Investigating Web Attacks

Module 08

Designed by Cyber Crime Investigators. Presented by Professionals.

C|HFI™ Computer Hacking Forensic Investigator

Module Objectives

After successfully completing this module, you will be able to:

1 Understand the importance of web application forensics

2 Illustrate the web application architecture and list the challenges in web application forensics

3 Indicate web attacks and define all the web application threats

4 Interpret the steps to investigate web attacks

5 Perform web attacks investigation on Windows-based servers

6 Describe IIS web server architecture and perform IIS logs investigation

7 Describe Apache web server architecture and perform Apache logs investigation

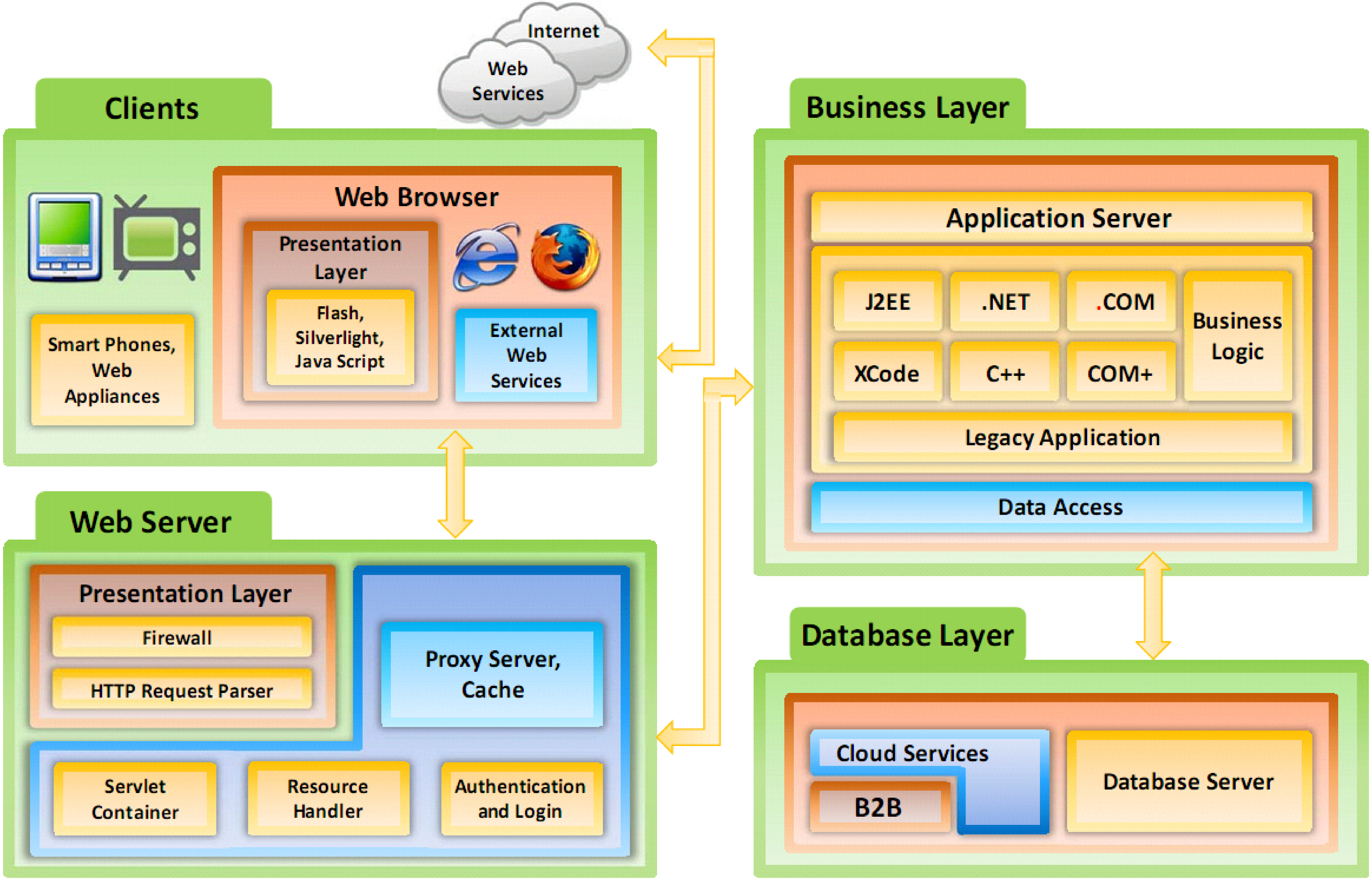
8 Investigate various attacks on web applications

Introduction to Web Application Forensics

1. Web applications **provide an interface between the end users and web servers** via a set of web pages that are generated at the server's end or contain script code, which is dynamically by the user's web browser.

