Section 21:Network Monitoring

168.SNMP

Simple Network Management Protocol (SNMP) - A tool that allows us to administer and manage network devices from a single devices

TERMs:

Managed Device:

Agent - Software built in that gives the device (a printer) to used SNMP

Individual devices listen on **UDP 161** if they are unencrypted
If encrypted they listen using TLS on **UDP port 10161**

SNMP Manager:

Running some kind of interface called a NMS (Network management station)
Unencrypted, listen on Port UDP 161
Encrypted, Listening on TLS Port UDP 10162

How to communicate between NMS and Managed Device:

SNMP is not just for printers. It is for many things so when setting up SNMP network you (which is build into every managed device) a:

MIB (Management Informaton Base) - Database that we query to be able to talk to that device. Different devices have different MIBs.

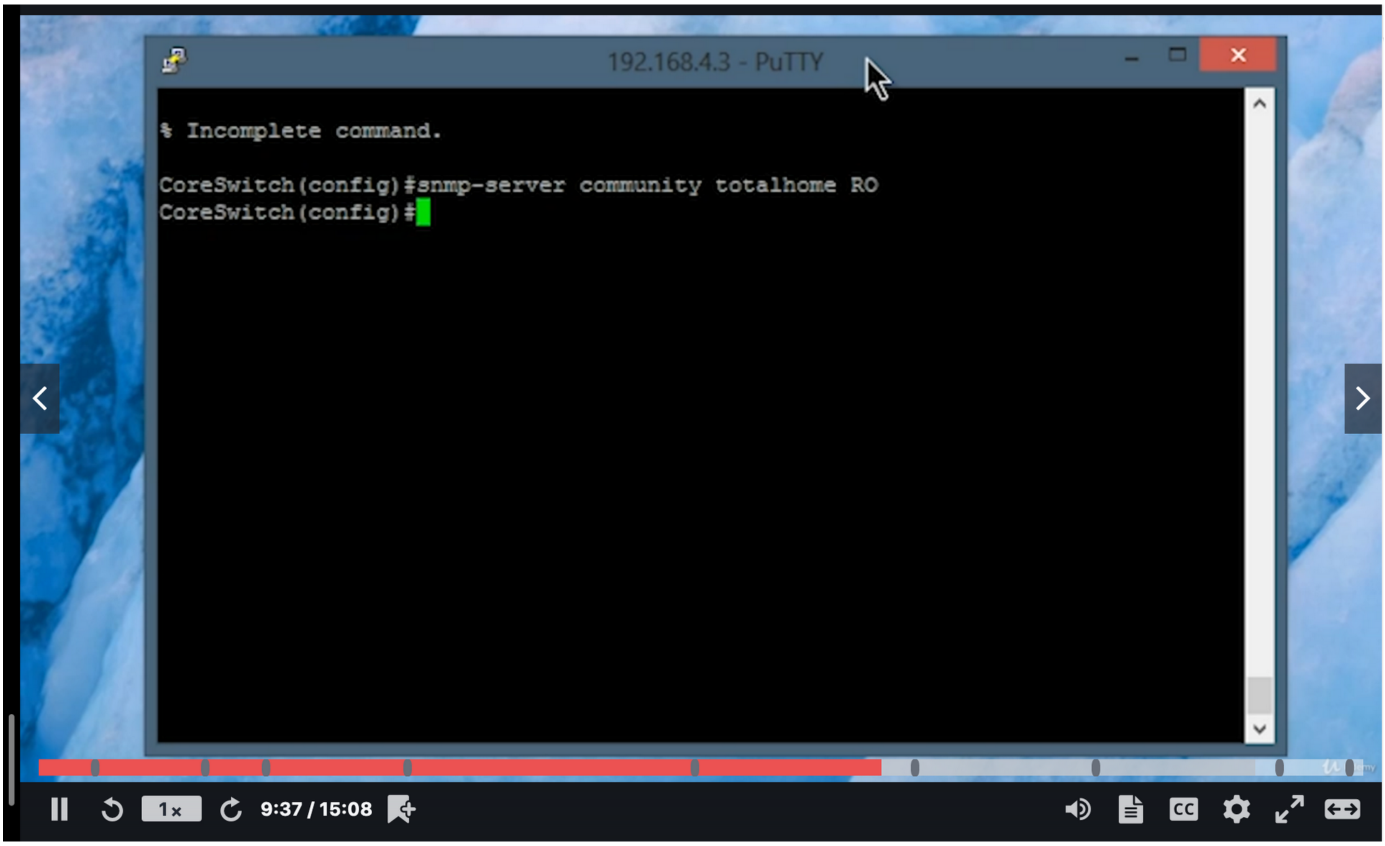
When setting up our NMS we download command lists from the internet that allows us to query devices on our network

