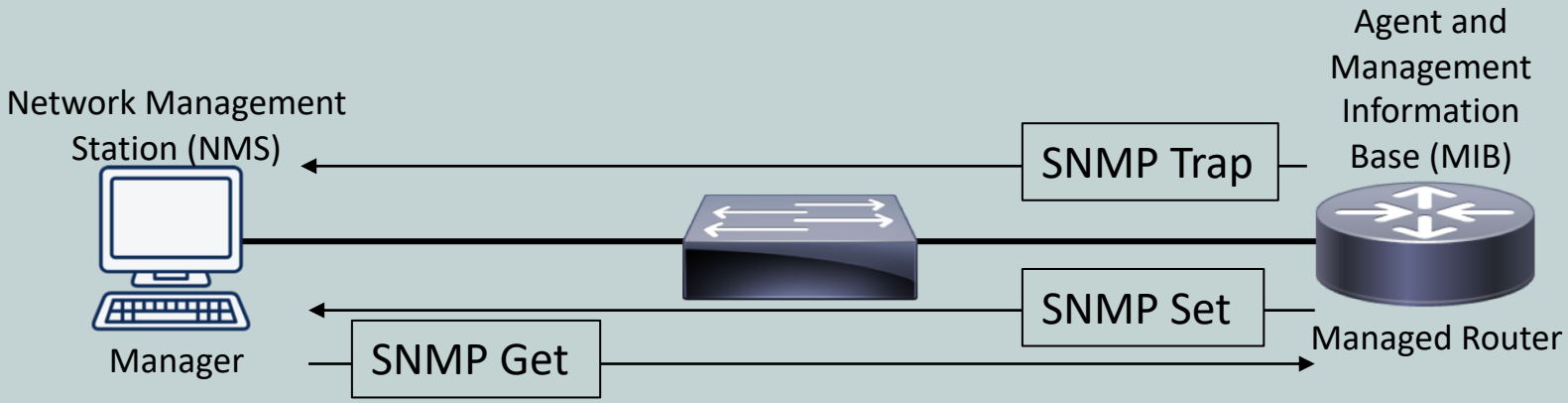
SNMP

CompTIA Network+ (N10-007)

Simple Network Management Protocol (SNMP)

- SNMP manager sends/receives messages to managed devices (routers, switches, servers)
  - SET sends information
  - GET requests information
  - TRAP receives unsolicited information from managed devices