2. Web application forensics involves **collection and analysis of logs** and other artifacts along the complete path taken by a web request. It includes web server, application server, database server, system events, etc., to determine the cause, nature and perpetrator of a web exploit.

Web Application Architecture



Challenges in Web Application Forensics

01 Web applications are generally **distributed in nature**

02 Traces of activities are **recorded across a number** of hardware and software infrastructures

03 **Very limited or no downtime** is allowed for investigation

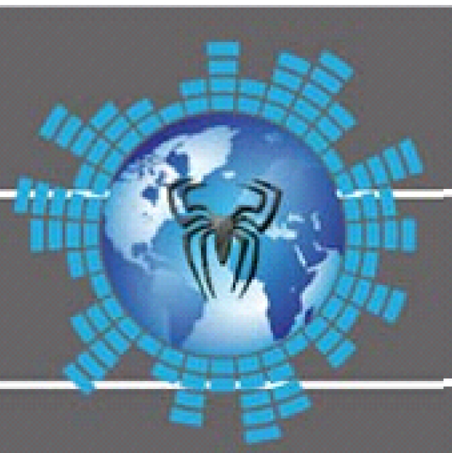
04 **Huge volume of logs** from different sources are analyzed and correlated

05 **Large databases** are analyzed

06 **Requires complete knowledge** of different web servers, application servers, databases and underlying applications

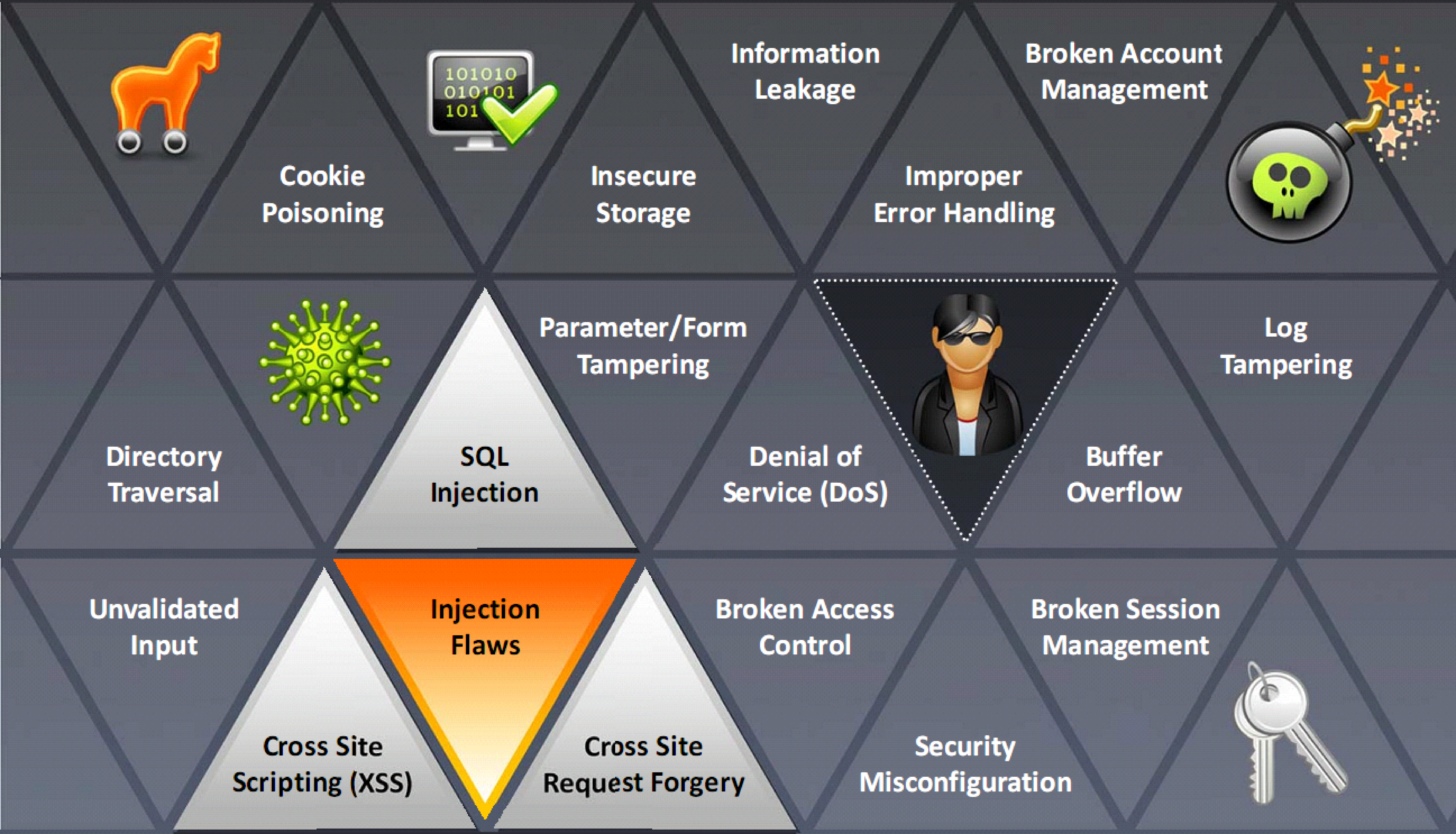
07 **Tracing back is difficult** in case of reverse proxies and anonymizers