Communications that are on the test:

*Get - NMS sends a get to the Managed device and the managed device sends back information
*Trap - Set up on managed devices and then the trap is sent to the NMS if there is an issue
*Walk/SNMPWalk - Batch process of Gets (Asking a lot of stuff from a managed device)
**Study more SNMP commands

Versions of SNMP (3):
-Differences:
- - SNMP V1 does not support encryption
- - SNMP V2 added basic encryption
- - SNMP V3 add Robust TLS encryption
* Its common to have different versions of SNMP in an enterprise and its okay because the NMS can talk to them all

Starting SNMP on a Managed Device:



```
% Incomplete command.

CoreSwitch(config)#snmp-server community totalhome RO
CoreSwitch(config)#
```

*Community - An organization of managed devices
*RO (Read Only) - A setting that you can set up that you can only read on the managed device

Configuring an NMS Using Cacti - Cacti is an open-source NMS for graphing SNMP data

NMS to check out: Nagios, Zabbix, Spiceworks

Review:

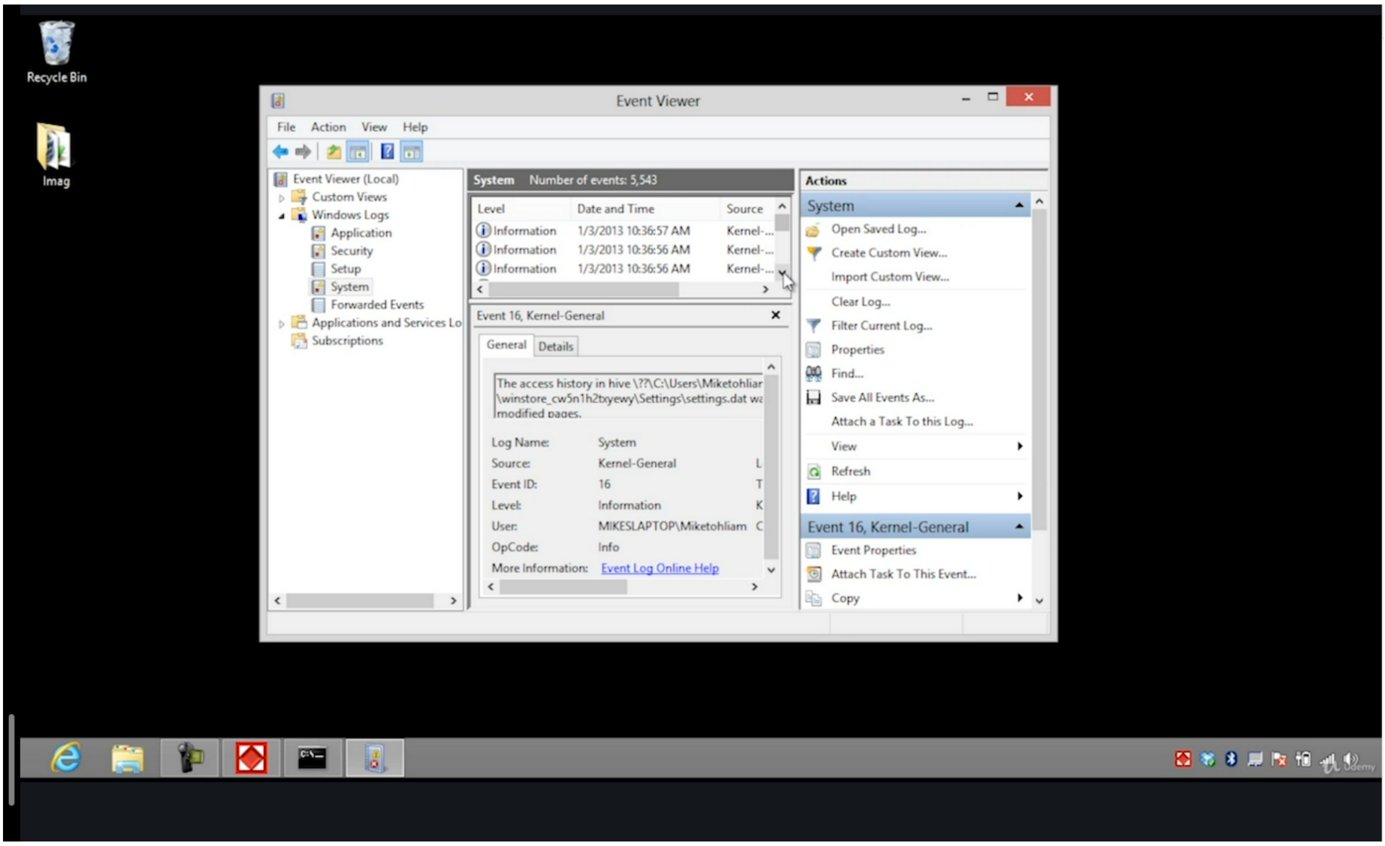
*SNMP uses UDP port 161 or port 10161 when using TLS
*SNMP-managed devices run an agent that talks with a Network Managemnt Station(NMS)
*Rembember the differences between the SNMP versions

