Technical Fundamentals for Evidence Acquisition

Information Security 4

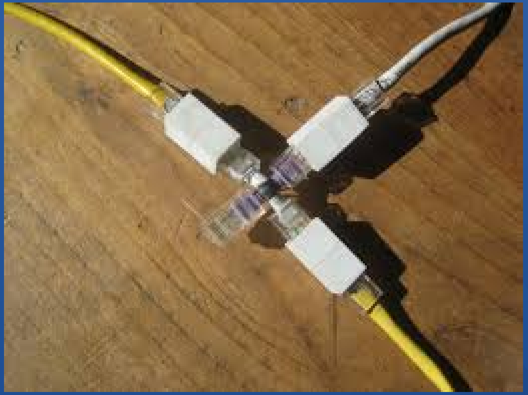
Goal

- Best possible outcome (impossible):
  - Perfect-fidelity evidence
  - Zero impact on network environment
  - Preserve evidence
- Reality:
  - Not possible to achieve a zero footprint investigation
  - Must use best practices to minimize investigative footprint
  - Verify evidence authenticity with cryptographic checksums
- Active vs. Passive
  - Passive – "… gathering forensic-quality evidence form networks without emitting data at Layer 2 and above." (Davidoff & Ham, 2012)
  - Active – "collecting evidence by interacting with workstations" (Davidoff & Ham, 2012)
  - Both techniques are used on a continuum

Sources of network-based evidence

Network environments are usually varied and unique and are a source of evidence.

- On the Wire
- In the Air
- Switches
- Routers
- DHCP Server
- Name Servers
- Authentication Server
- Network Intrusion Detection / Prevention Systems
- Firewalls, Load Balancers
- Web Proxies
- Application Server
- Central Log Server

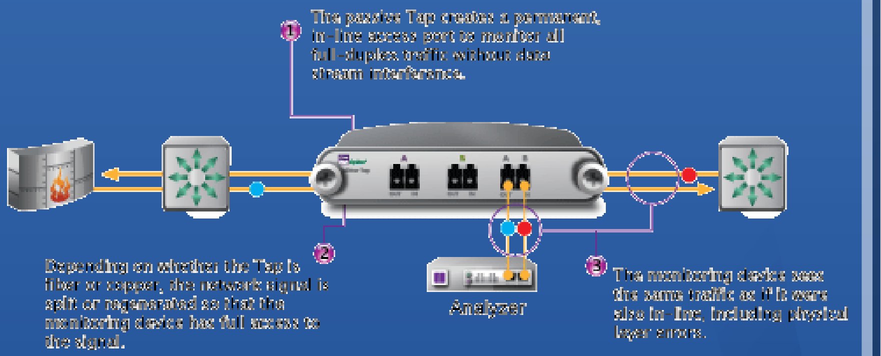


https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQgRO172pTPU9BgUHh5M--IM5zX7OaP4ZTHei0595gX6gcPW2tp

On the wire

- Physical cabling carries data over the network
- Typical network cabling;
    - Copper : twisted pair or coaxial cable
    - Fiber-optic lines
- **<u>Forensic Value:</u>**
    - Wire tapping can provide real-time network data
    - Tap types
        - “Vampire” tap – punctures insulation and touches cables
        - Surreptitious fiber tap – bends cable and cuts sheath, exposes light signal
        - Infrastructure tap – plugs into connectors and replicates signal – (usually used in coordination with ISPs for security monitoring)

Network Tap Implementation



1 The passive Tap creates a permanent, in-line access port to monitor all full-duplex traffic without data stream interference.

2 Depending on whether the Tap is fiber or copper, the network signal is split or regenerated so that the monitoring device has full access to the signal.