Indications of a Web Attack



- ☞ Customers being unable to access services
- ☞ Suspicious activities in user accounts
- ☞ Leakage of sensitive data
- ☞ Correct URLs redirecting to incorrect sites
- ☞ Web page defacements
- ☞ Unusually slow network performance
- ☞ Frequent rebooting of the server
- ☞ Anomalies in log files
- ☞ Error messages such as 500 errors, “internal server error,” and “problem processing your request”

Web Application Threats - 1



Cookie Poisoning

Insecure Storage

Information Leakage

Broken Account Management

Improper Error Handling

Directory Traversal

SQL Injection

Parameter/Form Tampering

Denial of Service (DoS)

Log Tampering

Buffer Overflow

Unvalidated Input

Injection Flaws

Broken Access Control

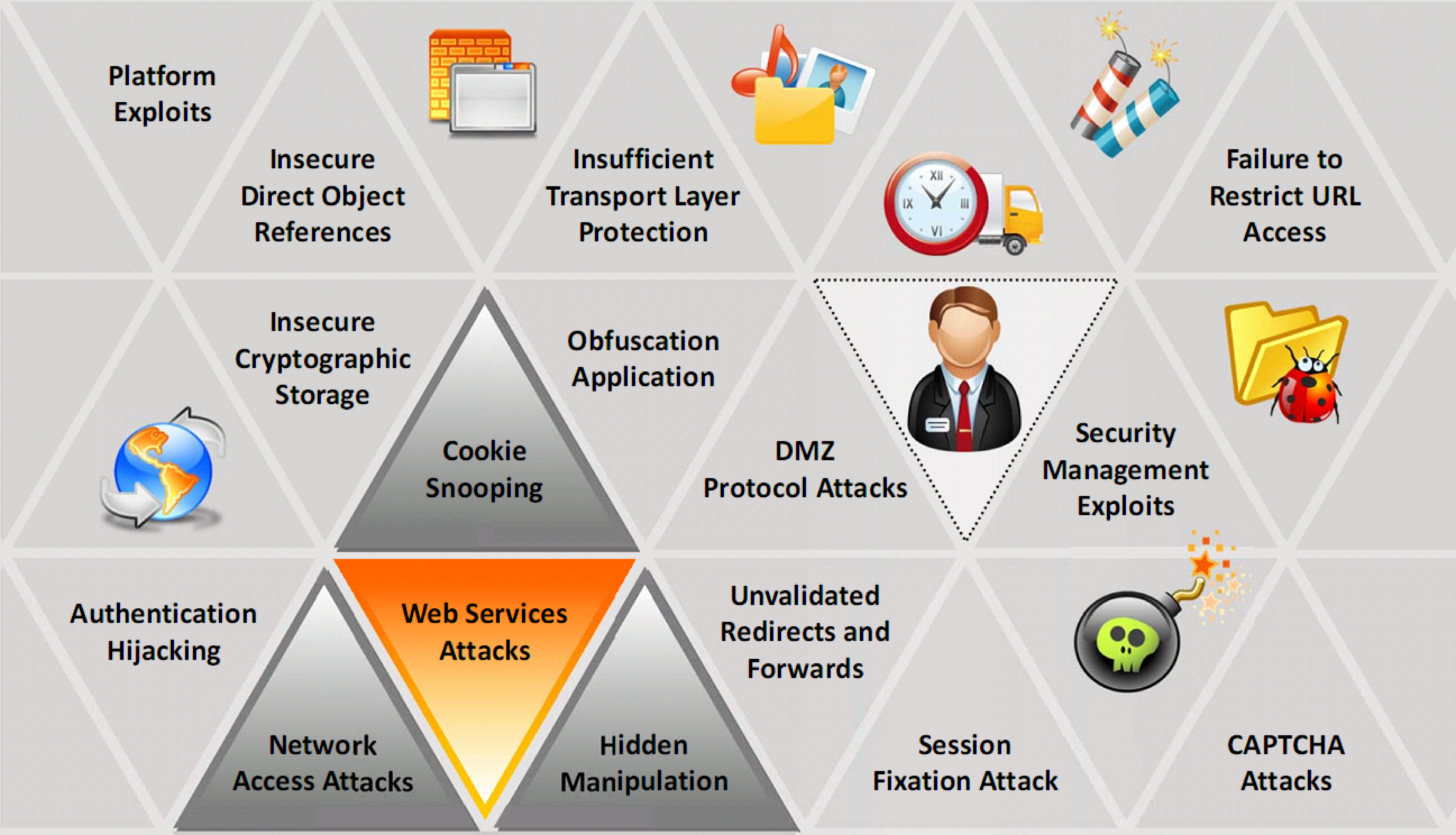
Broken Session Management

Cross Site Scripting (XSS)

Cross Site Request Forgery

Security Misconfiguration

Web Application Threats - 2



Platform Exploits

Insecure Direct Object References

Insufficient Transport Layer Protection

Failure to Restrict URL Access

Insecure Cryptographic Storage

Cookie Snooping

Obfuscation Application

DMZ Protocol Attacks

Security Management Exploits

Authentication Hijacking

Web Services Attacks

Unvalidated Redirects and Forwards

Network Access Attacks

Hidden Manipulation

Session Fixation Attack

CAPTCHA Attacks

Investigating a Web Attack

1. **Confirmation of the Attack and Identification of its Nature**

   Is it a distributed denial-of-service (DDoS) attack or an attack targeted just at you? Is someone trying to shut down your network altogether or attempting to infiltrate individual machines? Check the Security Information and Event Management (SIEM), Syslog or centralized/remote logs to confirm the attack.

2. **Capturing Volatile Data**

   Capture volatile data, such as processes, services, ports and network connections, memory dumps, logged in users, etc.

3. **Taking Snapshot or Shutting down the System**

   In virtualized environment, take a snapshot of the system. In the case of a physical system, shut down the server. You can move the services to alternate sites based on the availability of disaster recovery (DR) sites, backups, mirrors and business continuity requirements.

4. **Making Forensic Image/Mounting Snapshot**

   Make a bit-by-bit image of the system hard disk or mount the system snapshot on another virtual infrastructure to start the investigation.

Investigating a Web Attack (Cont'd)

5

Understanding the Flow of an Application

Look at the application documentation and testing reports to understand the normal application working.

6

Analysis of the Log Files

Examine the logs from web server, application server, database server, application, local system events, etc. for suspicious entries.

7

Collection of Application and Server Configuration Files

Application and server configuration files provide important application information, such as database bindings, application server configurations, etc.

