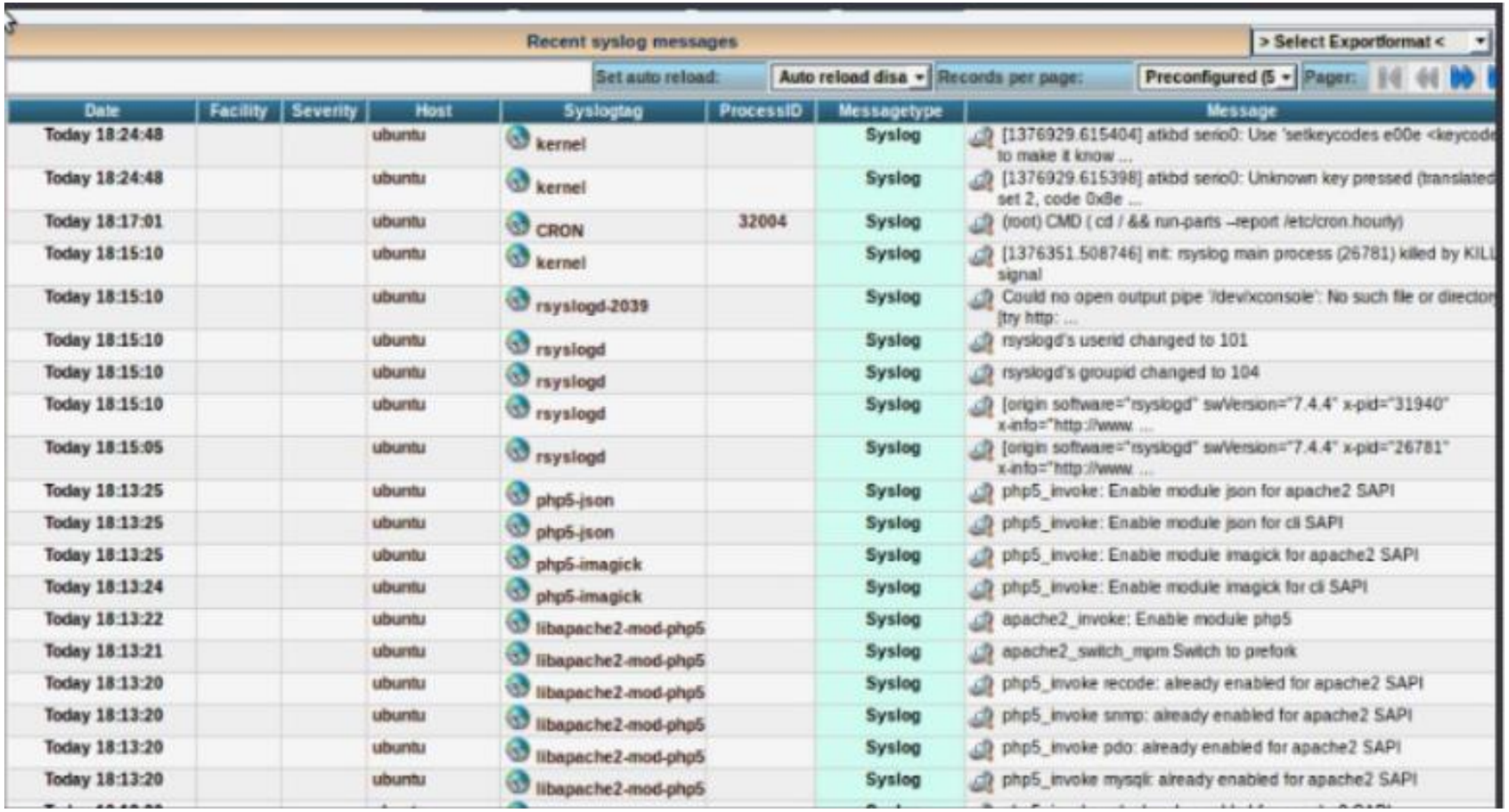


LOG ANALYZER

LOG ANALYZER



LOG ANALYZER



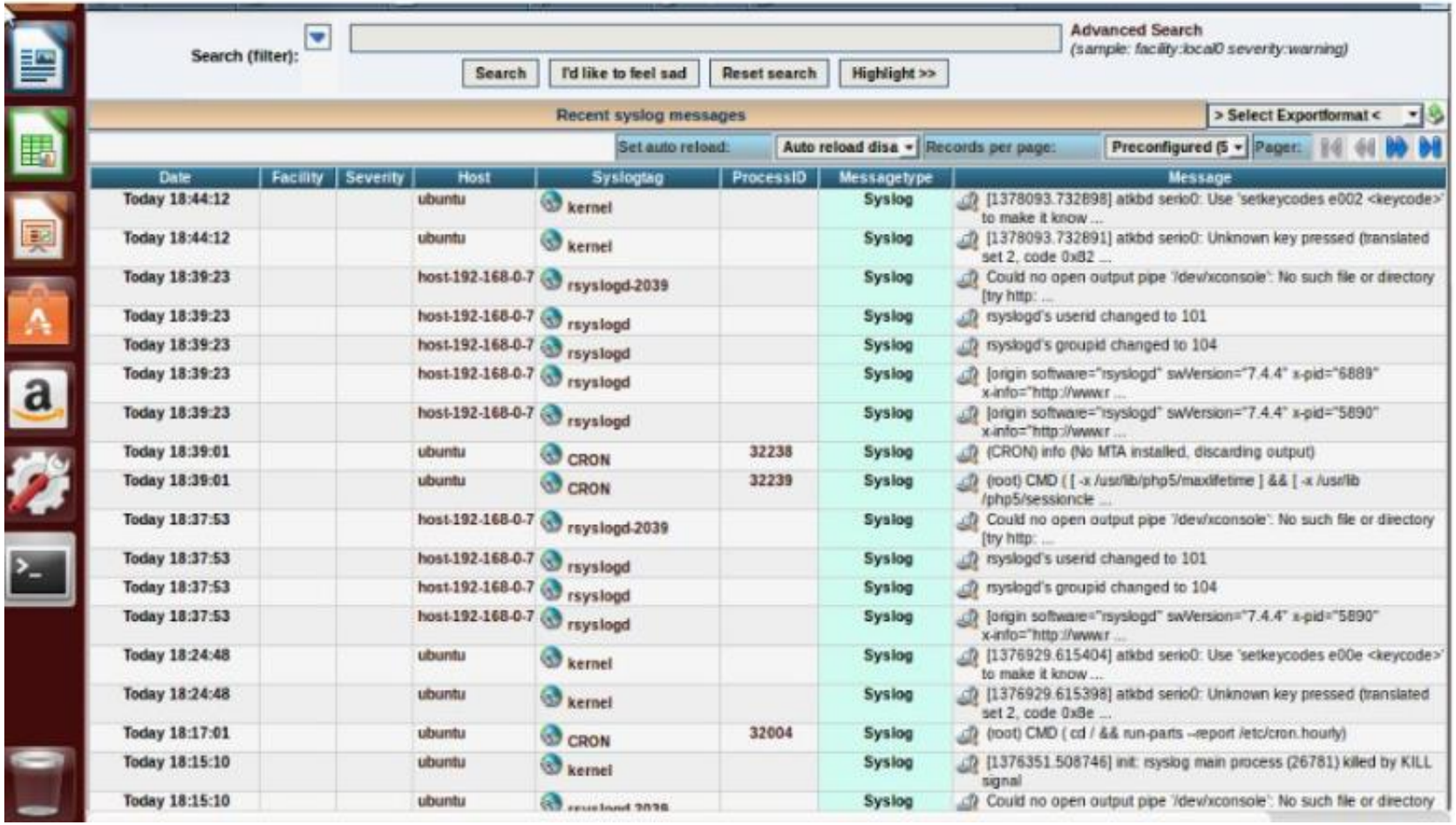
Recent syslog messages

> Select Exportformat <

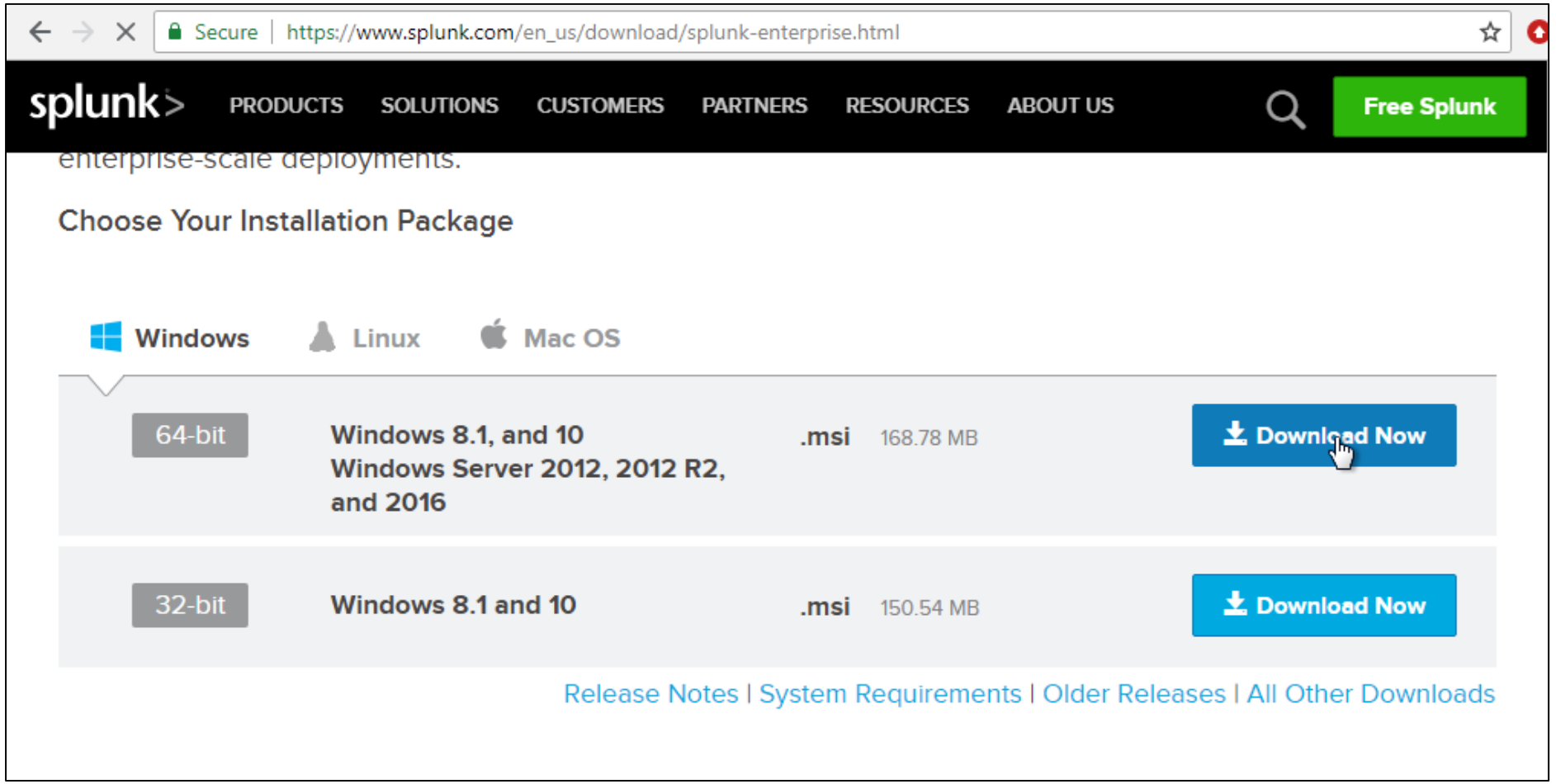
Set auto reload: Auto reload disa | Records per page: Preconfigured (5 | Pager:

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 18:24:48			ubuntu	kernel		Syslog	[1376929.615404] atkbd serio0: Use 'setkeycodes e00e <keycode> to make it know ...
Today 18:24:48			ubuntu	kernel		Syslog	[1376929.615398] atkbd serio0: Unknown key pressed (translated set 2, code 0x8e ...
Today 18:17:01			ubuntu	CRON	32004	Syslog	(root) CMD (cd / && run-parts --report /etc/cron.hourly)
Today 18:15:10			ubuntu	kernel		Syslog	[1376351.508746] init: rsyslog main process (26781) killed by KILL signal
Today 18:15:10			ubuntu	rsyslogd-2039		Syslog	Could no open output pipe '/dev/xconsole': No such file or director [try http: ...
Today 18:15:10			ubuntu	rsyslogd		Syslog	rsyslogd's userid changed to 101
Today 18:15:10			ubuntu	rsyslogd		Syslog	rsyslogd's groupid changed to 104
Today 18:15:10			ubuntu	rsyslogd		Syslog	[origin software="rsyslogd" swVersion="7.4.4" x-pid="31940" x-info="http://www. ...
Today 18:15:05			ubuntu	rsyslogd		Syslog	[origin software="rsyslogd" swVersion="7.4.4" x-pid="26781" x-info="http://www. ...
Today 18:13:25			ubuntu	php5-json		Syslog	php5_invoke: Enable module json for apache2 SAPI
Today 18:13:25			ubuntu	php5-json		Syslog	php5_invoke: Enable module json for cli SAPI
Today 18:13:25			ubuntu	php5-imagick		Syslog	php5_invoke: Enable module imagick for apache2 SAPI
Today 18:13:24			ubuntu	php5-imagick		Syslog	php5_invoke: Enable module imagick for cli SAPI
Today 18:13:22			ubuntu	libapache2-mod-php5		Syslog	apache2_invoke: Enable module php5
Today 18:13:21			ubuntu	libapache2-mod-php5		Syslog	apache2_switch_mpm Switch to prefork
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke recode: already enabled for apache2 SAPI
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke snmp: already enabled for apache2 SAPI
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke pdo: already enabled for apache2 SAPI
Today 18:13:20			ubuntu	libapache2-mod-php5		Syslog	php5_invoke mysqli: already enabled for apache2 SAPI