3 The monitoring device sees the same traffic as if it were also in-line, including physical layer errors.

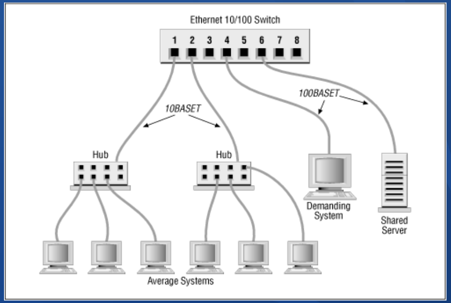
http://www.nextgigsystems.com/net_optics/10_GigaBit_Fiber_Tap_files/AppLC_SlimTap.png

In the air

- Wireless station – to – station signals
  - Radio frequency (RF)
  - Infrared (IR) – not very common
- **Forensic Value:**
  - Can be trivial as information is often encrypted, however valuable information can still be obtained
    - Management and controls frames are usually not encrypted
    - Access points (AP) advertise theirs names, presence and capabilities
    - Stations probes for APs and APs respond to probes
    - MAC addresses of legitimate authenticated stations
    - Volume-based statistical traffic analysis

Switches

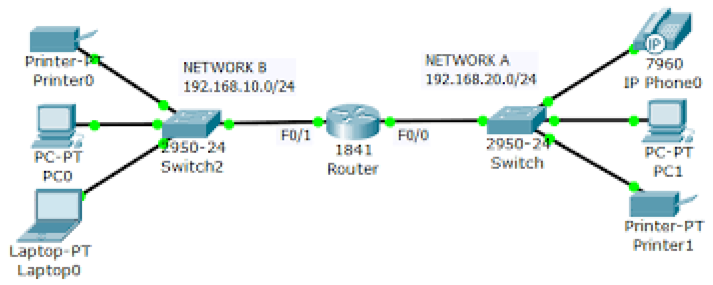
- “Switches are the glue that our hold LANs together” (Davidoff & Ham, 2012)
- Multiport bridges that physically connect network segments together
- Most networks connect switches to other switches to form complex network environments
- **Forensic Value:**
    - Content addressable memory (CAM) table
        - Stores mapping between physical ports and MAC addresses
    - Platform to capture and preserve network traffic
    - Configure one port to mirror traffic from other ports for capture with a packet sniffer



http://onlinemauritius-mu.blogspot.in/2011/10/connect-two-computers-to-my-internet.html

Routers

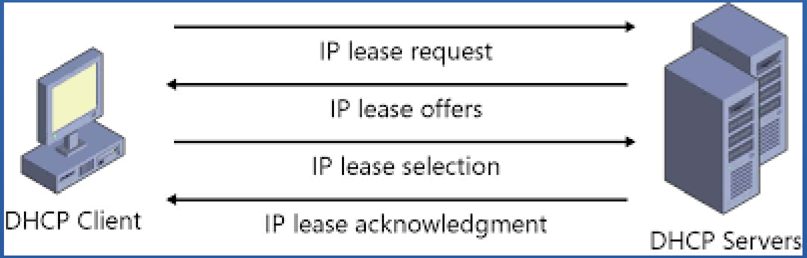
- Connect traffic on different subnets or networks
- Allows different addressing schemes to communicate
- MANs, WANs and LANs are all possible because of routers
- **Forensic Value:**
  - Routing tables
    - Map ports on the router to networks they connect
    - Allows path tracing
  - Can function as packet filters
  - Logging functions and flow records
  - Most widely deployed intrusion detection but also most rudimentary



https://broadcaststormblog.wordpress.com/2016/03/30/1-1-purpose-and-functions-of-network-devices-routers-switches-bridges-and-hubs/

DHCP Servers

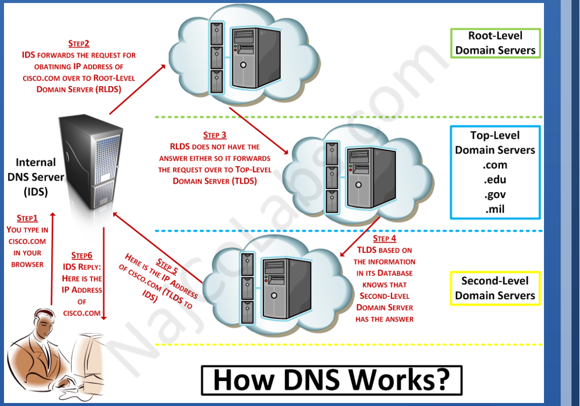
- Dynamic Host Configuration Protocol
- Automatic assignment of IP addresses to LAN stations
- **Forensic Value:**
  - Investigation often begins with IP addresses
  - DHCP leases IP addresses
  - Create log of events
    - IP address
    - MAC address of requesting device
    - Time lease was provided or renewed
    - Requesting systems host name



http://l4wisdom.com/linux-with-networking/dhcp-server.php

Name Servers

- Map IP addresses to host names
- Domain Name System (DNS)
- Recursive hierarchical distributed database
- **Forensic Value:**
    - Configured to log queries
        - Connection attempts from internal to external systems
            - EX: websites, SSH servers, external mail servers
        - Corresponding times
    - Create time-line of suspect activities