SNMP Versions

- SNMP v1
- SNMP v2
- SNMP v3

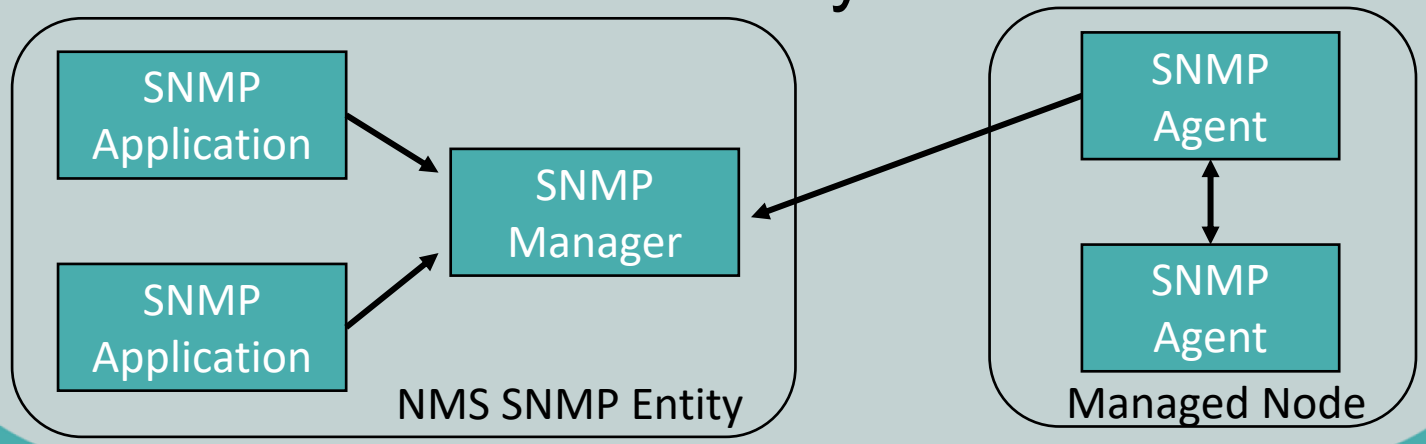
SNMP v1 and v2

- Use community strings to gain access to a device
- Default community strings of public (read-only) or private (read-write) devices are considered a security risk

SNMP v3

- SNMPv3 addressed the weakness of community strings with three enhancements
  - Hashes message before transmitting (integrity)
  - Validates source of message (authentication)
  - DES-56 to provides confidentiality and privacy (encryption)

- SNMPv3 also groups SNMP components as entities to increase security



Network Logging

CompTIA Network+ (N10-007)

Syslog

- Routers, switches, and servers can send their log information to a common syslog server
- Allows administrators to better correlate events and see trends
- Two primary components
  - Syslog servers
    - Receives and stores logs from clients
  - Syslog clients
    - Devices that send log information

Syslog Security Levels

Level	Name	Description
0	Emergencies	The most severe error conditions, which render the system unusable
1	Alerts	Conditions requiring immediate attention
2	Critical	A less-severe condition, as compared to alerts, which should be addressed to prevent an interruption of service
3	Errors	Notifications about error conditions within the system that do not render the system unusable
4	Warnings	Notifications that specific operations failed to complete successfully
5	Notifications	Non-error notifications that alert an administrator about state changes within a system
6	Informational	Detailed information about the normal operation of a system
7	Debugging	Highly detailed information (for example, information about individual packets), which is typically used for troubleshooting purposes