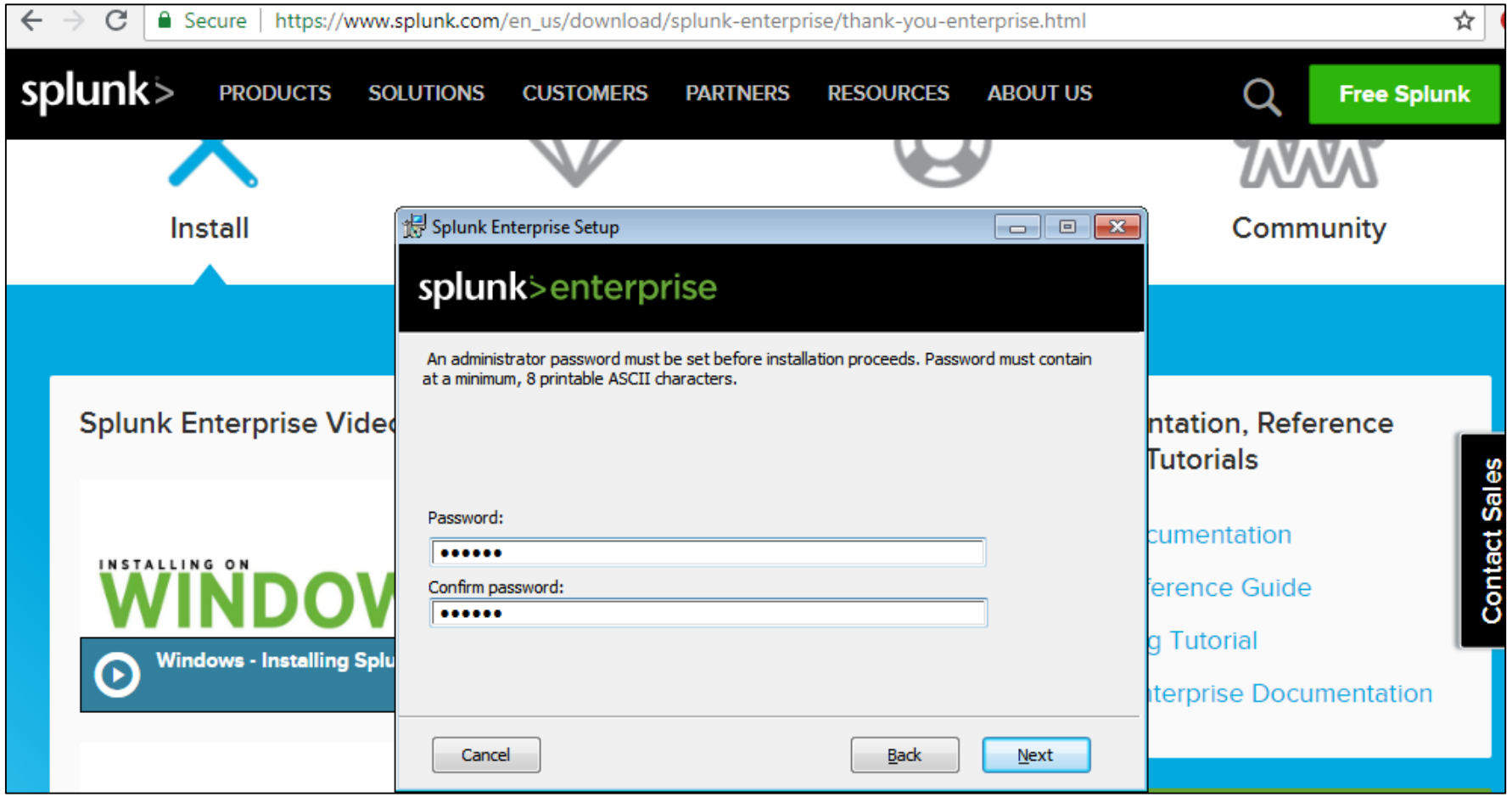
LOG ANALYZER



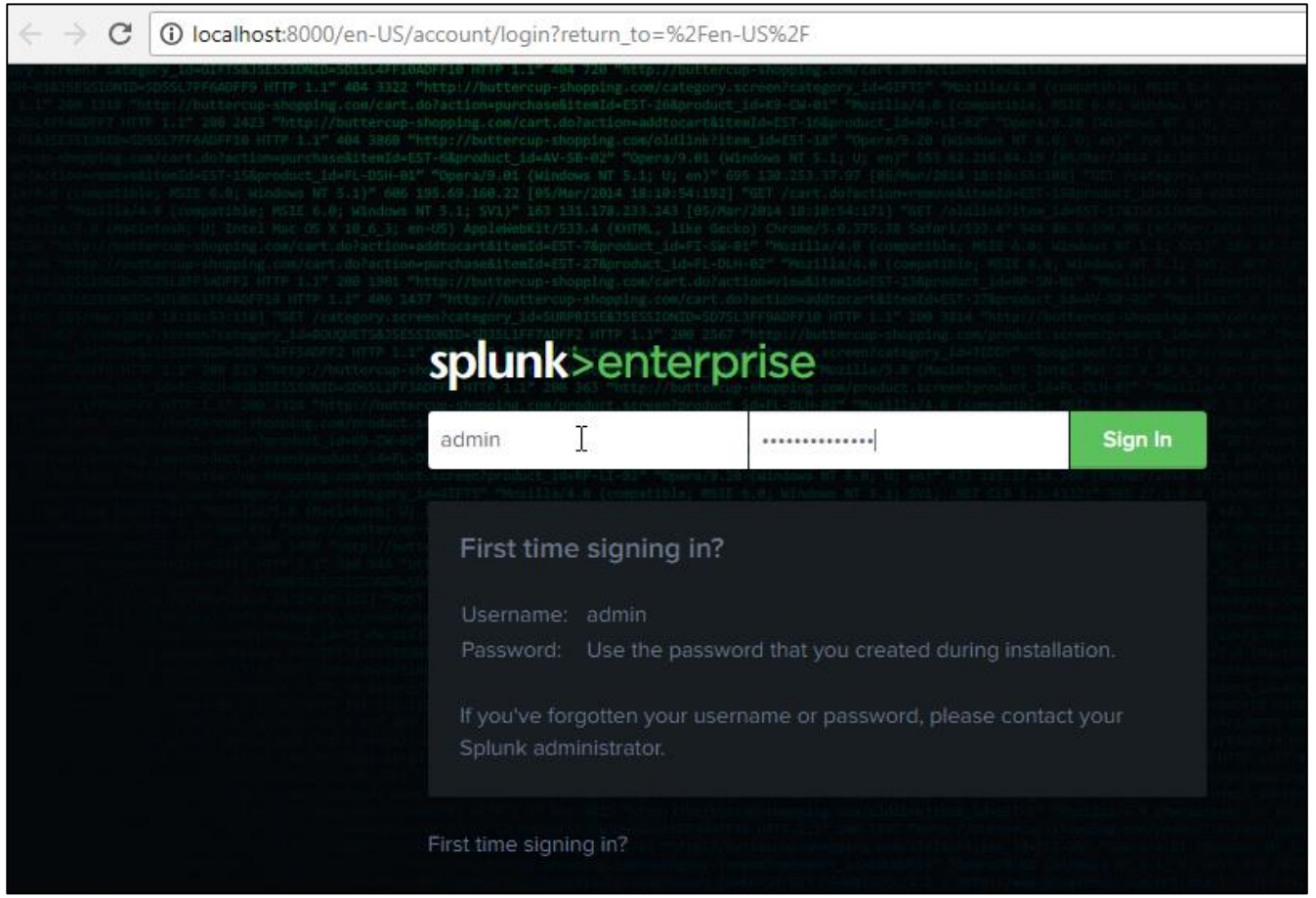
SPLUNK


Secure | https://www.splunk.com/en_us/download/splunk-enterprise.html
splunk>
PRODUCTS
SOLUTIONS
CUSTOMERS
PARTNERS
RESOURCES
ABOUT US
Free Splunk
enterprise-scale deployments.
Choose Your Installation Package
Windows
Linux
Mac OS
64-bit
Windows 8.1, and 10
Windows Server 2012, 2012 R2, and 2016
.msi
168.78 MB
Download Now
32-bit
Windows 8.1 and 10
.msi
150.54 MB
Download Now
Release Notes | System Requirements | Older Releases | All Other Downloads