Step2
IDS forwards the request for obatining IP address of cisco.com over to Root-Level Domain Server (RLDS)

Step 3
RLDS does not have the answer either so it forwards the request over to Top-Level Domain Server (TLDS)

Step 4
TLDS based on the information in its Database knows that Second-Level Domain Server has the answer

Step 5
Here is the IP Address of cisco.com (TLDS to IDS)

Step6
IDS Reply: Here is the IP Address of cisco.com

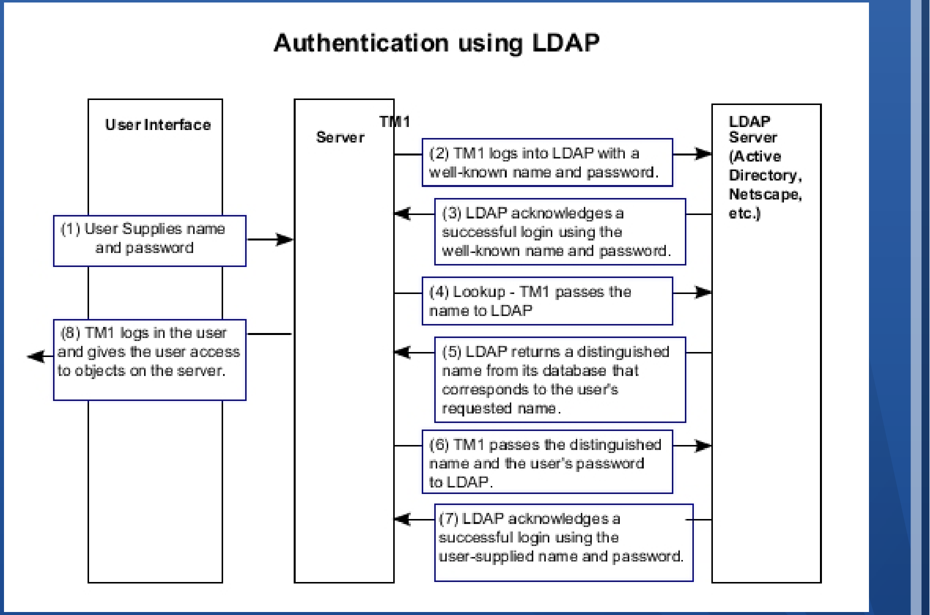
Step1
You type in cisco.com in your browser

Internal DNS Server (IDS)
Root-Level Domain Servers
Top-Level Domain Servers
.com
.edu
.gov
.mil
Second-Level Domain Servers
How DNS Works?

http://najcolabs.com/?p=257

Authentication Servers

- Centralized authentication services (Active Directory : LDAP)
- Streamline account provisioning and audit tasks
- **Forensic Value:**
    - Logs
        - Successful and/or failed attempts
        - Brute-force password attacks
        - Suspicious login hours
        - Unusual login locations
        - Unexpected privileged logins



Authentication using LDAP

(1) User Supplies name and password

(2) TM1 logs into LDAP with a well-known name and password.

(3) LDAP acknowledges a successful login using the well-known name and password.

(4) Lookup - TM1 passes the name to LDAP

(5) LDAP returns a distinguished name from its database that corresponds to the user's requested name.

(6) TM1 passes the distinguished name and the user's password to LDAP.

(7) LDAP acknowledges a successful login using the user-supplied name and password.