Lowest number is most severe level and logs the most detail

Syslog Structure

Time Stamps

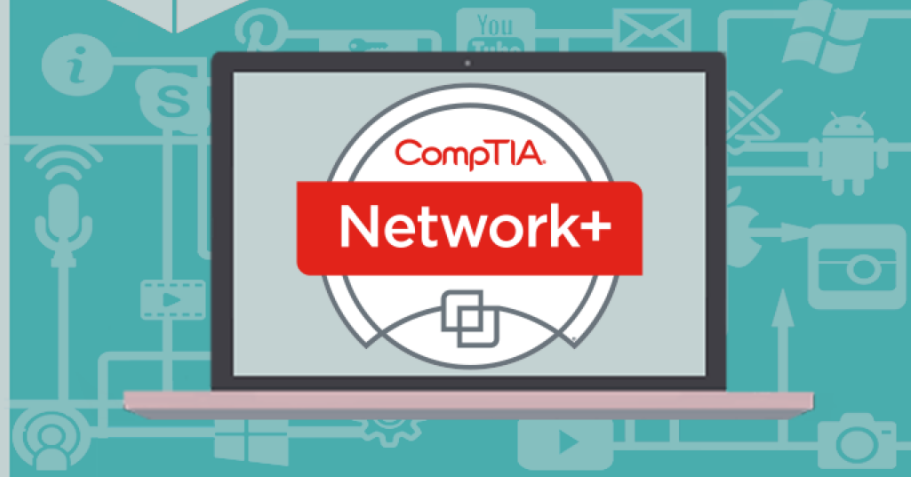
Log Level

Machine or IP

Text of Log Message

Date	Time	Facility	Level	Host Name	Message Text
2016-06-15	17:49:10	Syslog	Alert	qa-che-ayas-01	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:54	Lpr	Emerg	qa-che-ayas-01	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:54	UUCP	Error	10.100.113.136	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:54	System2	Error	10.100.113.136	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:54	Local0	Warning	2001:10:100:112:cd8c:6cf5:2843:7d3c	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:53	Local5	Error	qa-che-ayas-01	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:53	Kernel	Warning	2001:10:100:112:cd8c:6cf5:2843:7d3c	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:53	Local5	Info	qa-che-ayas-01	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:53	System3	Notice	qa-che-ayas-01	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:53	System0	Emerg	qa-che-ayas-01	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:52	System5	Notice	10.100.113.136	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:52	Lpr	Debug	10.100.113.136	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:52	Local2	Error	2001:10:100:112:cd8c:6cf5:2843:7d3c	This is a test message generated by Kiwi Syslog
2016-06-15	17:48:52	Local5	Critical	qa-che-ayas-01	This is a test message generated by Kiwi Syslog

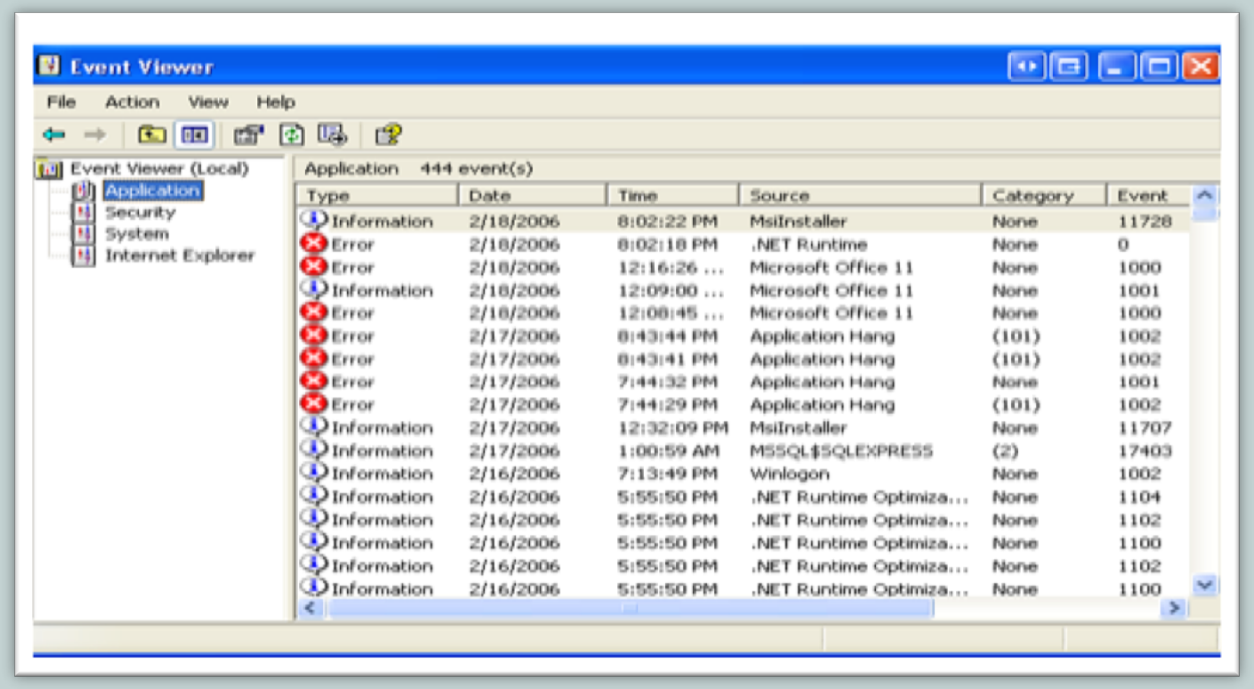
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