---

169. Documenting Logs

System logs/General Logs - Different for every device (Laptop, Switches, routers, etc.) (Keeping track of events that have happened)

Windows and event viewer:



System Number of events: 5,543

Level	Date and Time	Source
Information	1/3/2013 10:36:57 AM	Kernel-...
Information	1/3/2013 10:36:56 AM	Kernel-...
Information	1/3/2013 10:36:56 AM	Kernel-...

Event 16, Kernel-General

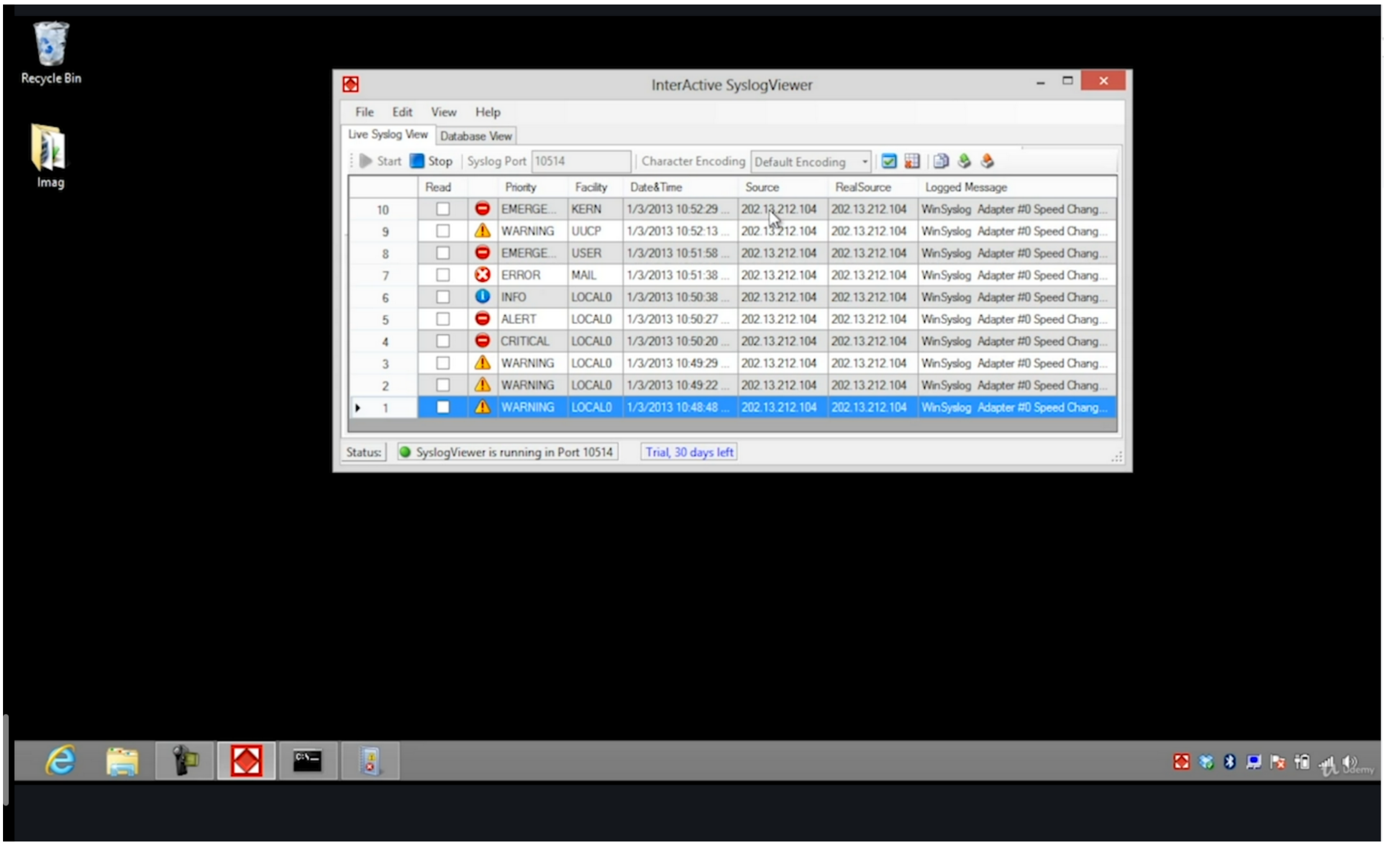
The access history in hive \??\C:\Users\Miketohliar
\winstore_cw5n1h2txyewy\Settings\settings.dat wa
modified pages.