(8) TM1 logs in the user and gives the user access to objects on the server.

https://www.ibm.com/support/knowledgecenter/en/SSD29G_2.0.0/com.ibm.swg.ba.cognos.tm1_inst.2.0.0.doc/c_ldapauthentication_n13008d.html

Network Intrusion Detection / Prevention Systems

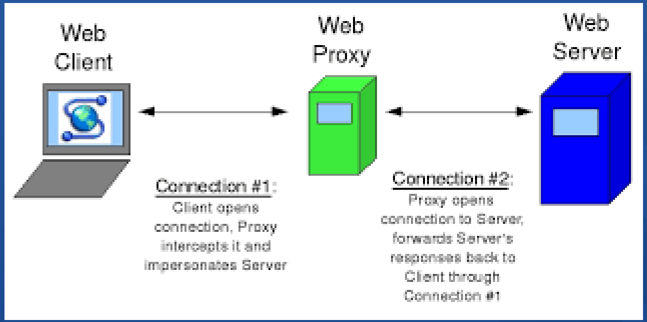
- NIDS and NIPS were designed for analysis and investigation
- Monitor real time network traffic
- Detect and alert security staff of adverse events
- **Forensic Value:**
    - Provide timely information
        - In progress attacks
        - Command – and – control traffic
    - Can be possible to recover entire contents of network packets
    - More often recovery is only source and destination IP addresses, TCP/UDP ports, and event time

Firewalls

- Deep packet inspection: forward, log or drop
- Based on source and destination IP, packet payloads, port numbers and encapsulation protocols
- **Forensic Value:**
  - Granular logging
  - Function as both infrastructure protection and IDSs
  - Log
    - Allowed or denied traffic
    - System configuration changes, errors and other events

Web Proxies

- Two uses:
    - Improve performance by caching web pages
    - Log, inspect and filter web surfing
- **<u>Forensic Value:</u>**
    - Granular logs can be retained for an extended period of time
    - Visual reports of web surfing patterns according to IP addresses or usernames (Active Directory logs)
    - Analyze
        - phishing email successes
        - Inappropriate web surfing habits
        - Web –based malware
    - View end-user content in cache



Web Client

Web Proxy

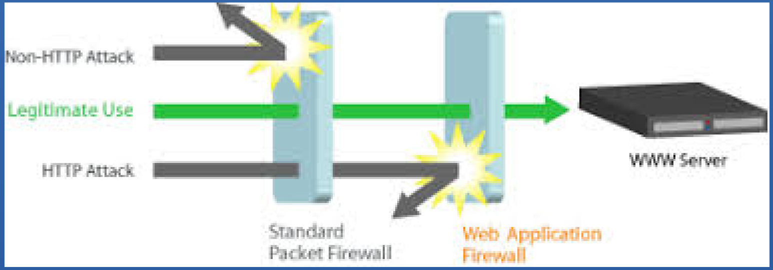
Web Server

Connection #1: Client opens connection, Proxy intercepts it and impersonates Server

Connection #2: Proxy opens connection to Server, forwards Server's responses back to Client through Connection #1

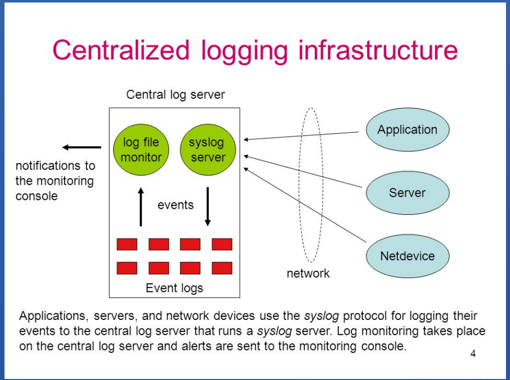
Application Servers

- Common types:
  - Database
  - Web
  - Email
  - Chat
  - VoIP / voicemail
- **Forensic Value:**
  - Far too many to list!



Central Log Server

- Combine event logs from many sources where they can be time stamped, correlated and analyzed automatically
- Can vary enormously depending on organization
- **Forensic Value:**
  - Designed to identify and respond to network security events
  - Save data if one server is compromised
  - Retain logs from routers for longer periods of time then routers offer
  - Commercial log analysis products can produce complex forensic reports and graphical representations of data



Centralized logging infrastructure

Applications, servers, and network devices use the *syslog* protocol for logging their events to the central log server that runs a *syslog* server. Log monitoring takes place on the central log server and alerts are sent to the monitoring console.