Logs

- Operating systems running on network clients and servers can also produce logs

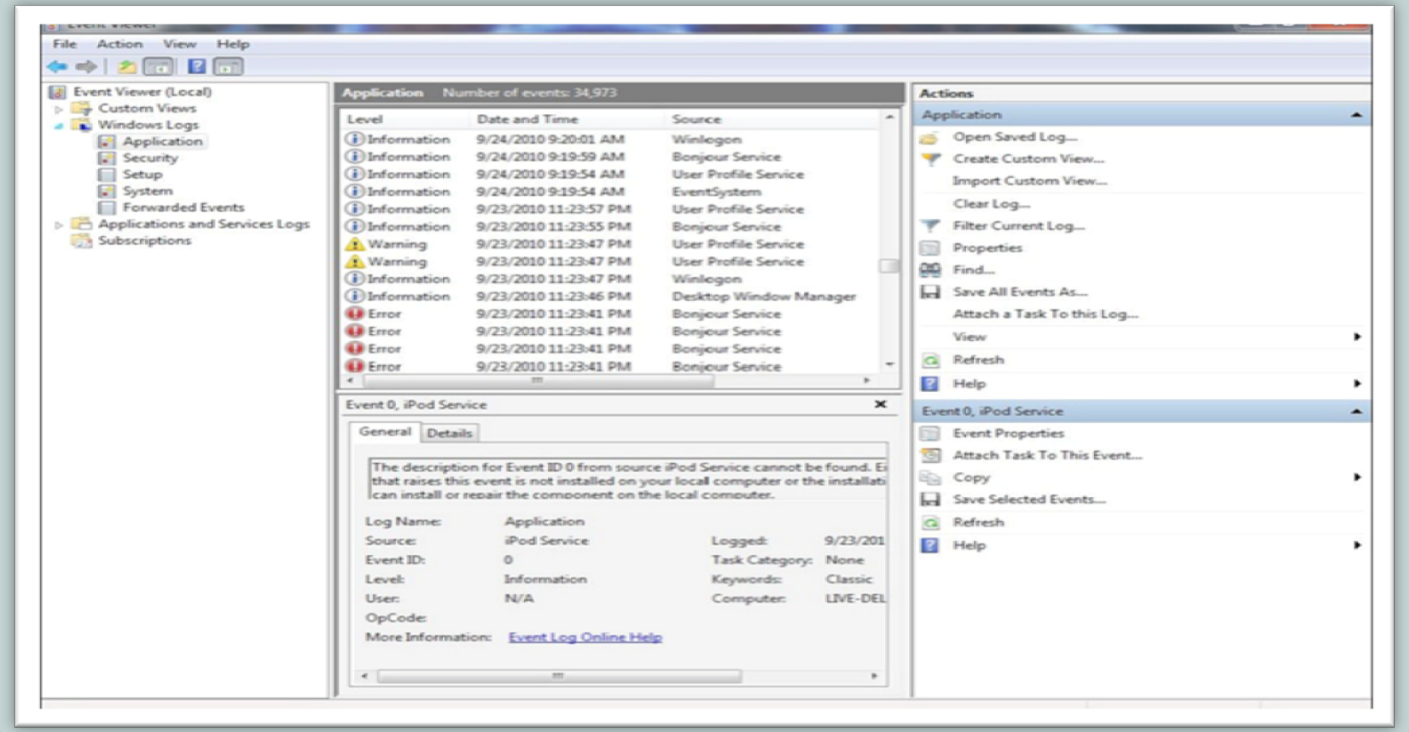
- Microsoft Windows provides an *Event Viewer* application to view logs