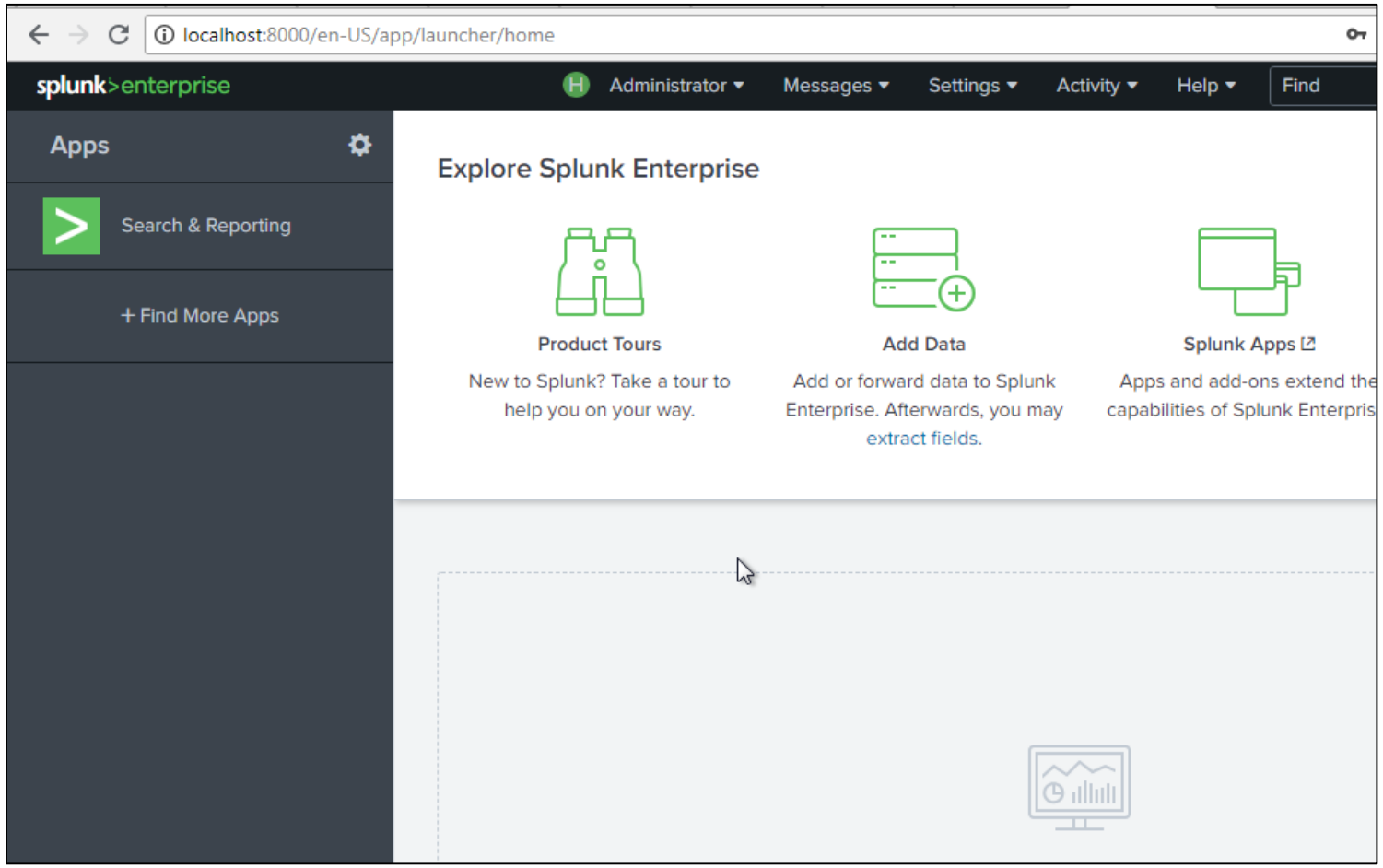
SPLUNK INSTALLATION WINDOWS



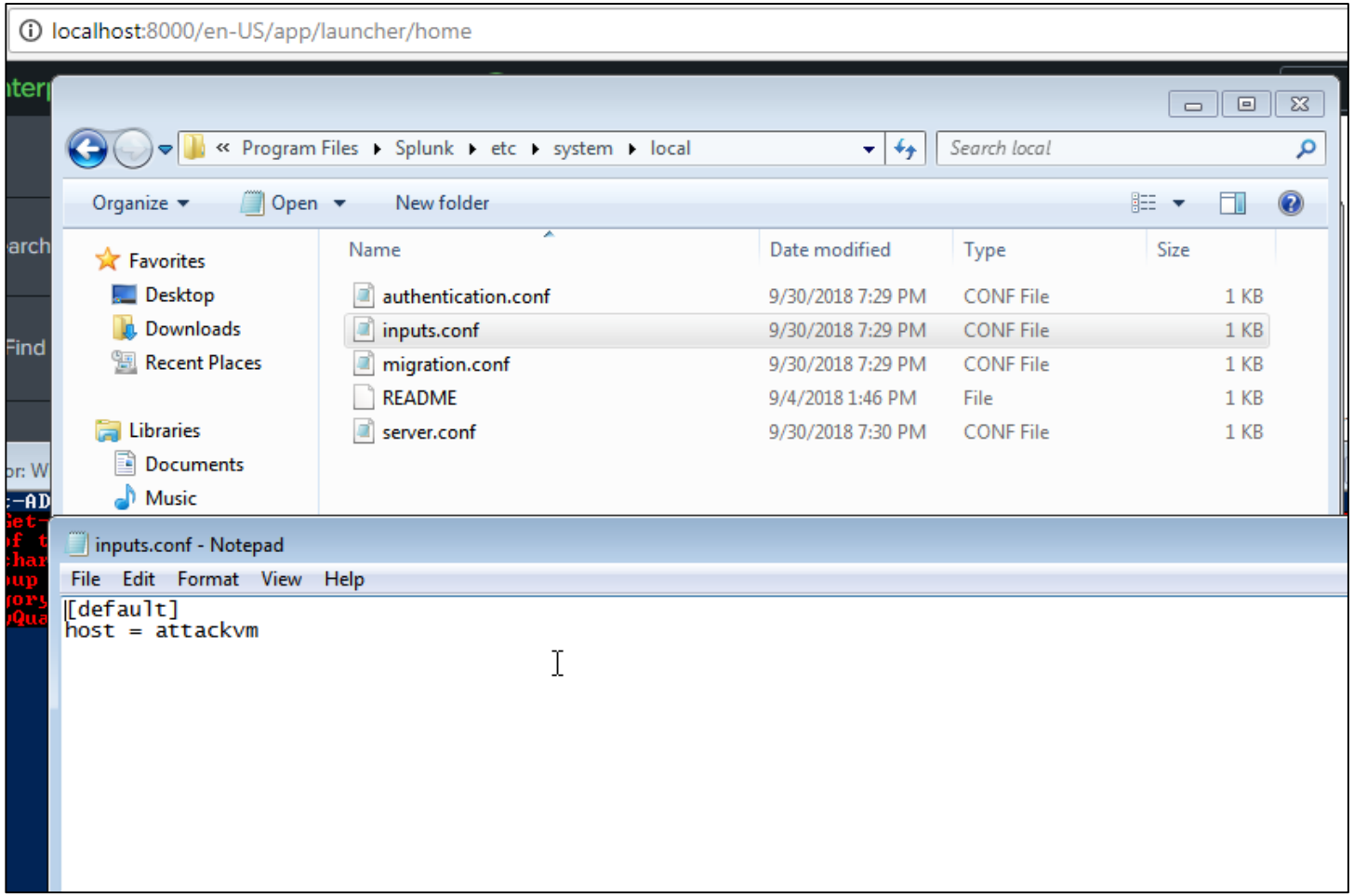
SPLUNK SERVER DASHBOARD



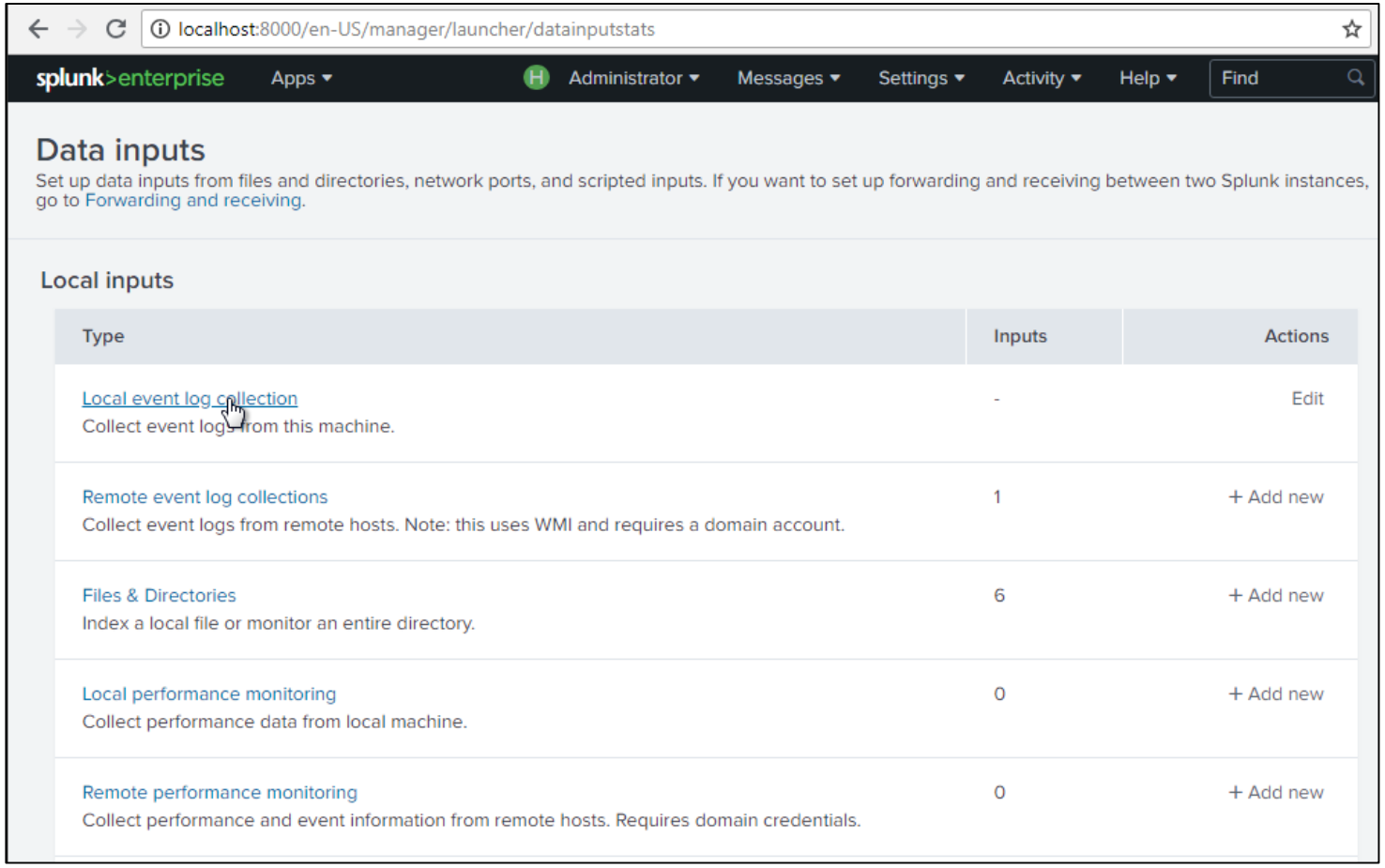
SPLUNK DASHBOARD



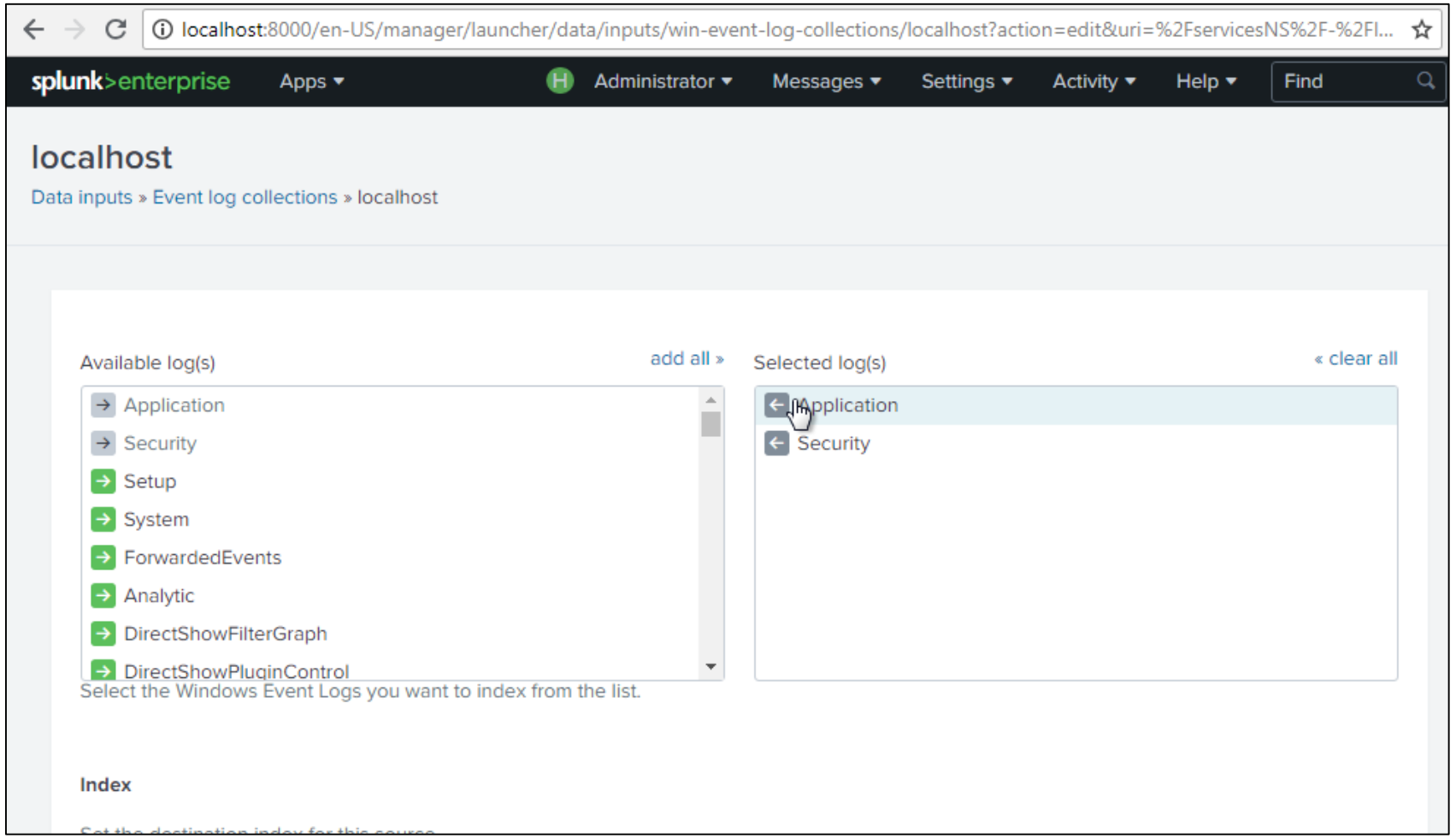
SPLUNK – GETTING INPUT DATA



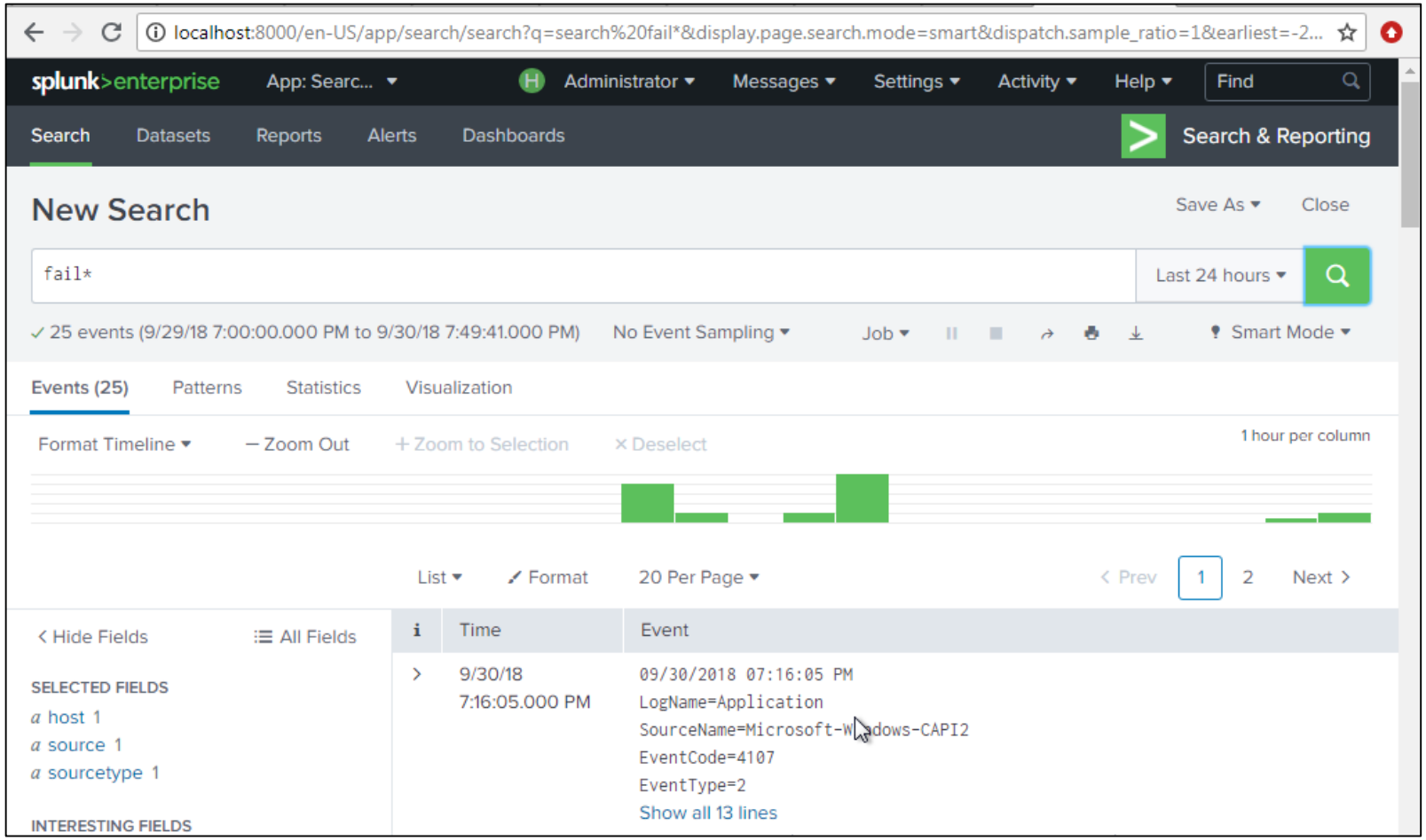
SPLUNK GETTING DATA



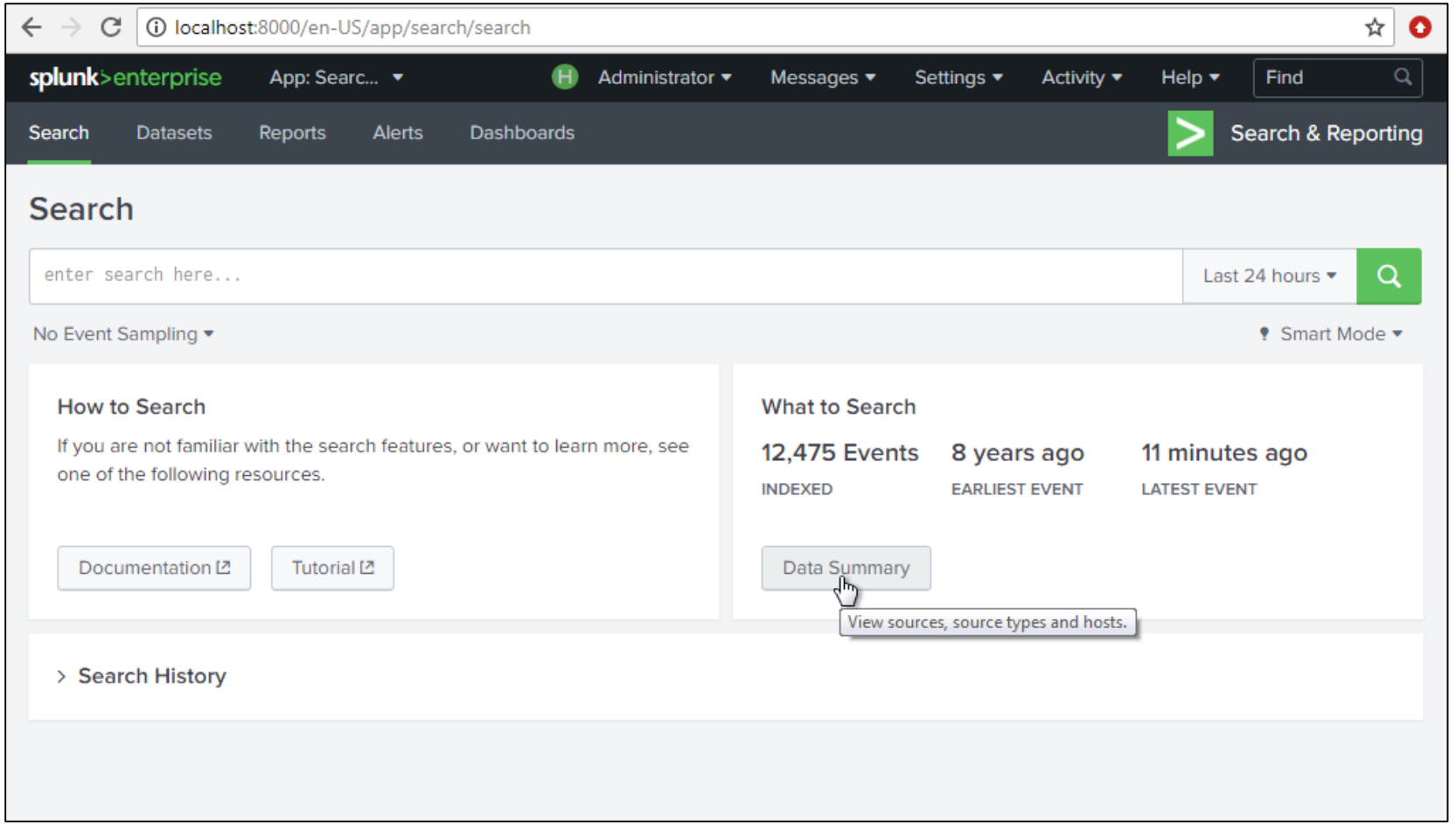
SPLUNK GETTING DATA



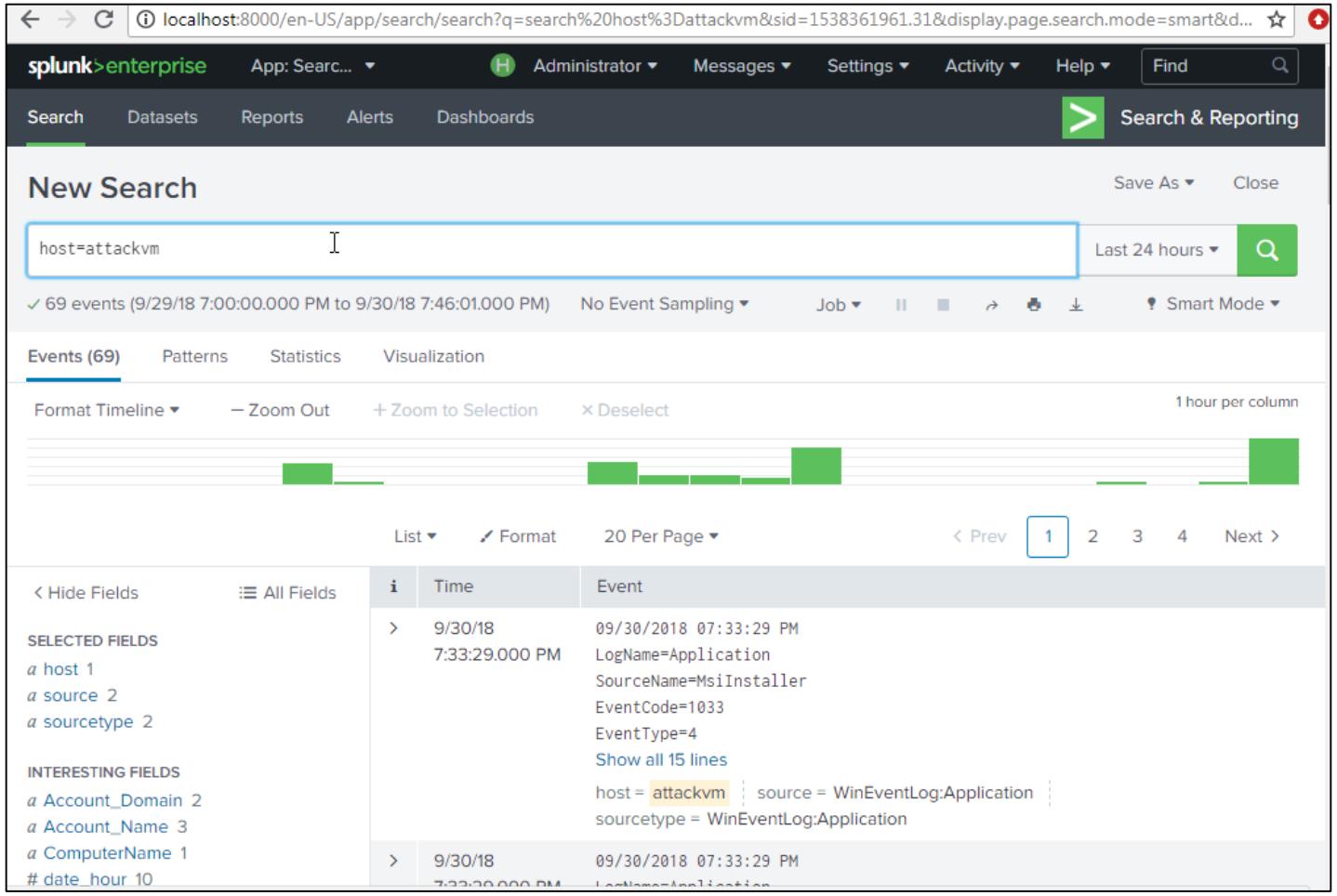
SPLUNK FAIL EVENTS



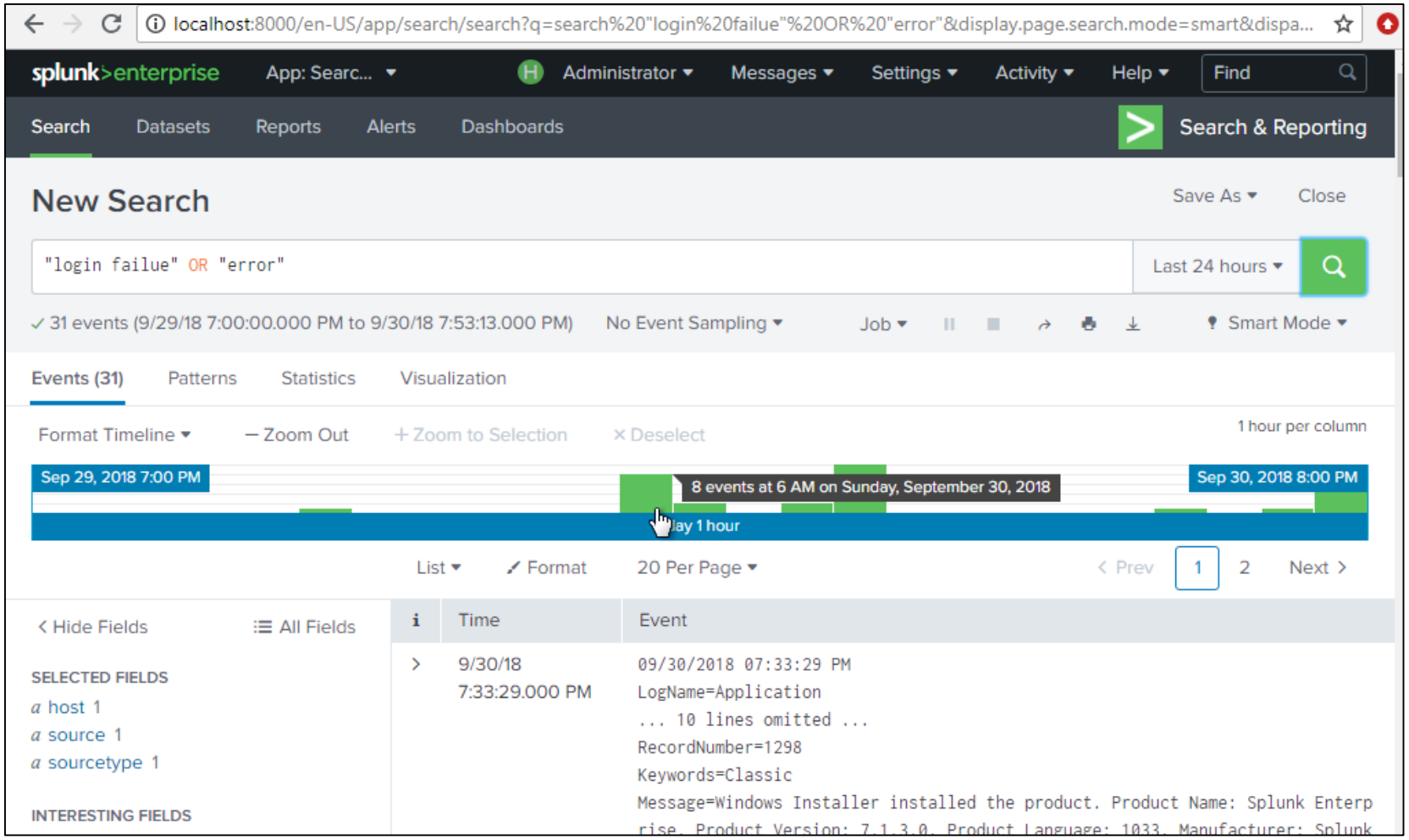
SPLUNK INDEXED DATA



SPLUNK SEARCH

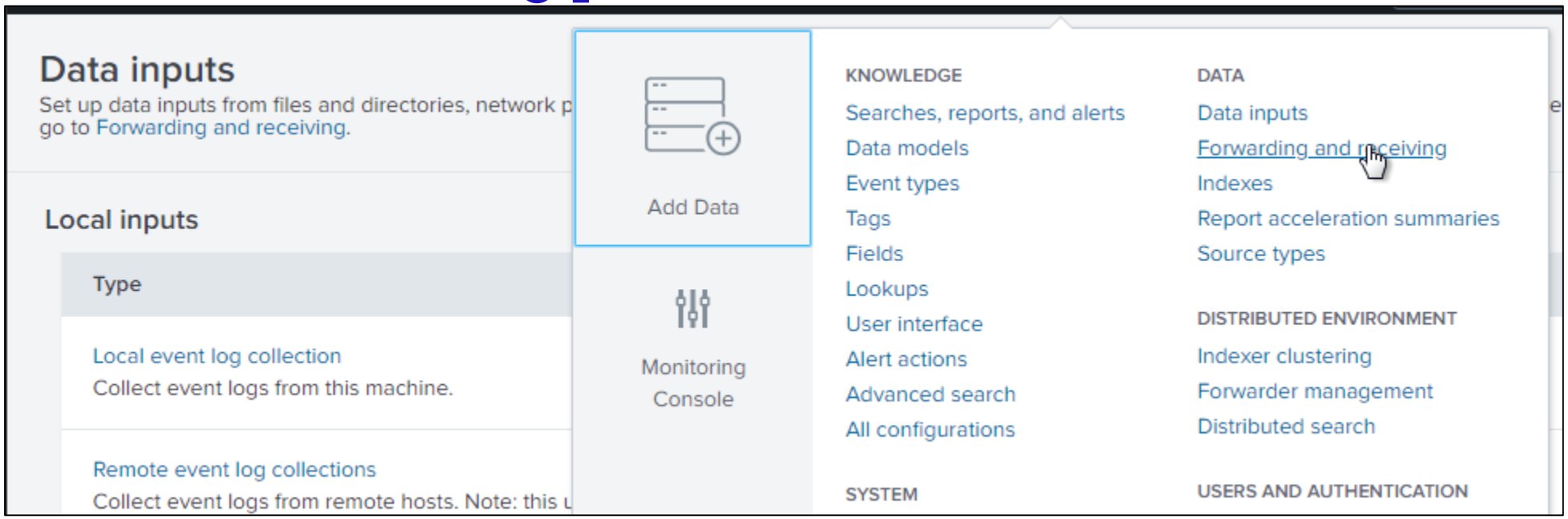


SPLUNK SEARCH QUERIES



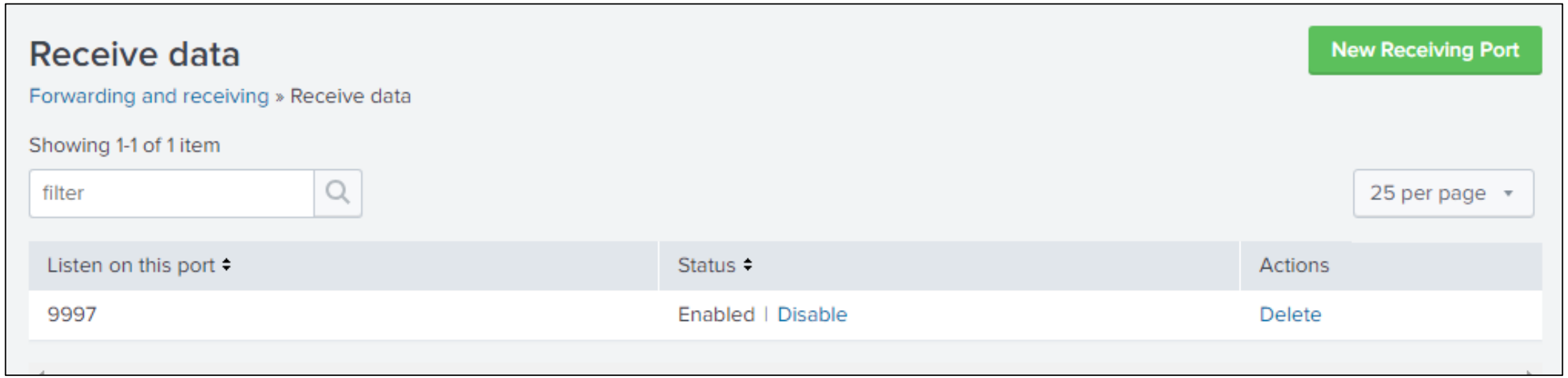
SPLUNK RECEIVED PORT

- Add new receiving port

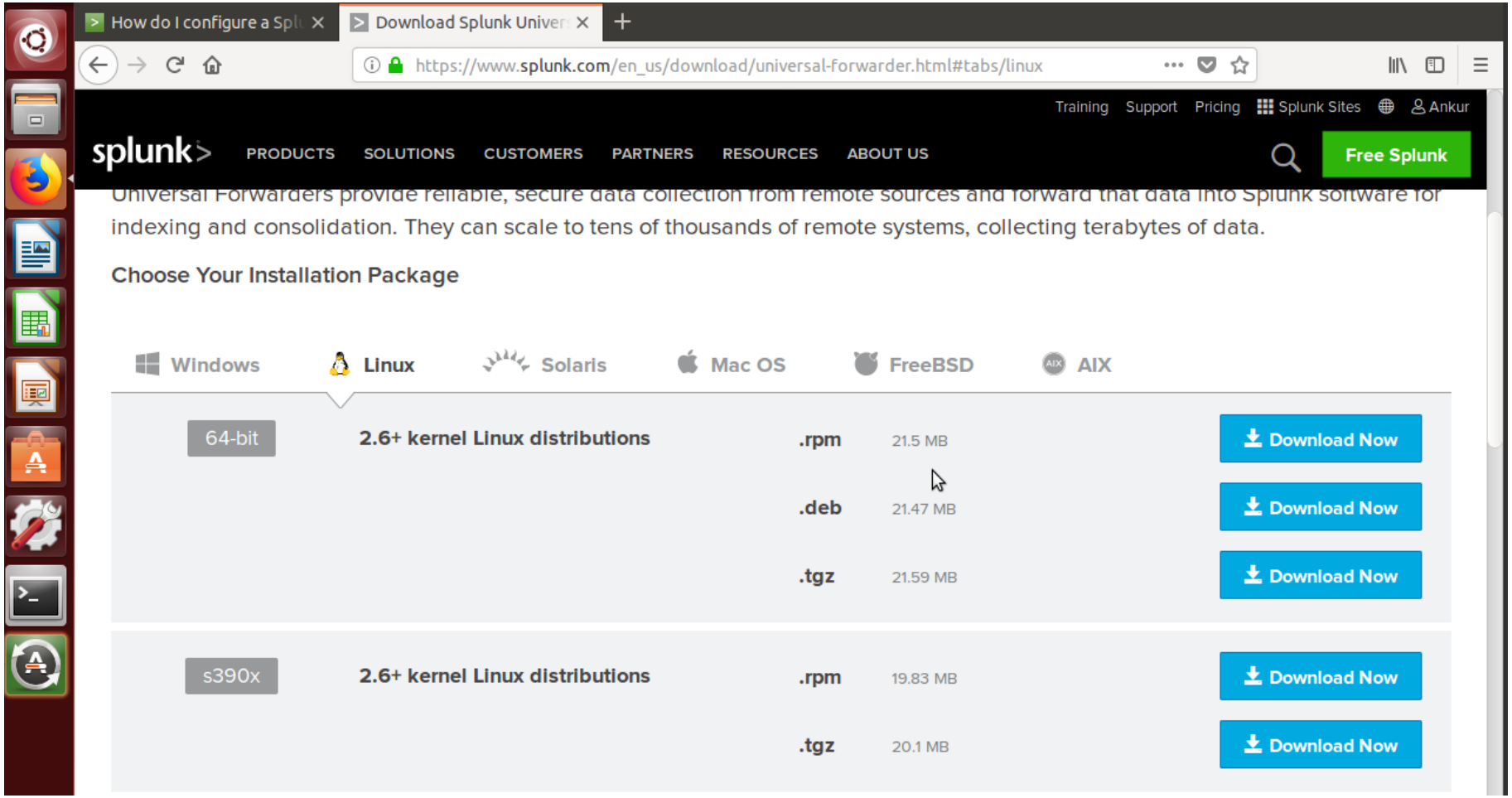


SPLUNK RECEIVING PORT

- Forwarding and Receiving -> Configure Receiving -> New Receiving Port



SPLUNK UNIVERSAL FORWARDER (CLIENT)



SPLUNK UNIVERSAL FORWARDER

- Download the Universal Forwarder
- Install using appropriate package (Windows/ Linux)

```
splunkforwarder-7.1.3-51d9cac7b837-linux-2.6-amd64.deb
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i splunkforwarder-7.1.3-51d9cac7b837-linux