4

Internet Protocol Suite review

- Forensic investigators must know TCP / IP very well, including key protocols and header fields.
- Must have a clear understanding of protocol including flow record analysis, packet analysis and web proxy dissection
- Designed to handle addressing and routing
- IP operates on layer 3 (network layer)
- Connectionless
- Unreliable
- Includes a header but no footer
- Header plus payload is called an IP packet
- Wireshark tool

Try it out

- Study about VPNs
- See how security is bypassed by a VPN
- What are the security mechanisms you could envisage to monitor VPNs?

- Will it be a challenge if some one attacks a network using VPN?
  - Is it possible?
  - Has this happened before ?

Traffic Acquisition software

- Libpcap
  - UNIX C library
  - Provides an API for capturing and filtering data link-layer frames
  - WinPcap
    - Based on libpcap but designed for windows
  - Most popular tools that use this library
    - Tcpdump
    - Wireshark
    - Snort
    - Nmap
    - Ngrep
  - Captures packets at Layer 2 and stores them for later analysis

Berkeley Packet Filter

- Included in libpcap
- Powerful filtering language
  - Filter traffic based on comparison values at Layers 2, 3, and 4
- BPF primitives
  - Type – ex: Host, net, port or port range
  - Dir – ex: Src, dst, src or dst, src and dst, addr1
  - Proto – ex: ehter, fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp and udp
- Example filter:
  - ‘host 192.168.0.1 and not host 10.1.1.1 and (port 138 or port 139 or port 445)’

BPF continued

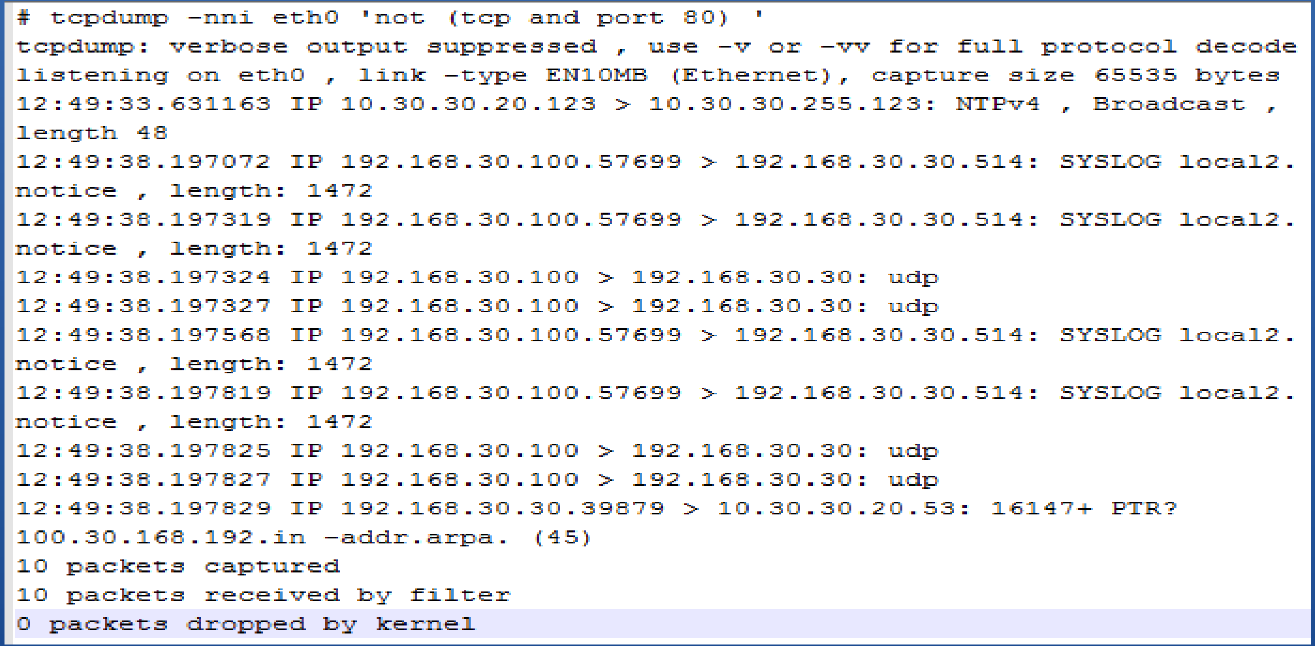
- Filter by byte value
  - Remember byte offsets start at 0
  - Examples:
    - ip[8] < 64 - match all packets where the single byte field starting at the eighth of the IP header offset is less then 64 (TTL field matches Linux systems)
    - ip[9] != 1 - match frames where the single byte field at the ninth byte offset of the IP header does not equal 1 (ICMP field set)
    - tcp[0:2] = 31337 - equivalent of ‘src port 31337’
- Filter by bit value
  - Built with bitmasking and value comparisons
  - Complex expressions with nested ANDs and ORs