Application Logs

- Contains information about software applications running on a client or server

- Severity levels:
  - Information, Warning, and Error



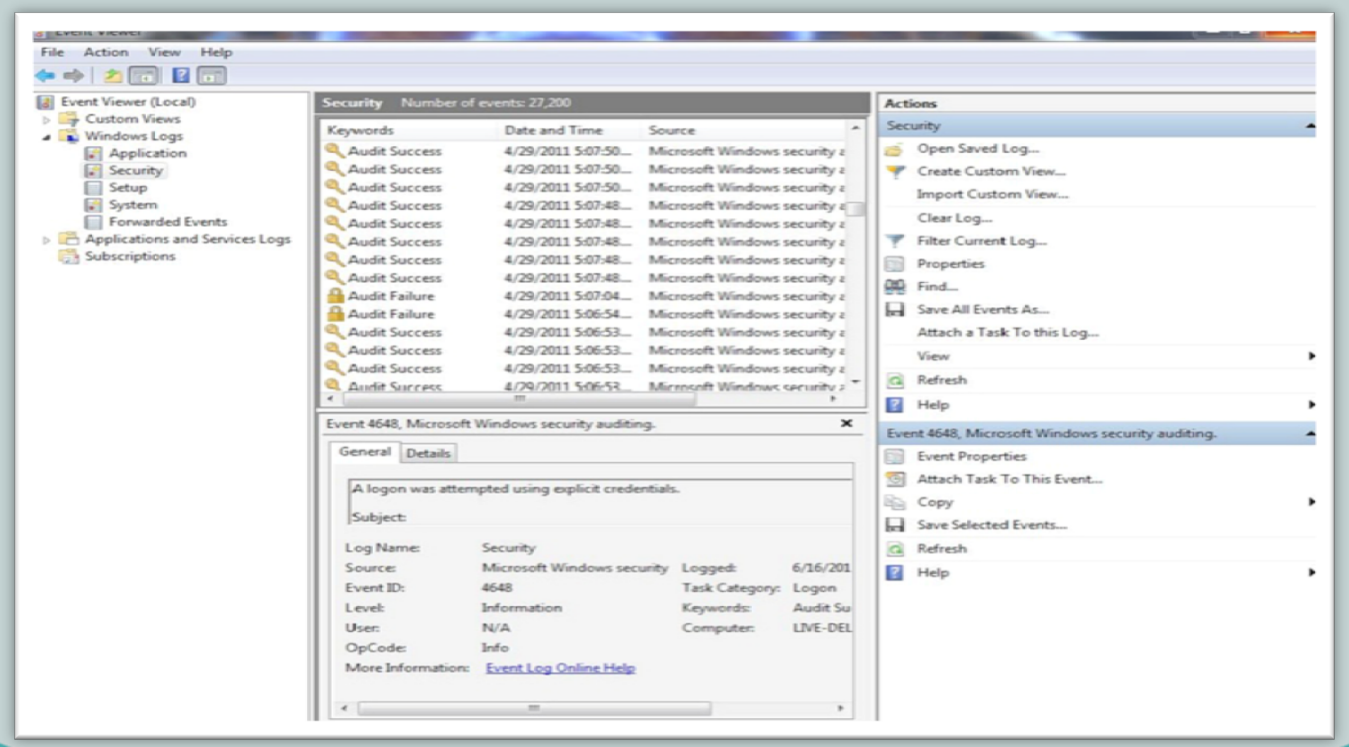
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Security Logs

- Contains information about the security of a client or server

- Contains logs of successful/failed logins and other pertinent security information