-2.6-amd64.deb
[sudo] password for ubuntu:
Selecting previously unselected package splunkforwarder.
(Reading database ... 80%
```

- $sudo /opt/splunkforwarder/bin/splunk enable boot-start

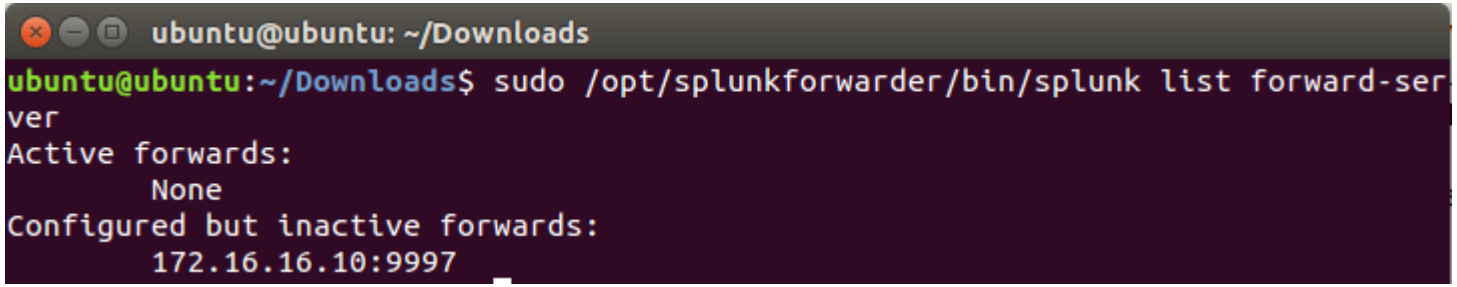
```
Please enter a new password:
Please confirm new password:
 Adding system startup for /etc/init.d/splunk ...
   /etc/rc0.d/K20splunk -> ../init.d/splunk
   /etc/rc1.d/K20splunk -> ../init.d/splunk
   /etc/rc6.d/K20splunk -> ../init.d/splunk
   /etc/rc2.d/S20splunk -> ../init.d/splunk
   /etc/rc3.d/S20splunk -> ../init.d/splunk
   /etc/rc4.d/S20splunk -> ../init.d/splunk
   /etc/rc5.d/S20splunk -> ../init.d/splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
```


SPLUNK UNIVERSAL FORWARDER

- Add server IP and Port on the client

```
ubuntu@ubuntu:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk add forward-serv
er 172.16.16.10:9997
Added forwarding to: 172.16.16.10:9997.
```

- $ sudo vim /opt/splunkfowarder/etc/system/local/output.conf
- $ sudo /opt/splunkforwarder/bin/splunk list forward-server