Log Name:	System
Source:	Kernel-General
Event ID:	16
Level:	Information
User:	MIKESLAPTOP\Miketohliam
OpCode:	Info
More Information:	Event Log Online Help

Application Logs: Individual problems that have to do with applications
Security Logs: Individual events that deal with security
Setup Logs: Installations, updates, etc
System Logs: The general logs

*Logs can only be set to be kept for a certain amount of time
*You can choose what you want to log

Syslog:
-closest thing to a log standard that we have,
-works great with SNMP
-has a hierarchy of priorities (Error go from 0 to 7)



Syslog Port: 10514

Character Encoding: Default Encoding

	Read		Priority	Facility	Date&Time	Source	RealSource	Logged Message
10	□	⛔	EMERGE...	KERN	1/3/2013 10:52:29 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
9	□	⚠	WARNING	UUCP	1/3/2013 10:52:13 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
8	□	⛔	EMERGE...	USER	1/3/2013 10:51:58 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
7	□	✖	ERROR	MAIL	1/3/2013 10:51:38 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
6	□	ℹ	INFO	LOCAL0	1/3/2013 10:50:38 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
5	□	⛔	ALERT	LOCAL0	1/3/2013 10:50:27 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
4	□	⛔	CRITICAL	LOCAL0	1/3/2013 10:50:20 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
3	□	⚠	WARNING	LOCAL0	1/3/2013 10:49:29 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
2	□	⚠	WARNING	LOCAL0	1/3/2013 10:49:22 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...
▸ 1	□	⚠	WARNING	LOCAL0	1/3/2013 10:48:48 ...	202.13.212.104	202.13.212.104	WinSyslog Adapter #0 Speed Chang...

Status: SyslogViewer is running in Port 10514 | Trial, 30 days left

History Logs: Change logs - keeping track of what has been changed or updated over time

Review:

Logs are only as good as what you set it to log
Event Viewer is a windows tool that displays vario9us types of logs
Many Unix systems use syslog, which works with SNMP

---

170. System Monitoring

Core things to consider when doing network monitoring:

- Error Rate: frames and/or packets that are malformed, broken etc and its above our bandwidth rate
- Utilization: CPU utilization (CPU Load)
- Packet Drops: Measure the amount of packets that particular device cant handle. (Buffer overflow)
- Bandwidth: How much data am I moving per second
- File Integrity: Monitoring Critical Files (e.g. hash values, size, etc)

Review:

*Abnormal warnings of high error rate or utilization might signify security breaches or broken equipment
*A baseline helps identify irregular activity that needs to be investigated
*File Integrity is an important part of a monitoring program

171.SIEM (Security Information and Even Management)

1. Aggregation: grabbing data from a different places and storing it
    - Time synchronization
    - Event duplication
    - Normalization (Creates tables)
    - Logs (Puts logs together) "WORM (Write Once, Read Many)"
2. Correlation: analyzing the data and reporting in a way tha we can understand the data and utilize it
    - Alerting
        - For notification if something goes bad
    - Triggering
        - Exceeding thresholds

Examples of software:
- Splunk
- ArcSight
- ELK

Review:

*SIEM tools aggregate and correlate data, allowing organization in valuble information
*a SIEM tool accessess and correlates across logs to review an event
*SIEMs have alerts and the ability to notify based on a configurable trigger

---

QUIZ

1. Which choice is not a command protocol in SNMP
   a. snmpget
   b. snmpstep
   c. snmpset
   d. snmpgetnext
2. Which of the following is not a normal Windows log?
   a. Application
   b. Security Policies
   c. Setup
   d. Network
   e. System
   f. Forwarded events
3. A network technician has been tasked with monitoring the network. Which network function is it not necesary for her to monitor?
   a. File hash changes
   b. Server Utilization

c. Error Alerts

d. Banwidth