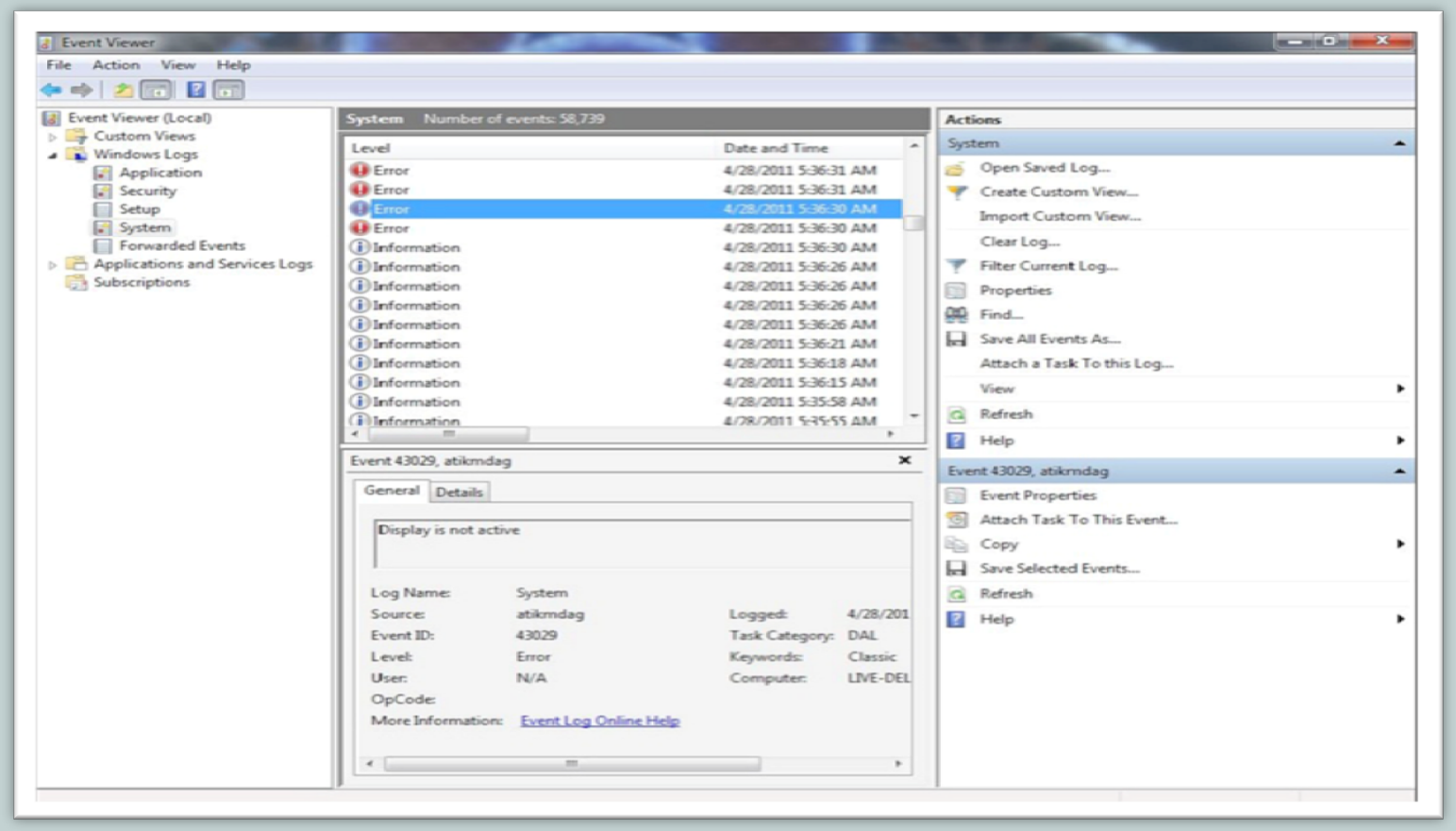


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

System Logs

- Contains information about operating system events



Remote Access

CompTIA Network+ (N10-007)

Remote Access Review

- Many ways to access data remotely and either control a client, server, or other device over a network connection

- This lesson serves as a quick review of technologies discussed throughout this course and how they are used to manage and configure network devices

Telnet
Port 23

- Permits sending commands to remote devices

```
Last login: Sun Feb 18 12:48:48 on ttys000
Jasons-MacBook-Pro:~ konsole$ telnet rainmaker.wunderground.com
Trying 35.160.169.47...
Connected to rainmaker.wunderground.com.
Escape character is '^]'.
------------------------------------------------------------------------------
*               Welcome to THE WEATHER UNDERGROUND telnet service!           *
------------------------------------------------------------------------------
*                                                                            *
*   National Weather Service information provided by Alden Electronics, Inc. *
*    and updated each minute as reports come in over our data feed.          *
*                                                                            *
*   **Note: If you cannot get past this opening screen, you must use a       *
*   different version of the "telnet" program--some of the ones for IBM      *
*   compatible PC's have a bug that prevents proper connection.              *
*                                                                            *
*           comments: jmasters@wunderground.com                              *
------------------------------------------------------------------------------
```