SPLUNK FORWARDER START

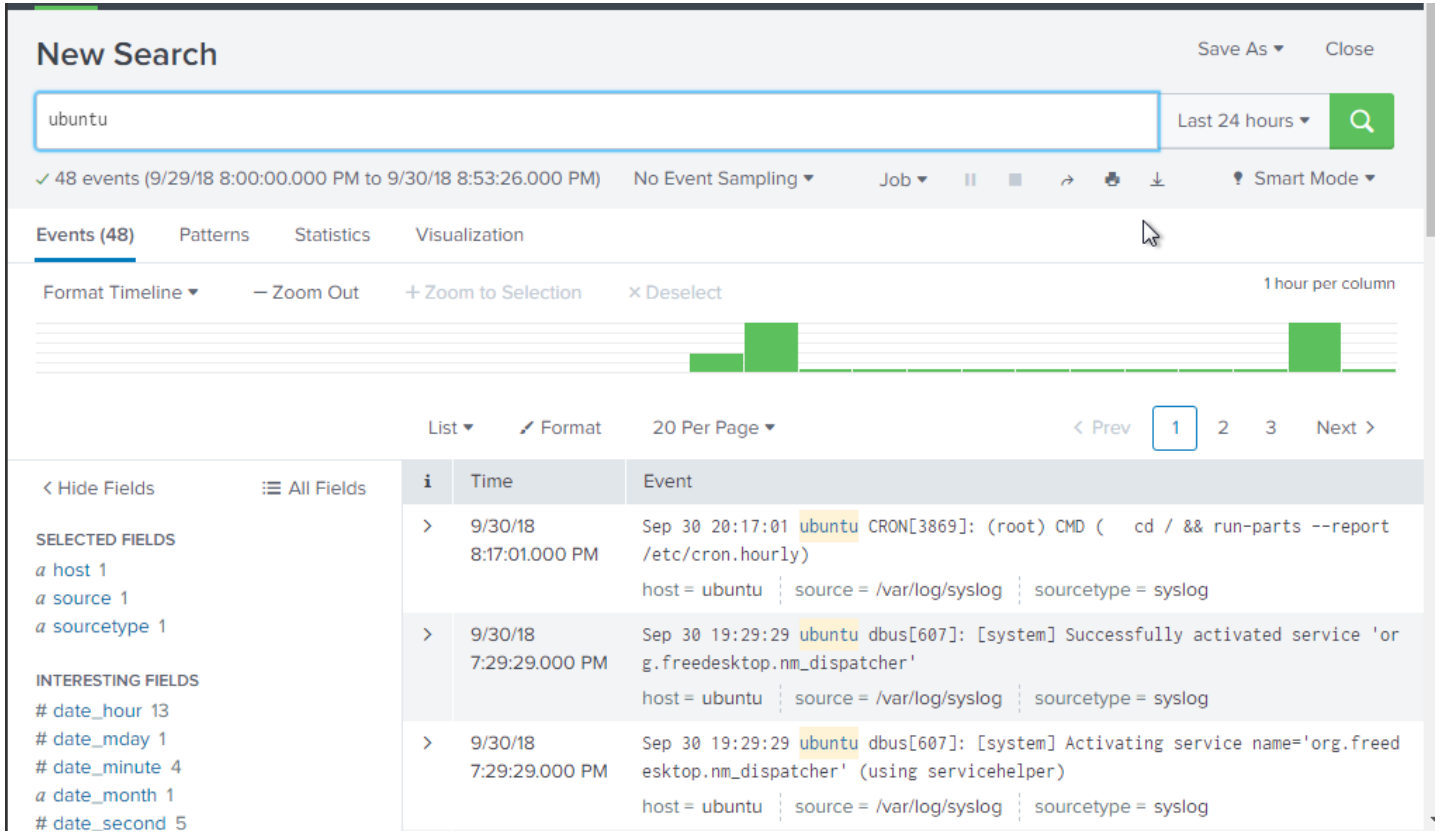
- $sudo /opt/splunkforwarder/bin/splunk start

```
ubuntu@ubuntu:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk list forward-s
ver
Splunk username: admin
Password:
Active forwards:
        172.16.16.10:9997
Configured but inactive forwards:
        None
```

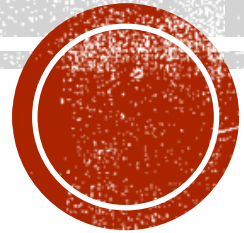
- Add monitor
- $sudo /opt/splunkforwarder/bin/splunk add monitor –index splunk-main
- $sudo cat /opt/splunkforwarder/etc/apps/search/local/inputs.conf

```
ubuntu@ubuntu:~/Downloads$ sudo /opt/splunkforwarder/bin/splunk add monitor /va
/log/auth.log -index linux-main
Added monitor of '/var/log/auth.log'.
ubuntu@ubuntu:~/Downloads$ sudo cat /opt/splunkforwarder/etc/apps/search/local/
nputs.conf
[monitor:///var/log/auth.log]
disabled = false
index = linux-main
ubuntu@ubuntu:~/Downloads$ sudo cat /opt/splunkforwarder/etc/apps/search/local/
nputs.conf
```


CHECK FORWARDER DATA ON SPLUNK SERVER



SECURITY AUDITING AND HOST BASED INTRUSION DETECTION



Security Auditing, Host based IDS, Issues with HIDS

SECURITY AUDITING

- Corporate network is means of information sharing and communication.
- Network faces attacks everyday.
- Company needs to be aware of unauthorized access and take preventive measures to deal with threats.

SECURITY AUDITING

- Evaluation of information system of a company to measure how well it conforms to established criteria.
- Audit comprise of assessment of system's physical configuration, environment, information handling procedures, etc.
- Audits help determine compliance in wake of legislative acts e.g- HIPAA.

SECURITY AUDIT TYPES

Self Audits / Informal Audits

- Applications to monitor and report security incidents and events.
- Centralized log collection to prepare reports and graphs based on alerts.

IT Audit / Formal Audits

- Independent IT department to perform risk assessment and security compliance checks
- Directed test cases towards server and environment.

BASIC SECURITY AUDITING

- ✓Physical Security
- ✓Account Security
- ✓File System Security
- ✓Authenticated User Group

LOCAL SECURITY POLICIES

- ✓ Password Policies
- ✓ Account Lockout Policies
- ✓ Audit Policies
- ✓ User Right Assignment
- ✓ Security Options

OTHER SECURITY AUDIT CONSIDERATIONS

- Default Shares
- Services
- Ports
- Modems
- Security Event Logging
- Logon Warning

OTHER SECURITY AUDIT CONSIDERATIONS

- Backups
- Disable display of last user logon name
- Test Security Settings
- Anonymous Access to registry report

HOST BASED INTRUSION DETECTION SYSTEM (HIDS)

- HIDS refers to tool that conducts intrusion detection on a single system.
- Reports system configuration and application activity.
- Baselines system host to detect configuration variations, e.g- Cisco ASA, tripwire.

HIDS TYPES

Signature based IDS - Searching network traffic for pattern, malicious sequence. This type of IDS can detect only known signature patterns.

Anomaly based IDS - Baselining the normal system behavior. Security engine dissects and analyses payloads and protocols to understand goal. This type of IDS can be slow and normally produces higher amount of false positives.

AUDITD

✓This tool helps in logging server actions and events.
✓Detects misuse and unauthorized access to server.

AUDITD INSTALLATION AND CONFIGURATION

$sudo yum list audit audit-libs
$sudo nano /etc/audit/auditd.conf
num_logs = 10 #Audit log files on server
max_log_file = 30 #Size in MB
 max_log_file_action = ROTATE #
$ cat /etc/audit/rules.d/audit.rules # Specifies auditing rules

AUDITD TESTING

Logs are generated at
/var/log/audit/audit.log
#Auditing rule (temporary)
sudo auditctl -w /etc/ssh/sshd_config -p rwxa -k
sshconfigchange
#Run command
$ cat /etc/ssh/sshd_config

AUDITD LOGS

- type=SYSCALL msg=audit(1434371271.277:135496): arch=c000003e syscall=2 success=yes exit=3 a0=7fff0054e929 a1=0 a2=1fffffffff0000 a3=7fff0054c390 items=1 ppid=6265 pid=6266 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=113 comm="cat" exe="/usr/bin/cat" key="sshconfigchange"

AUDITD LOG ANALYSIS

- type=SYSCALL
- audit(time_stamp:ID)
- arch=c000003e (hex for x86_64)
- sudo ausyscall 2 -> open
- success=yes # Syscall succeded or failed?

AUDITD LOG ANALYSIS

- ppid=6265 (Parent Process ID)
- auid=1000 (User ID of user who triggered audit message)
- Uid = 0 (User who started the analyzed process)
- Comm # Name of the command that triggered audit message.
- exe="/usr/bin/cat" #Path of coomand that triggered audit message.

AUDITD LOG ANALYSIS

- type=CWD msg=audit(1434371271.277:135496): cwd="/home/sammy"
  - Directory from which auditing message was triggered.
  - E.g.- Syscall was triggered from home directory of user sammy

AUDITD LOG ANALYSIS

type=PATH msg=audit(1434371271.277:135496): item=0
name="/etc/ssh/sshd_config" inode=392210 dev=fd:01
mode=0100600 ouid=0 ogid=0 rdev=00:00
objtype=NORMAL

- PATH # Path that was used to invoke syscall argument.
- msg # Timestamp indicates that all records part of same audit event
- ouid=0 # User ID of object owner

AUSEARCH – SEARCHING AUDITD LOGS

Search today's events

$sudo ausearch -m LOGIN --start today -i

Search by event id

$sudo ausearch -a 27020

Search for events related to a particular file

$sudo ausearch -f /etc/ssh/sshd_config -i

AUDIT REPORTS

$sudo aureport -x --summary # Summary of events
$sudo aureport --failed # Report on failed events
$sudo aureport -f -i # Report of file access with syscalls and usernames.

- Autrace # Used to analyse individual process

TRIPWIRE

$sudo apt-get install tripwire

- Site Key - Protects configuration files. This key can be used across multiple servers.
- Local Key - Protects system binaries, ensures no binary file is run without consent.

TRIPWIRE DATABASE

$sudo twadmin --create-polfile /etc/tripwire/twpol.txt
#Policy file used during installation. Encrypted file will be created in /etc/tripwire corresponding to plaintext file.
$sudo tripwire --init # Initialize tripwire
$sudo sh -c 'tripwire --check | grep Filename > test_results'
#Check results
$sudo tripwire --check #Verify configuration

- Modify policy file to reduce noise and eliminate false positives.

ISSUES WITH HIDS

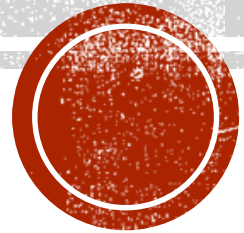
Method	Example
Self Referencing Directories	`/_vti_pvt/./././././administrators.pwd`
Double Slashes	`/_vti_pvt///administrators.pwd`
Reverse Traversal	`/scripts/../_vti_pvt/administrators.pwd`

ISSUES WITH HIDS – SUBSTITUTION ATTACKS

Method	Example
Shell Alias	`#Alias pass='more ''/etc/''passwd'` `#pass`
Environment Variables	`#test=/etc` `#more $test/passwd`

Windows Command-Line Variables	`C:\> set blah=c:\winnt\system32`
	`C:\> set extra=\cmd.exe`
	`C:\> %blah%%extra% /c dir c:`

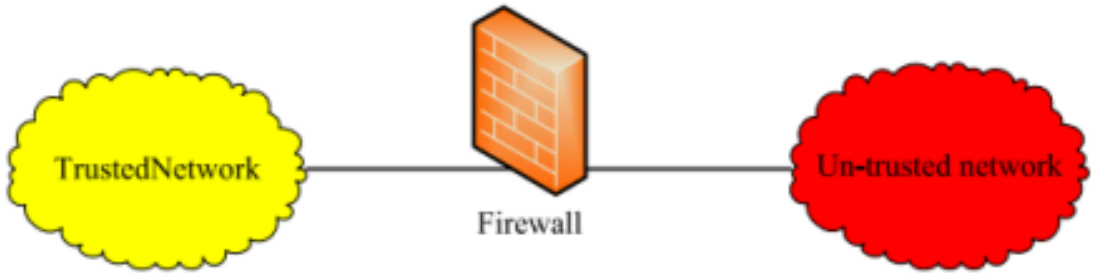
PREVENTIVE TECHNIQUES



Firewalls, Intrusion Prevention

WHAT IS A FIREWALL?

- A component or set of components that **restricts access** between a protected network and the Internet, or between other sets of networks.



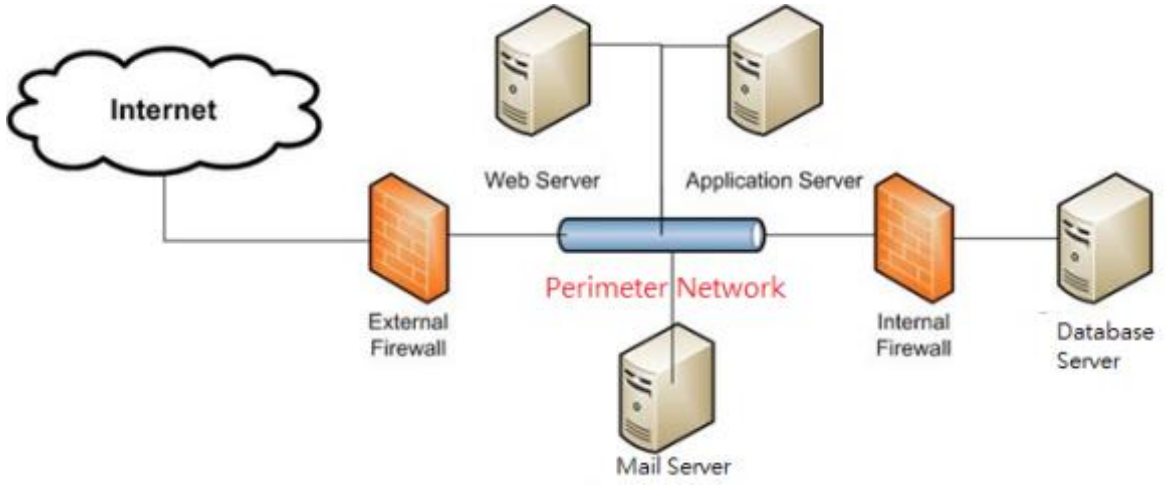
- A **choke point** to control and monitor incoming/outgoing traffic.

WHAT IS A FIREWALL?

- Interconnects networks with differing trust.
- Imposes restrictions on network services
  - only authorized traffic is allowed.
- **Auditing** and controlling access.
- Provides **perimeter defense.**

PERIMETER NETWORK

- A network added between a protected network and an external network, in order to **provide an additional layer of security**.
- A perimeter network is sometimes called a **DMZ** (De-Militarized Zone).

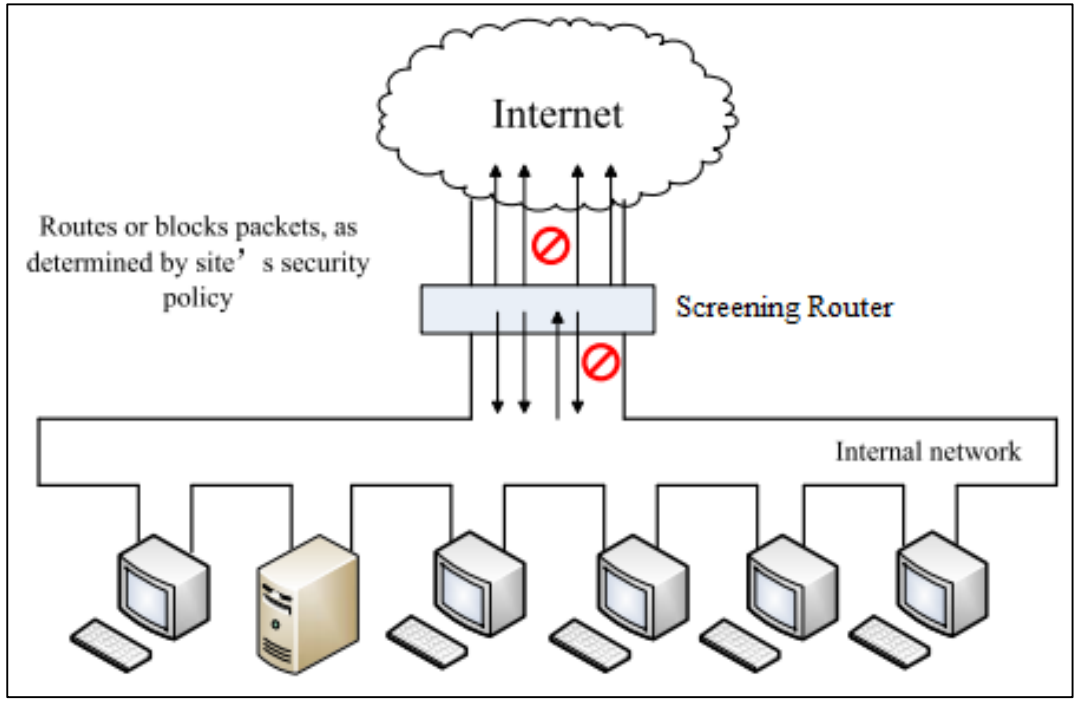


FIREWALL ARCHITECTURE

- Single-Box Architecture
  - Screening Router
  - Dual-Homed Host
  - Multiple-Purpose Boxes
- Screened Host Architecture
- Screened Subnet Architecture

SCREENING ROUTER

- ***Screening Router***: the type of router used in a packet filtering firewall.
- ***Packet filtering***: selectively routes packets between internal and external hosts according to rules that reflect the organization's network security policy.
- The screening router passes/rejects an packet based on information contained on the ***packet's header*** (IP addresses and TCP/UDP ports).