TCPdump

- UNIX tool
- WinDump for Windows
- Purpose
    - Capture network traffic for later analysis
    - Capture traffic on a target segment over a period of time
- Captures bit-by-bit
- High fidelity
- Can be used with BPF to weed out traffic that is not pertinent to investigation

TCPDUMP example

- This example excludes TCP port 80 traffic from the eth0 network interface using BPF

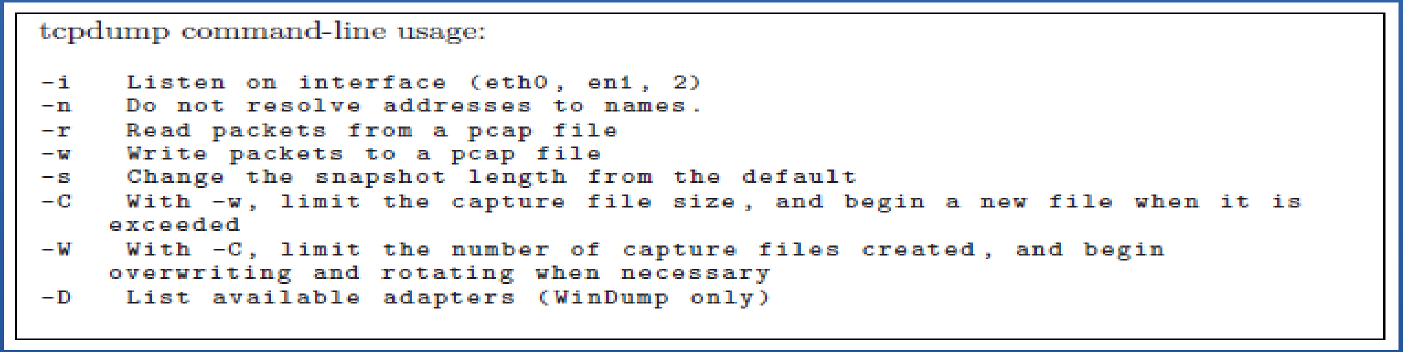


```
# tcpdump -nni eth0 'not (tcp and port 80) '
tcpdump: verbose output suppressed , use -v or -vv for full protocol decode
listening on eth0 , link -type EN10MB (Ethernet), capture size 65535 bytes
12:49:33.631163 IP 10.30.30.20.123 > 10.30.30.255.123: NTPv4 , Broadcast ,
length 48
12:49:38.197072 IP 192.168.30.100.57699 > 192.168.30.30.514: SYSLOG local2.
notice , length: 1472
12:49:38.197319 IP 192.168.30.100.57699 > 192.168.30.30.514: SYSLOG local2.
notice , length: 1472
12:49:38.197324 IP 192.168.30.100 > 192.168.30.30: udp
12:49:38.197327 IP 192.168.30.100 > 192.168.30.30: udp
12:49:38.197568 IP 192.168.30.100.57699 > 192.168.30.30.514: SYSLOG local2.
notice , length: 1472
12:49:38.197819 IP 192.168.30.100.57699 > 192.168.30.30.514: SYSLOG local2.
notice , length: 1472
12:49:38.197825 IP 192.168.30.100 > 192.168.30.30: udp
12:49:38.197827 IP 192.168.30.100 > 192.168.30.30: udp
12:49:38.197829 IP 192.168.30.30.39879 > 10.30.30.20.53: 16147+ PTR?
100.30.168.192.in -addr.arpa. (45)
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

TCPDUMP – 5 common commands

- tcpdump -i eth0 -w great_big_packet_dump.pcap
  - Listening in eth0 and writing all the packets in a single file
- tcpdump -i eth0 -s 0 -w biggest_possible_packet_dump.pcap
  - Same as above except by setting the snaplength to 0 it grabs the entire frame regardless of its size (this is not necessary in newer versions)
- tcpdump -i eth0 -s 0 -w targeted_full_packet_dump.pcap 'host 10.10.10.10‘
  - Grab packets sent to or from 10.10.10.10
- tcpdump -i eth0 -s 0 -C 100 -w rolling_split_100MB_dumps.pcap
  - Grabs every frame but splits the capture into multiple files no larger than 100MB
- tcpdump -i eth0 -s 0 -w RFC3514_evil_bits.pcap 'ip[6] & 0x80 != 0‘
  - Targets first byte of the IP fragmentation field, bitmask narrows it to single highest order bit “IP reserved bit” and finally packets are only stored if this value is nonzero

TCPDUMP command-line usage

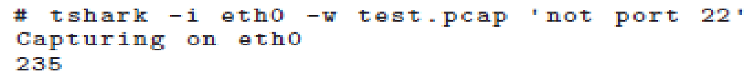


tcpdump command-line usage:

```
-i    Listen on interface (eth0, en1, 2)
-n    Do not resolve addresses to names.
-r    Read packets from a pcap file
-w    Write packets to a pcap file
-s    Change the snapshot length from the default
-C    With -w, limit the capture file size, and begin a new file when it is
     exceeded
-W    With -C, limit the number of capture files created, and begin
     overwriting and rotating when necessary
-D    List available adapters (WinDump only)
```

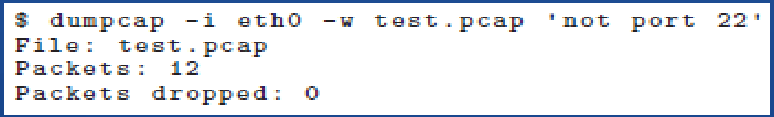
wireshark

- Open source GUI
- Captures – shows in real time and saves in a file
- Filters – easy filtering with many options
- Analyzes – powerful protocol analyzer
- Includes tshark
    - Command line network protocol analysis tool
    - Reads and saves files in same format
    - Ex:



```
# tshark -i eth0 -w test.pcap 'not port 22'
Capturing on eth0
235
```

- Includes dumpcap
    - Especially designed for packet capturing
    - Ex:



```
$ dumpcap -i eth0 -w test.pcap 'not port 22'
File: test.pcap
Packets: 12
Packets dropped: 0
```

Active Acquisition

- Modifies the environment – forensic investigators must minimize the impact!
- Common interfaces
  - Console
  - Secure Shell (SSH)
  - Secure Copy (SCP) and SSH File Transfer Protocol (SFTP)
  - Telnet
  - Simple Network Management Protocol (SNMP)
  - Trivial File Transfer Protocol (TFTP)
  - Web and proprietary interfaces

Console

- Input display system – keyboard and monitor
  - Most network devices have serial port to connect to a console
- USB-to-serial adapters available for new machines
- Best practice says to connect directly avoiding remote connections
  - Remote connections create excess traffic and can change CAM tables
-

SSH

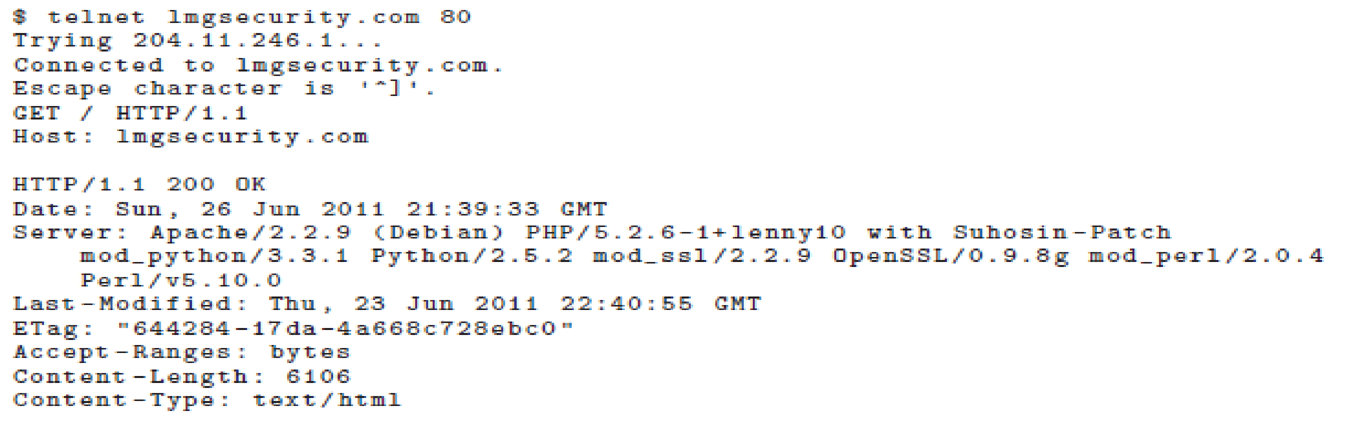
- Common remote access
- Replaces insecure telnet
- Encrypts authentication credentials and data
- OpenSSH – widely used implementation
    - Open source
- Command line interaction

SCP and SFTP

- Used in conjunction with SSH for secure file transfer and handling

Telnet

- Early design means limited security
  - Plaintext
  - Unencrypted credentials and data
- Sometimes it is the only option
  - Network devices have limited hardware or software
  - Not capable of upgrades to SSH
- Ex:



```
$ telnet lmgsecurity.com 80
Trying 204.11.246.1...
Connected to lmgsecurity.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: lmgsecurity.com

HTTP/1.1 200 OK
Date: Sun, 26 Jun 2011 21:39:33 GMT
Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny10 with Suhosin-Patch
    mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g mod_perl/2.0.4
    Perl/v5.10.0
Last-Modified: Thu, 23 Jun 2011 22:40:55 GMT
ETag: "644284-17da-4a668c728ebc0"
Accept-Ranges: bytes
Content-Length: 6106
Content-Type: text/html
```

SNMP

- “Most commonly used protocol for network device inspection and management” (Davidoff & Ham, 2012)
- Poll network devices from a central server
- Push information from remote agents to central collection point
- Used in two ways
    - Event-based alerting
    - Configuration queries
- Basic operations
    - Polling: GET, GETNEXT, GETBULK – retrieve information
    - Interrupt: TRAP, INFORM – timely notification
    - Control: SET – control configuration of remote devices

TFTP

- Transfers files between remote systems
- Transfers without authentication
- Services are small and limited, but still widespread
- UDP on port 69
- VoIP
- Firewalls
- Network devices often communicate with central servers
    - Backup configurations on routers and switches
- Forensic investigators uses
    - Export files form network devices not supported by SCP or SFTP

Web and Proprietary Interfaces

- New network devices come with web-based management
    - Access configuration menus
    - Event logs
    - Other common data
- Typically HTTP
- Forensic challenge
    - GUI inhibits logging
    - Best fallback is often screenshots and notes

Inspection Without Access

- Port scanning
  - Nmap
    - Will generate network traffic
    - Can modify the state of the target device
- Vulnerability scanning
  - Provide clues as to how breach or compromise may have occurred
  - Generate network traffic
  - Can modify the state of target device
  - Can crash target device

Strategy

- Refrain from rebooting or powering devices down
  - Volatile data lost in reboot
    - Ex: ARP tables, current state of devices
  - May modify persistent logfiles
- Connect via console instead of remotely over network
- Record system time
  - Check time skew
- Collect evidence according to volatility
  - When all else is equal go with data most likely to change or be lost
- Document all activities
  - Record commands – using “screen” or “script”
  - Important to make a record of all activities – mistakes and all
  - Screenshots of all GUI related activities

Works Cited

Davidoff, S., & Ham, J. (2012). *Network Forensics Tracking Hackers Through Cyberspace.* Boston: Prentice Hall.