- Information is sent in plain text

- Telnet should never be used over an insecure connection and is a huge security risk to use

Secure Shell Protocol (SSH) Port 22

- Works like telnet, but uses encryption to create a secure channel between the client and the server

```
Jasons-MacBook-Pro:~ konsole$ ssh narnia0@narnia.labs.overthewire.org -p 2226
This is a OverTheWire game server. More information on http://www.overthewire.org/wargames
narnia0@narnia.labs.overthewire.org's password:

                         _____                     ____
      ,----..           ,----,                   .---.
     /   /   \         ,/   .`|                  /. ./|
    /   .     :      ,`   .'  :     .--'.   ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /   ` ; .'___,/    ,' .--'.   '   \' .
  ;   |  ; \ ; | |    :     | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `____'  |  |  \   ;  `      |
  '   ;  \; /  |      '   :  ;   .   \    .\  ;
   \   \  ',  /       |   |  '    \   \   ' \ |
    ;   :    /        '   :  |     :   '   |--"
     \   \ .'          ;   |.'      \   \  ;
  www. `---` ver      '---' he       '---" ire.org
```

- SSH should always be used instead of telnet

Remote Desktop Protocol (RDP) Port 3389

- Allows remote access to a machine over the network as if you were sitting right in front of it

- Provides GUI access through an RDP client

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA Network+

Virtual Network Computing (VNC) Port 5900

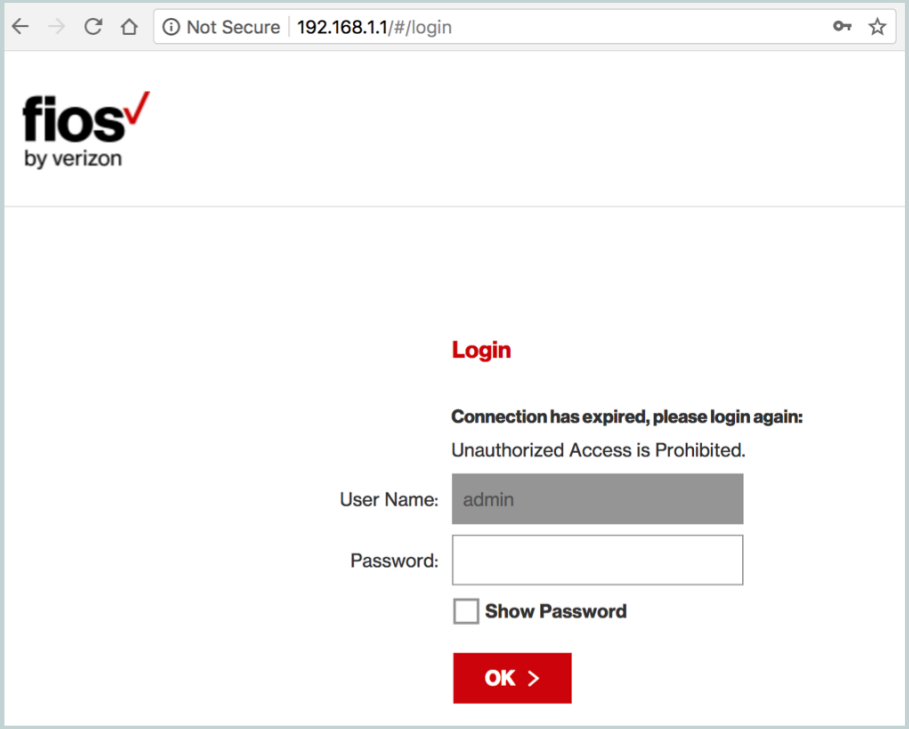
- Originally used in thin client architectures

- Operates much like RDP, but a cross-platform solution for Windows, Linux, and OS X

HTTPS and Management URLs

- Many systems provide a management system that is accessed through a web browser