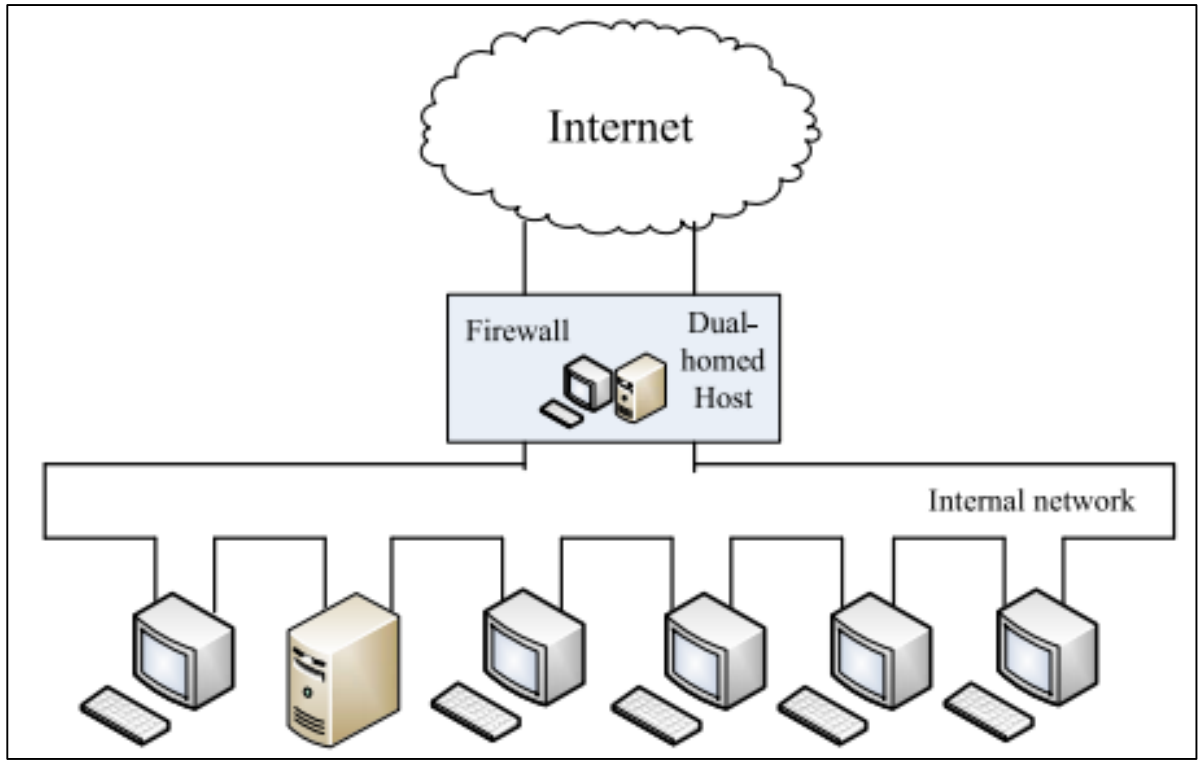


DISADVANTAGE OF SCREENING ROUTER

- A little or no logging capability
  - difficult for an administrator to determine whether the router has been compromised or is under attack.
- Packet filtering rules are difficult to test thoroughly
  - may leave a site open to untested vulnerabilities.
- Complex filtering rules may become unmanageable
- Only take care of transport and network layers

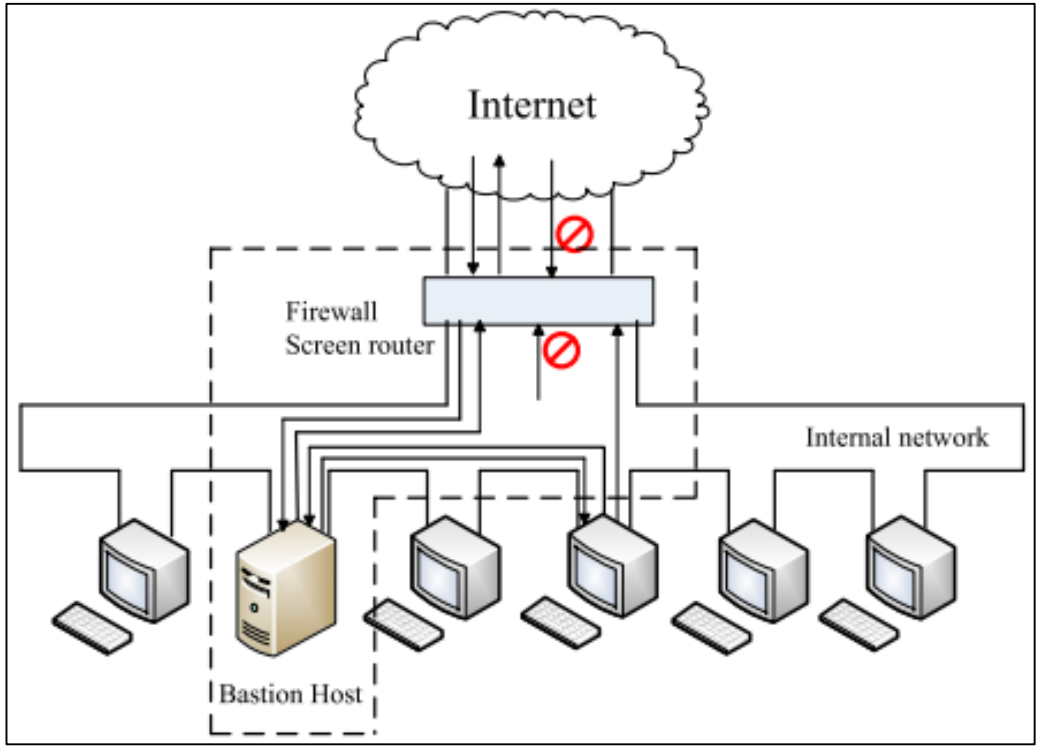
DUAL HOMED HOST

- ***Dual-homed host*** : a computer with at least two network interfaces.
- It could act as a router, but usually the routing functions are disabled.
  - No external packets can reach to the internal network
- It can only provide services by **proxying** them, or by having users log into the dual-homed host directly.
  - Major issue: user accounts



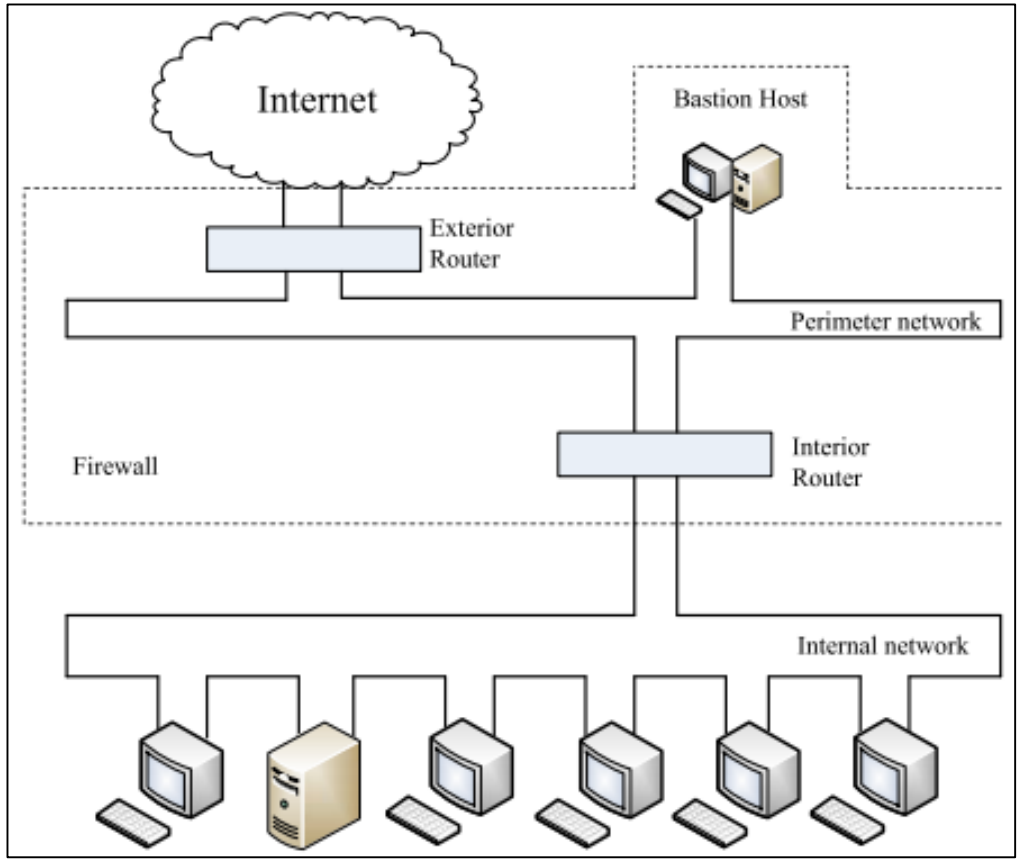
SCREENED HOST ARCHITECTURE

- Two major components:
  - ***Screening router*** provides packet filtering functions
  - ***Bastion host*** is the only system on the internal network that allows the connection from Internet.
- The bastion host thus needs to maintain a high level of host security.



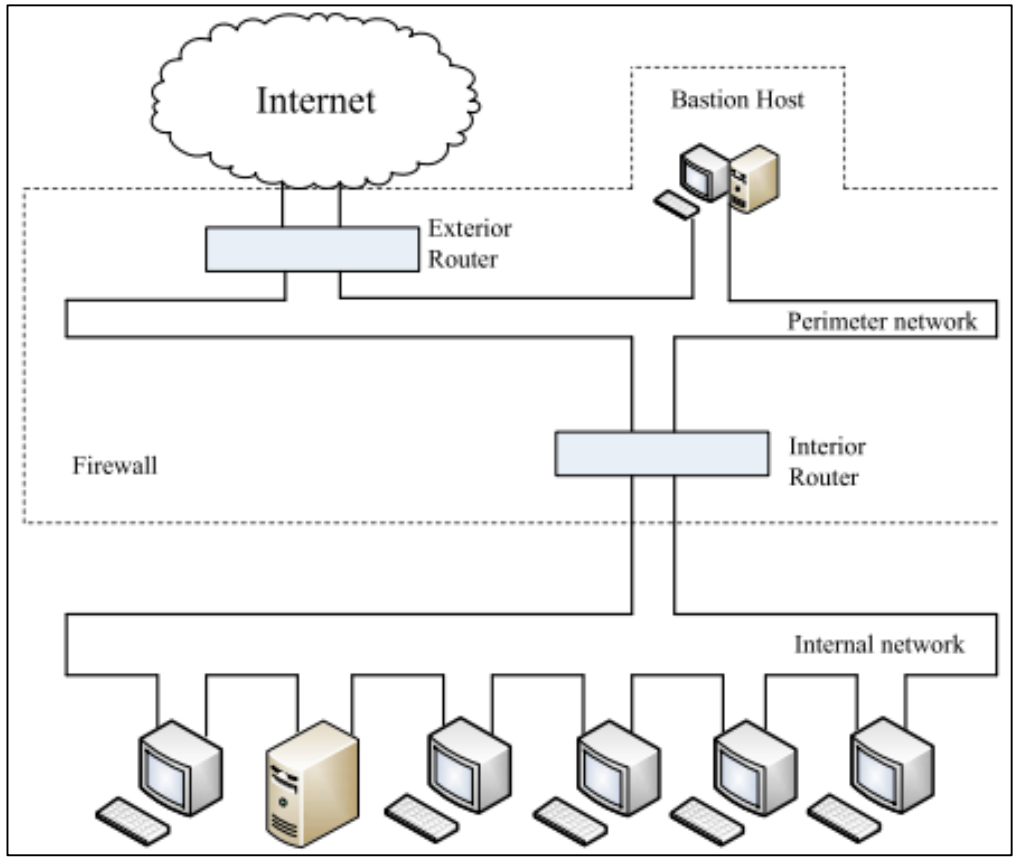
SCREENED SUBNET ARCHITECTURE

- Screened Subnet: adding a perimeter network (DMZ) that further isolates the internal network from the Internet.
  - Move the bastion host (the most tempting target) to the DMZ.
    - To handle incoming traffic, such as email, FTP, DNS query, and Web request
    - act as a proxy server to allow internal clients to access external servers indirectly.



INTERIOR ROUTER VS EXTERIOR ROUTER

- The exterior router (access router)
  - tend to allow almost anything outbound from the perimeter net, and the generally do very little packet filtering.
  - Special rules to protect the hosts on the perimeter net.
- The interior router (choke router) does most of the packet
  - It allows selected services from the internal to the Internet. These services can safely support and safely provide using packet filtering rather than proxies.



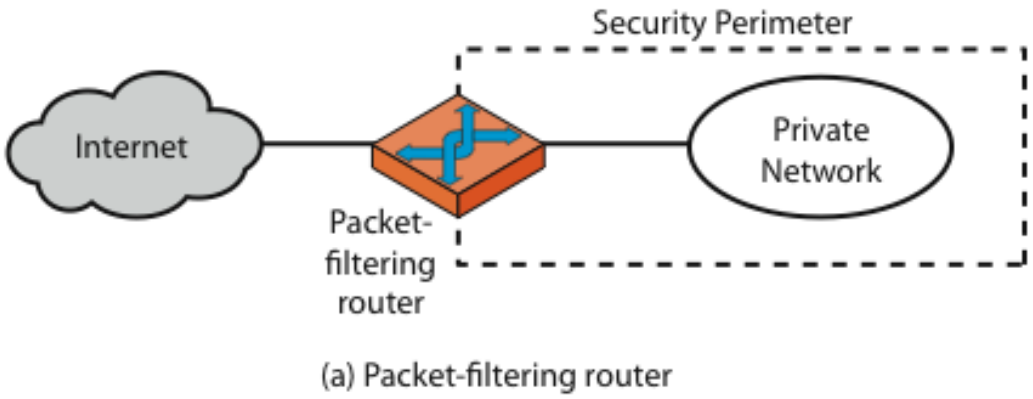
FIREWALL TYPES

Characterized by **protocol level** it controls in

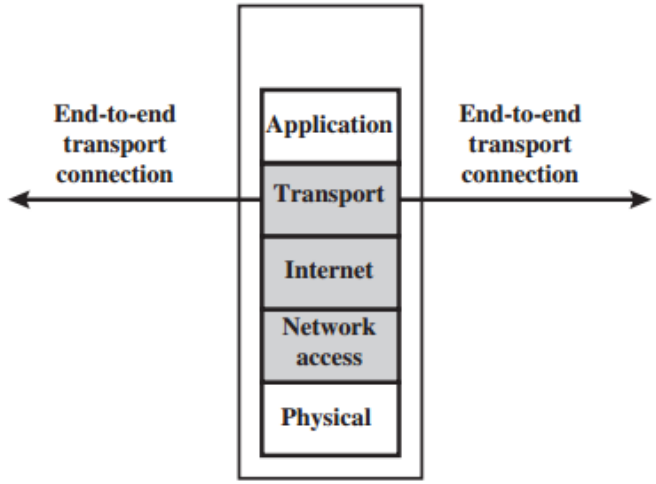
- Packet filters
- Circuit gateways
- Application gateways
- Dynamic packet filters

PACKET FILTERING FIREWALL

- Packet filtering is generally accomplished using Access Control Lists (ACL) on routers or switches and are normally very fast.



(a) Packet-filtering router



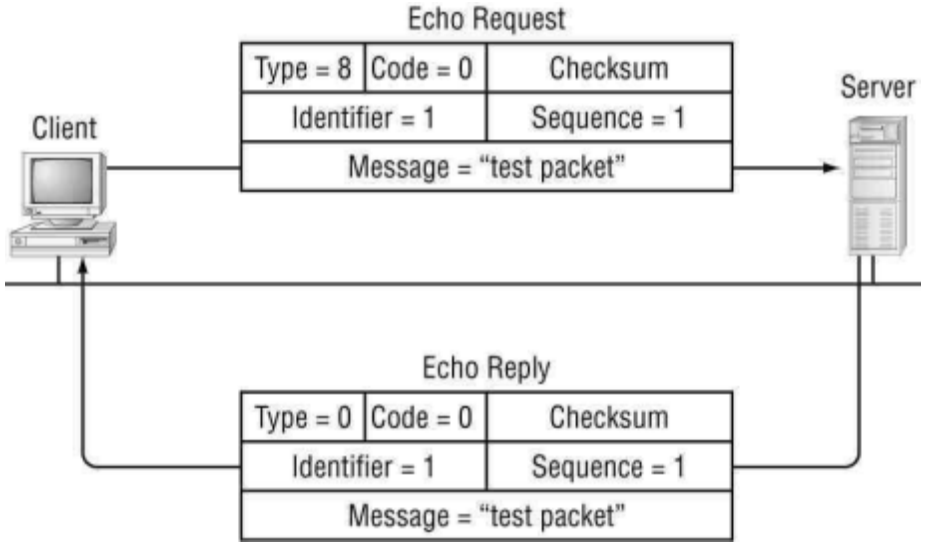
PACKET FILTERING FIREWALL

- Simplest, fastest firewall component
- Uses transport-layer information only (no context)
  - IP Source Address, Destination Address
  - Protocol/Next Header (TCP, UDP, ICMP, etc)
  - TCP or UDP source & destination ports
  - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
  - ICMP message type
- Permit or deny according to rules
- Possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

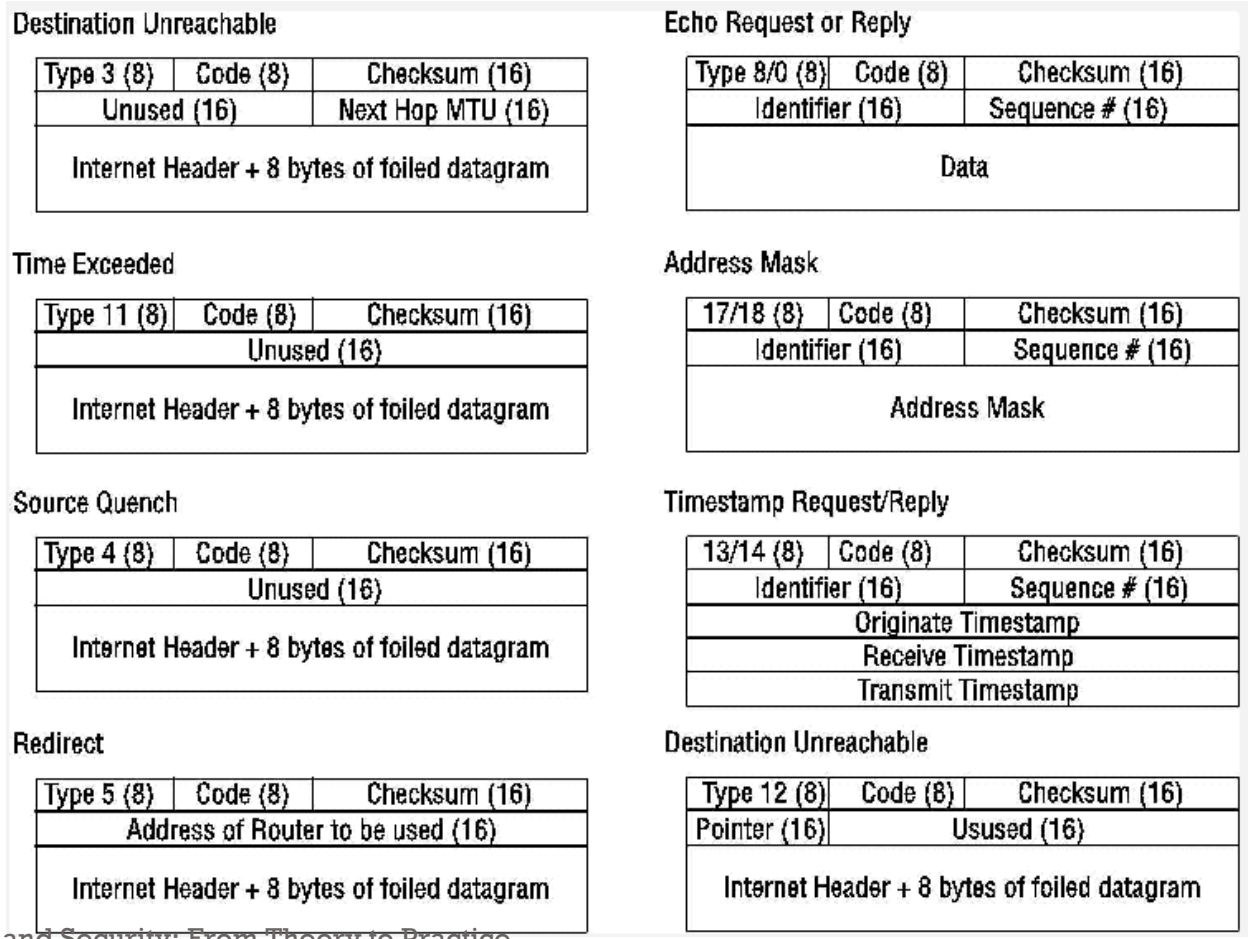
ICMP PACKET

- Internet Control Message Protocol
  - are typically used for diagnostic or control purposes or generated in response to errors in IP operations.
- Two major types used to Ping
  - Echo Request (8)
  - Echo Reply (0)