- Examples:
  - Wireless access points
  - Modems
  - Routers
  - Firewalls



Remote File Access (FTP/FTPS, SFTP, TFTP)

- FTP – File Transfer Protocol
  - Port 20/21
  - Unencrypted file transfers (insecure)

- FTPS – File Transfer Protocol Secure
  - Port 20/21
  - Adds SSL/TLS to FTP to secure data

- SFTP – Secure File Transfer Protocol
  - Port 22
  - File transfer over SSH to increase security

- TFTP – Trivial File Transfer Protocol
  - Port 69
  - UDP version of FTP that sacrifices reliability for efficiency

VPNs

- Permits secure connections to different parts of the network for management and access
- IPSec
  - Ensures authentication, integrity, & confidentiality
- SSL/TLS/DTLS
  - Use of web browsers for secure VPN connections
- Site-to-Site VPN
  - Connect one network to another
- Client-to-Site VPN
  - Connect a single client to a network

Out-of-Band Management

- Connect to the device using a modem, console router, or direct cable for configuration
- Separation of data and management networks provides additional security to the network
- Requires additional configuration and equipment to implement

Configuration Management

CompTIA Network+ (N10-007)

Configuration Management

- Focuses on maintaining up-to-date documentation of a network's configuration

- Procedures include
  - Asset management
  - Baselining
  - Cable management
  - Change management
  - Network documentation

Asset Management

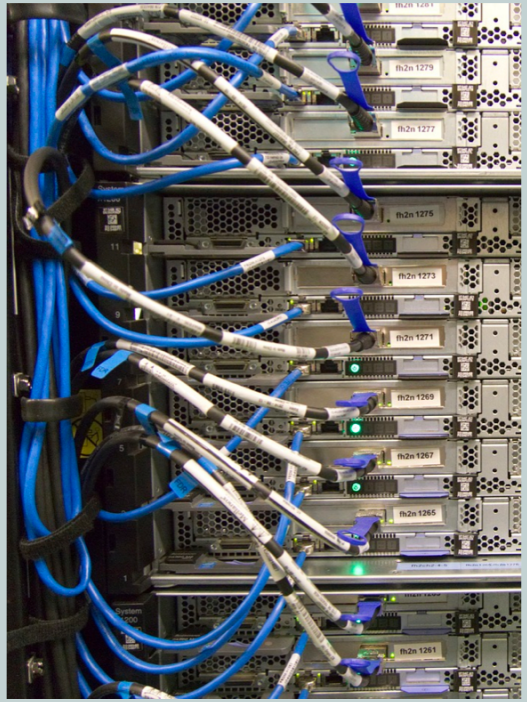
- Formalized system of tracking network components and managing the component's lifecycle
  - Prepare
    - Budget for the items and gather requirements
  - Plan
    - Determine what components to acquire
  - Design
    - Determine the best configuration for the devices
  - Implement
    - Purchase, install, and configure the devices
  - Operate
    - Maintain operations and support on a daily basis
  - Optimize
    - Improve the network design through new devices

Create a Baseline

- Collection of data under normal operating conditions
- Useful during comparison when troubleshooting network issues
- How do you know if your network is running normally if you don't know what normal is?

Cable Management

- Process of documenting the network's existing cable infrastructure
  - Diagrams
  - Cable labeling
  - Locations of punch-down blocks
  - Source cable locations
  - Destination cable locations



- Using standard naming conventions are considered a best practice
  - `HR_D_RM102_0012`
  - `IT_L_RM205_0004`

Change Management

- Coordinated system to account for upgrades, installs, and network outages
- Simple router or switch upgrades may cause unwanted downtime…
  ….they must be pre-coordinated
- Consider downtime, impacts, and vulnerabilities that may be introduced

Network Documentation

- Document the network appropriately
- Keep materials up-to-date
- Includes
  - Contact Information of administrators
  - Policies
  - Network maps and diagrams
  - Documentation (vendors, warranties, ...)
  - Wiring schematics
  - Standard Operating Procedures and Instructions