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0 ()
    Checksum: 0x525c [correct]
    Identifier: 0x0200
    Sequence number: 256 (0x0100)
    Data (32 bytes)
```



ICMP PACKET


Destination Unreachable
Type 3 (8)
Code (8)
Checksum (16)
Unused (16)
Next Hop MTU (16)
Internet Header + 8 bytes of foiled datagram
Echo Request or Reply
Type 8/0 (8)
Code (8)
Checksum (16)
Identifier (16)
Sequence # (16)
Data
Time Exceeded
Type 11 (8)
Code (8)
Checksum (16)
Unused (16)
Internet Header + 8 bytes of foiled datagram
Address Mask
17/18 (8)
Code (8)
Checksum (16)
Identifier (16)
Sequence # (16)
Address Mask
Source Quench
Type 4 (8)
Code (8)
Checksum (16)
Unused (16)
Internet Header + 8 bytes of foiled datagram
Timestamp Request/Reply
13/14 (8)
Code (8)
Checksum (16)
Identifier (16)
Sequence # (16)
Originate Timestamp
Receive Timestamp
Transmit Timestamp
Redirect
Type 5 (8)
Code (8)
Checksum (16)
Address of Router to be used (16)
Internet Header + 8 bytes of foiled datagram
Destination Unreachable
Type 12 (8)
Code (8)
Checksum (16)
Pointer (16)
Ususd (16)
Internet Header + 8 bytes of foiled datagram

USAGE OF PACKET FILTER

- Filtering with incoming or outgoing interfaces
  - E.g., Ingress filtering of spoofed IP addresses
  - Egress filtering
- Permits or denies certain services
  - Requires intimate knowledge of TCP and UDP port utilization on a number of operating systems

CONFIGURATION OF PACKET FILTER

- Start with a security policy
- Specify allowable packets in terms of logical expressions on packet fields
- Rewrite expressions in syntax supported by your vendor
- General rules - least privilege
  - All that is not expressly permitted is prohibited
  - If you do not need it, eliminate it

PROBLEMS WITH STATELESS FIREWALL

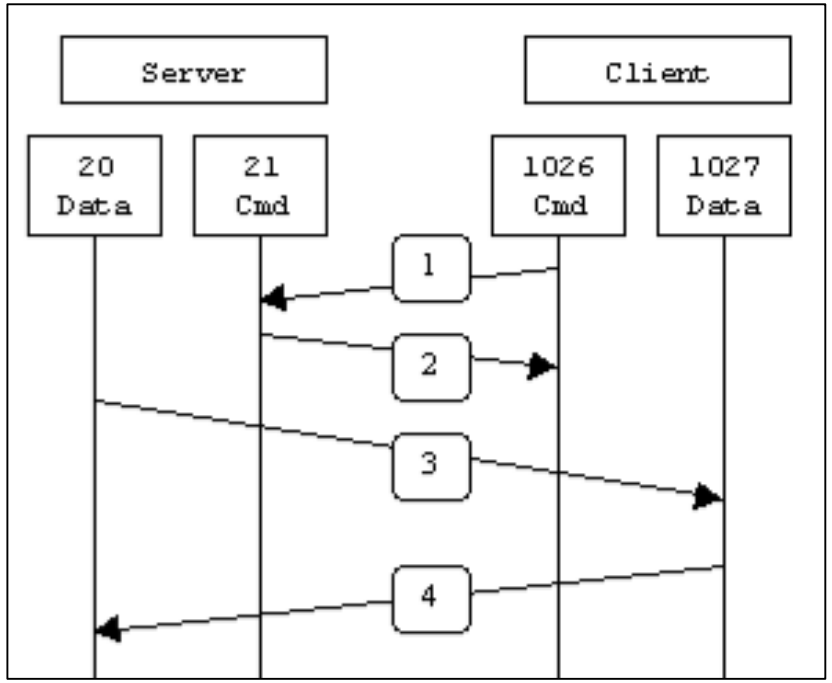
- Our defined restriction is based solely on the outside host's port number, which we have no way of controlling.
- Now an enemy can access any internal machines and port by originating his call from port 25 on the outside machine.
- What can be a better solution ?

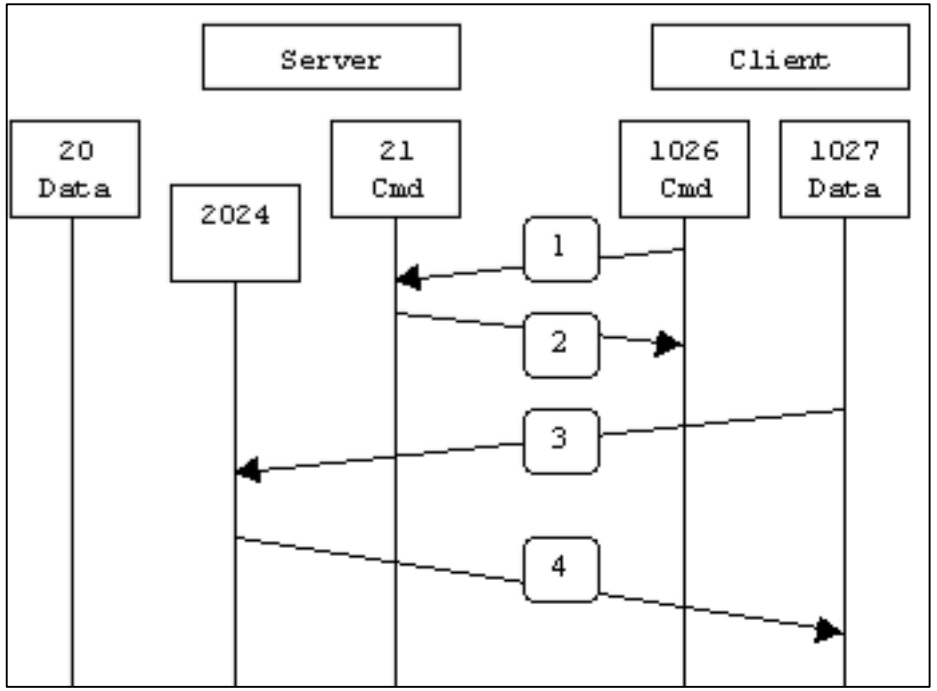
PROBLEMS OF STATELESS FIREWALL

- The ACK signifies that the packet is part of an ongoing conversation
- Packets without the ACK are connection establishment messages, which we are only permitting from internal hosts
  - Thus, we need to remember the established connection from inside to outside, i.e., maintain the states → stateful firewalls

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		*our packets to their SMTP port*
allow	*	25	*	*	ACK	*their replies*

ACTIVE VS PASSIVE FTP



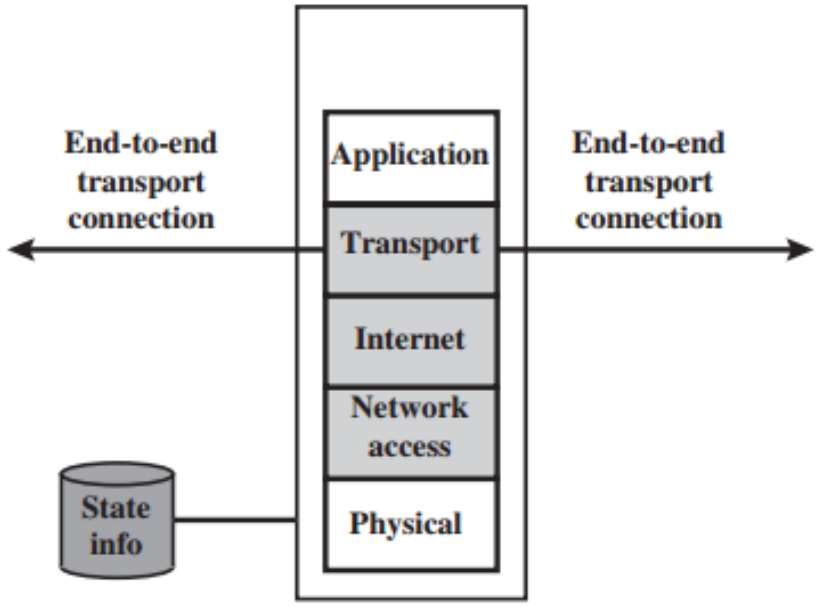


ATTACKS ON PACKET FILTERS

- IP address spoofing
  - Fake source address to be trusted
  - Solution: add filters on router to block
- Tiny fragment attacks
  - Split TCP header info over several tiny packets
  - Solution: either discard or reassemble before check
- Source routing attacks
  - attacker sets a route other than default
  - block source routed packets

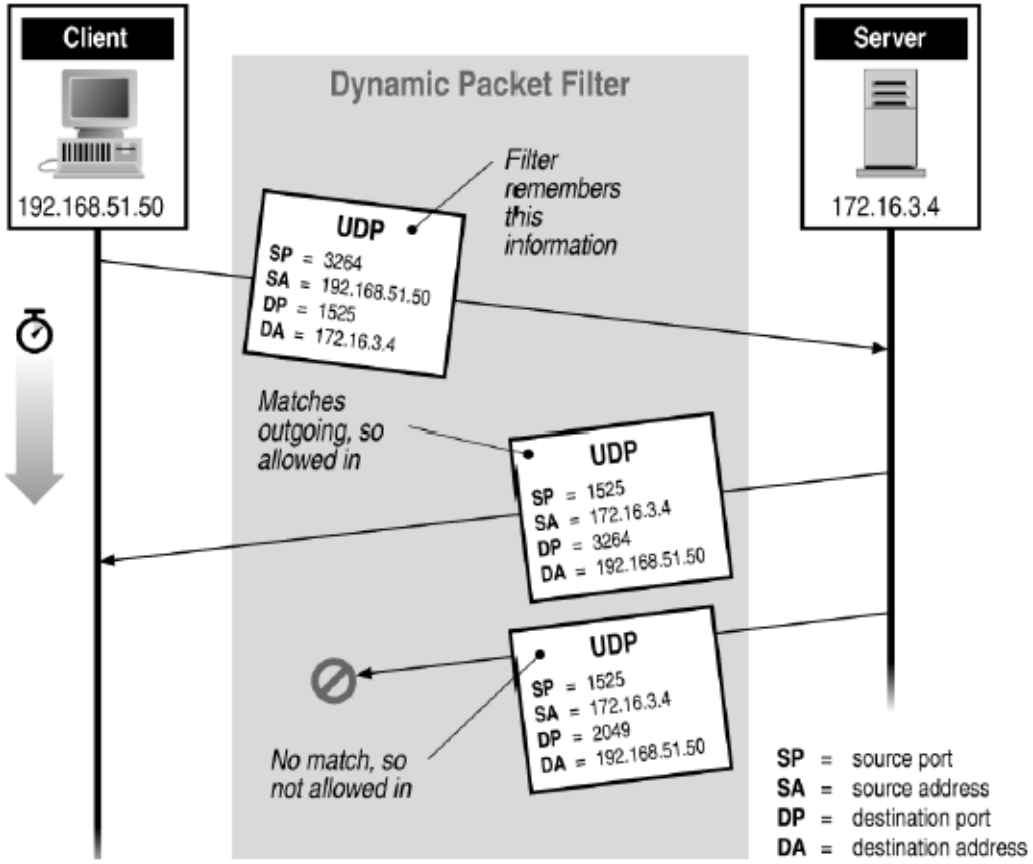
STATEFUL PACKET FILTERS (IPTABLES)

- Traditional packet filters do not examine higher layer context
  - i.e., matching return packets with outgoing flow
- They examine each IP packet in context
  - Keep track of client-server sessions
  - Check each packet validly belongs to one
- Hence are better able to detect bogus packets out of context



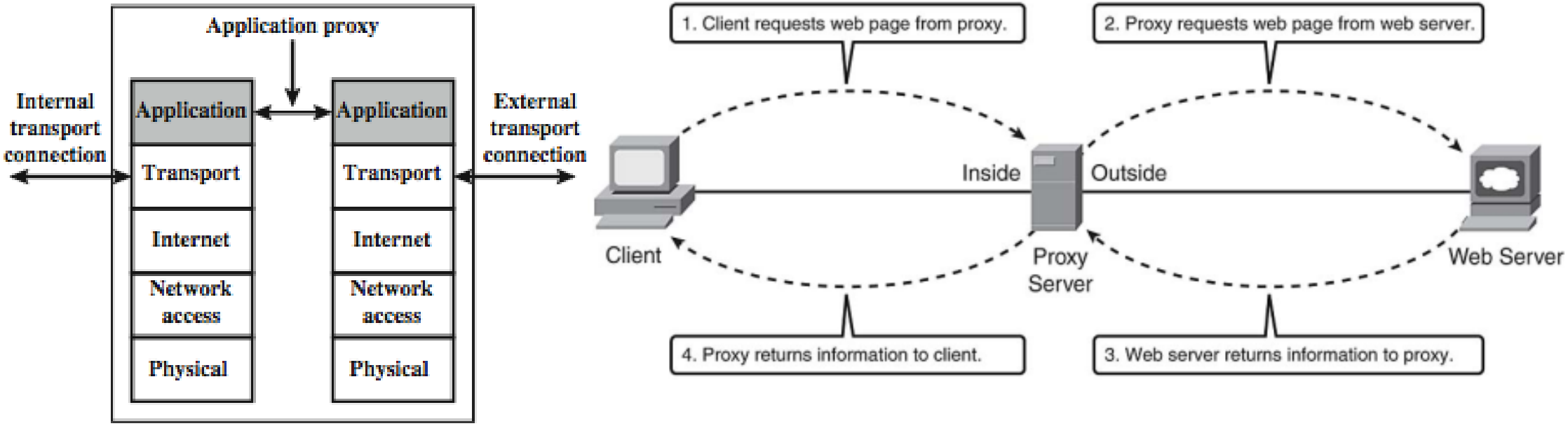
(c) Stateful inspection firewall

STATEFUL FILTERING

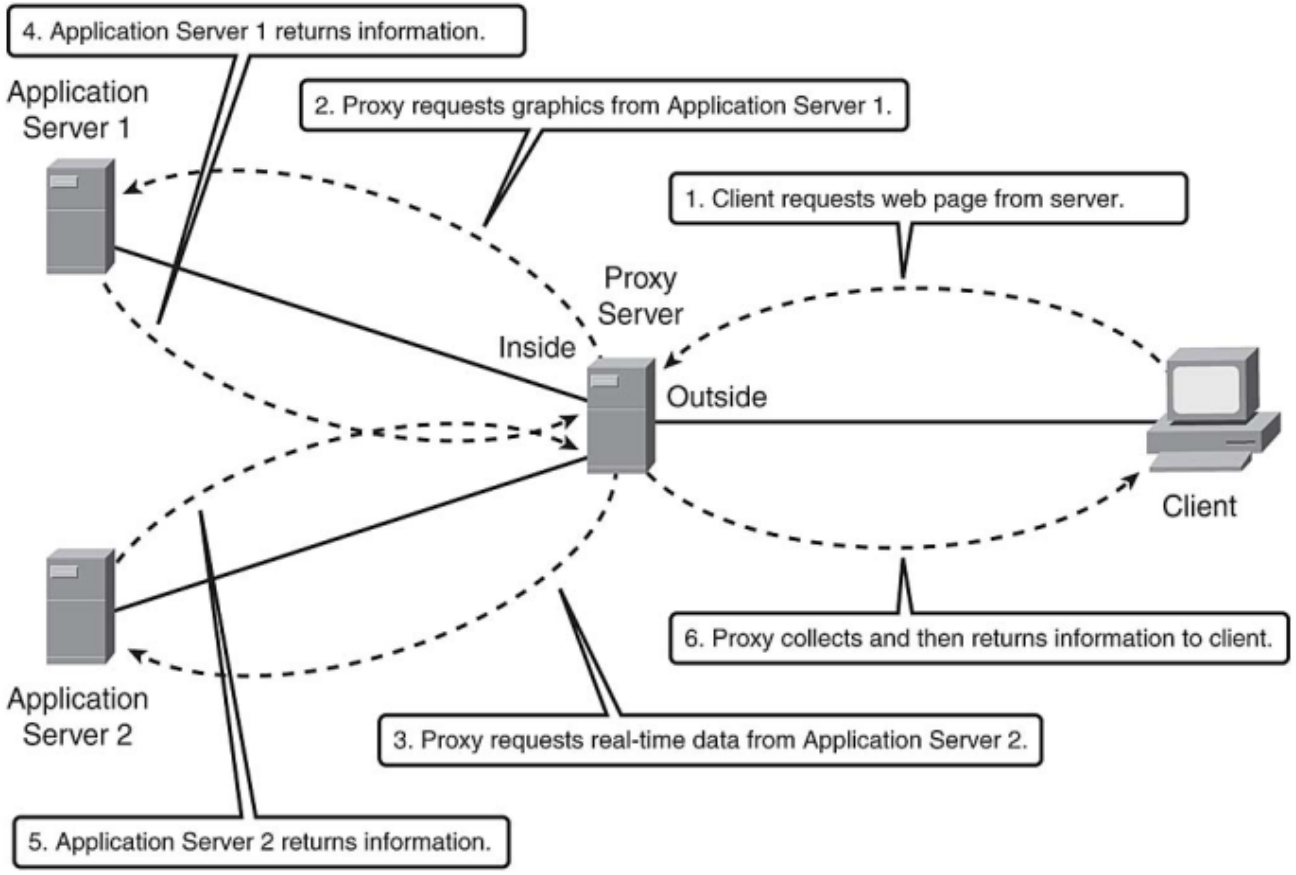


FIREWALL APPLICATION LEVEL GATEWAY (OR PROXY)

- Tailored to application layer protocol, e.g., http, ftp, smtp, etc.



REVERSE PROXY

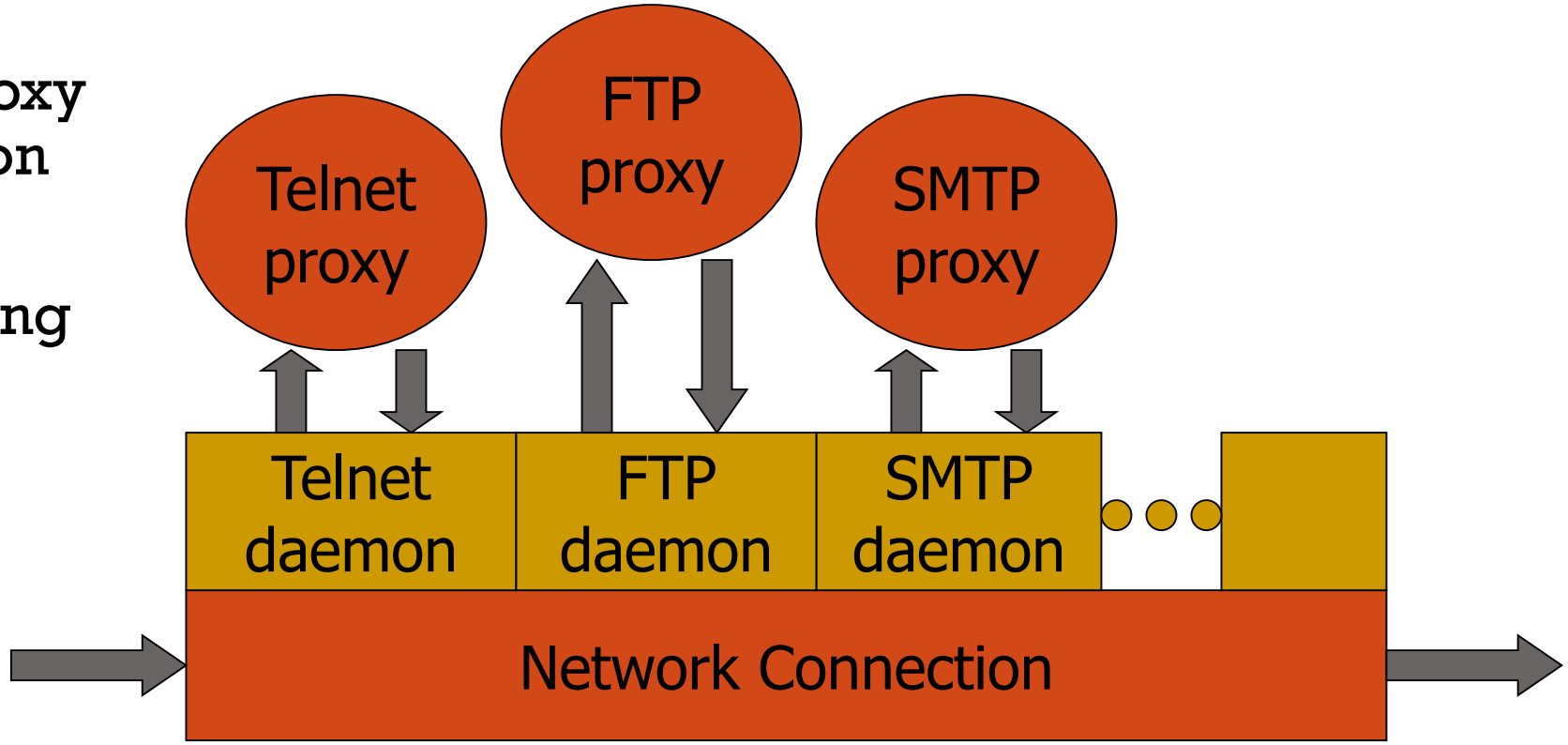


APPLICATION LEVEL FILTERING

- Has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- Need separate proxies for each service
  - E.g., SMTP (E-Mail), NNTP (Net news), DNS (Domain Name System), NTP (Network Time Protocol)
  - custom services generally not supported
- Proxy protects clients from malicious and outside attacks, but also make itself vulnerable to application attacks.

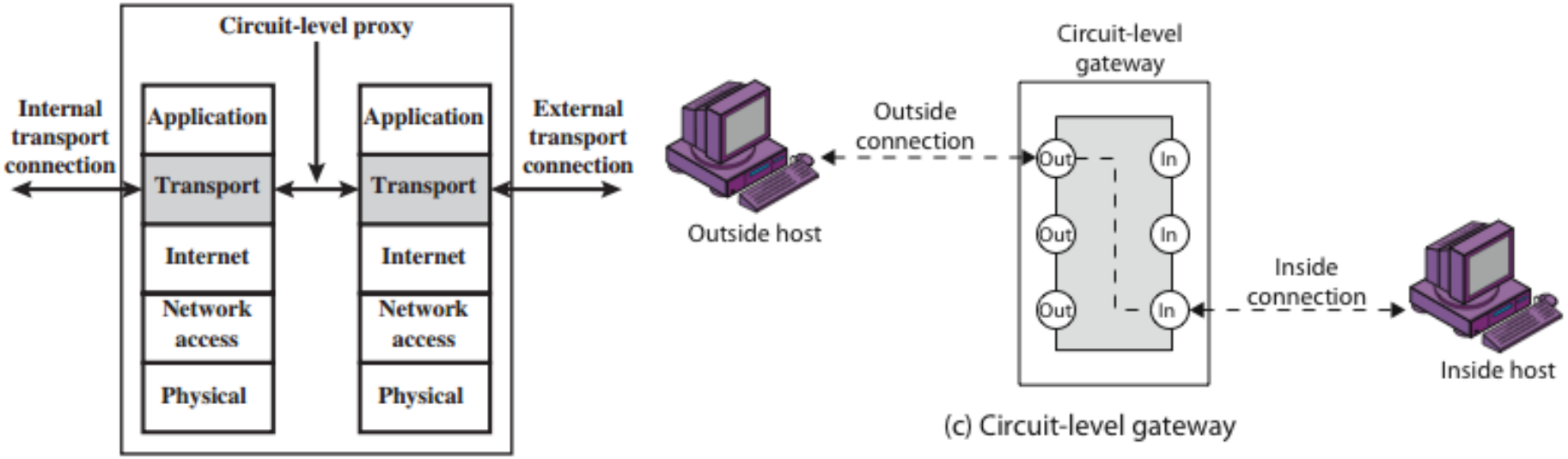
APPLICATION FIREWALL ARCHITECTURE

- Daemon spawns proxy when communication detected …
- Additional processing overhead on each connection.



FIREWALL CIRCUIT LEVEL GATEWAY

- Relay two TCP connections
- Once allowed, it just relays traffic without examining contents
- Typically used for outbound connection from trusted internal users
- SOCKS (socket secure) is commonly used



INTRUSION PREVENTION SYSTEM (IPS)

- IPS often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content.
- Unlike its predecessor the Intrusion Detection System (IDS)—which is a passive system that scans traffic.c and reports back on threats—the IPS is placed inline.
- Some IPS actions include:
  - Sending an alarm to the administrator (as would be seen in an IDS)
  - Dropping the malicious packets
  - Blocking traffic from the source address
  - Resetting the connection

SNORT NIPS CONFIGURATION

- To configure snort to run as Network Intrusion Prevention System NIPS
  - sudo apt-get install libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev libnfnetlink0 -y
  - go to ~/snort_src/cd daq-2.0.06
  - Run ./configure --enable-nfq-module=yes
- Make && sudo make install

SNORT NIPS CONFIGURATION

- at line 168, add the following lines:
  - config daq: nfq
  - config daq_mode: inline
  - config daq_var: queue=0
- Set up iptables to forward packets to snort inline mode:
  - Iptables –A FORWARD –j NFGUEUE --queue-num=0
- Now run snort again to drop the ping packets:
  - sudo snort –A console –q –c /etc/snort/snort.conf Q

CITE THIS WORK

```
@book{huang2018software,
title={Software-Defined Networking and Security: From Theory to Practice},
author={Huang, Dijiang and Chowdhary, Ankur and Pisharody, Sandeep},
year={2018},
publisher={CRC Press}}
```


REFERENCES

- https://www.sans.org/reading-room/whitepapers/riskmanagement/securing-common-vectors-cyber-attacks-37995
- https://en.wikipedia.org/wiki/Security_information_and_event_management
- http://yallalabs.com/linux/how-to-setup-loganalyzer-with-rsyslog-on-ubuntu-16-04-lts-ubuntu-18-04-lts/
- https://answers.splunk.com/answers/50082/how-do-i-configure-a-splunk-forwarder-on-linux.html
- https://nmap.org/book/man-briefoptions.html
- https://highon.coffee/blog/nmap-cheat-sheet/

REFERENCES

- https://www.upcloud.com/support/installing-snort-on-ubuntu/
- http://www.ubuntu-howtodoit.com/?p=138
- https://snort.org/
- https://www.digitalocean.com/community/tutorials/how-to-use-the-linux-auditing-system-on-centos-7
- http://searchcio.techtarget.com/definition/security-audit
- https://www.sans.org/reading-room/whitepapers/auditing/security-auditing-continuous-process-1150
- https://lifeasageek.github.io/class/cs52700-fall16/slides/mimicry.pdf

REFERENCES

- https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-evasion-attackers-burglar-alarm-1284
- https://www.sans.org/security-resources/idfaq/what-is-a-host-intrusion-detection-system/1/24
- https://www.digitalocean.com/community/tutorials/how-to-use-tripwire-to-detect-server-intrusions-on-an-ubuntu-vps