8

Identification of Abnormal Activities

Identify malicious data from the client, discrepancies in normal web access, uncommon referrers, mid-session changes to cookie values, etc.

Investigating a Web Attack (Cont'd)

09

Corroboration with Firewall and IDS Logs

IDS and the firewall can monitor the network traffic and store logs of each entry. These logs can help to identify if the source is a compromised host on the network or a third party.

10

Blocking the Attack

Once you know how the attacker has entered the system, you can block that particular IP port or hole to prevent further intrusion. If any compromised systems are identified, disconnect them from the network until they can be disinfected.

11

Tracing Back Attack IPs

Traceback attack IPs to identify the perpetrator of the attack. It is generally very difficult as attackers often use proxies and anonymizers to hide their identity.

12

Full-proof Documentation

Document every step of the investigation as it is essential for any legal proceedings.

Investigating Web Attacks in Windows-Based Servers

Run **Event Viewer** to look at the logs:

```
C:\> eventvwr.msc
```

Check if the following **suspicious events** have occurred:

- Event log service ends
- Windows File Protection is inactive on the system
- The MS Telnet Service is running

Find if the system has **failed login** attempts or **locked-out accounts**

Investigating Web Attacks in Windows-Based Servers (Cont'd)

- Review file shares to ensure their purpose

  `C:\> net view <IP Address>`

- Verify the users using open sessions

  `C:\> net session`

- Check if the sessions have been opened with other systems

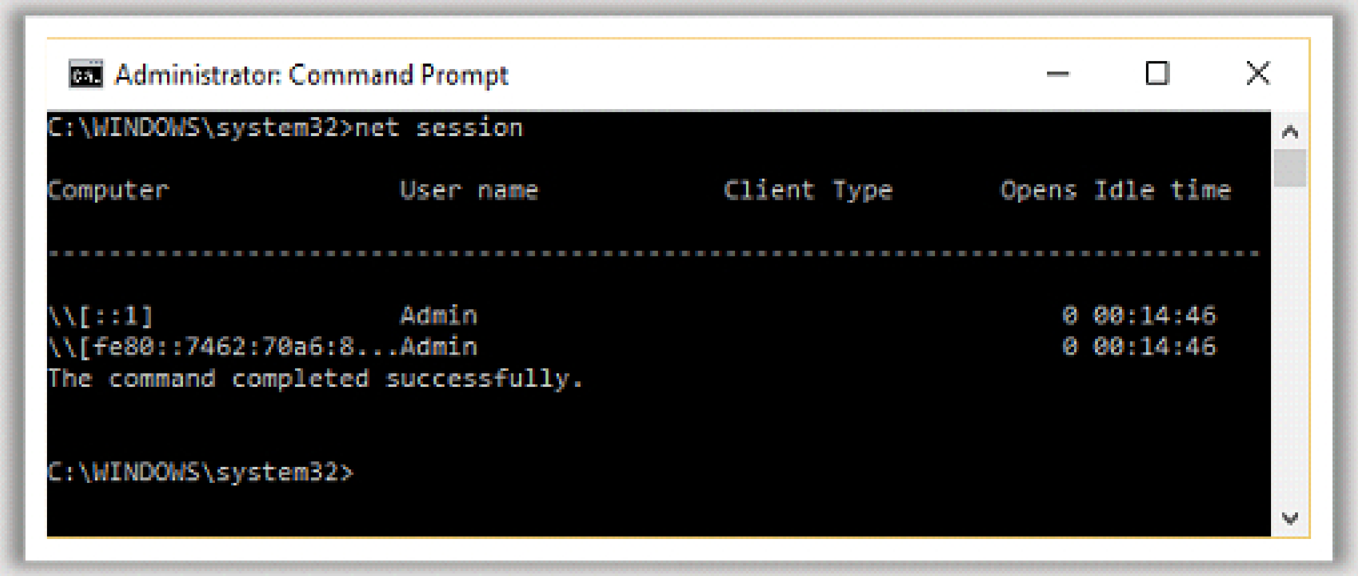
  `C:\> net use`

- Analyze at NetBIOS over TCP/IP activity

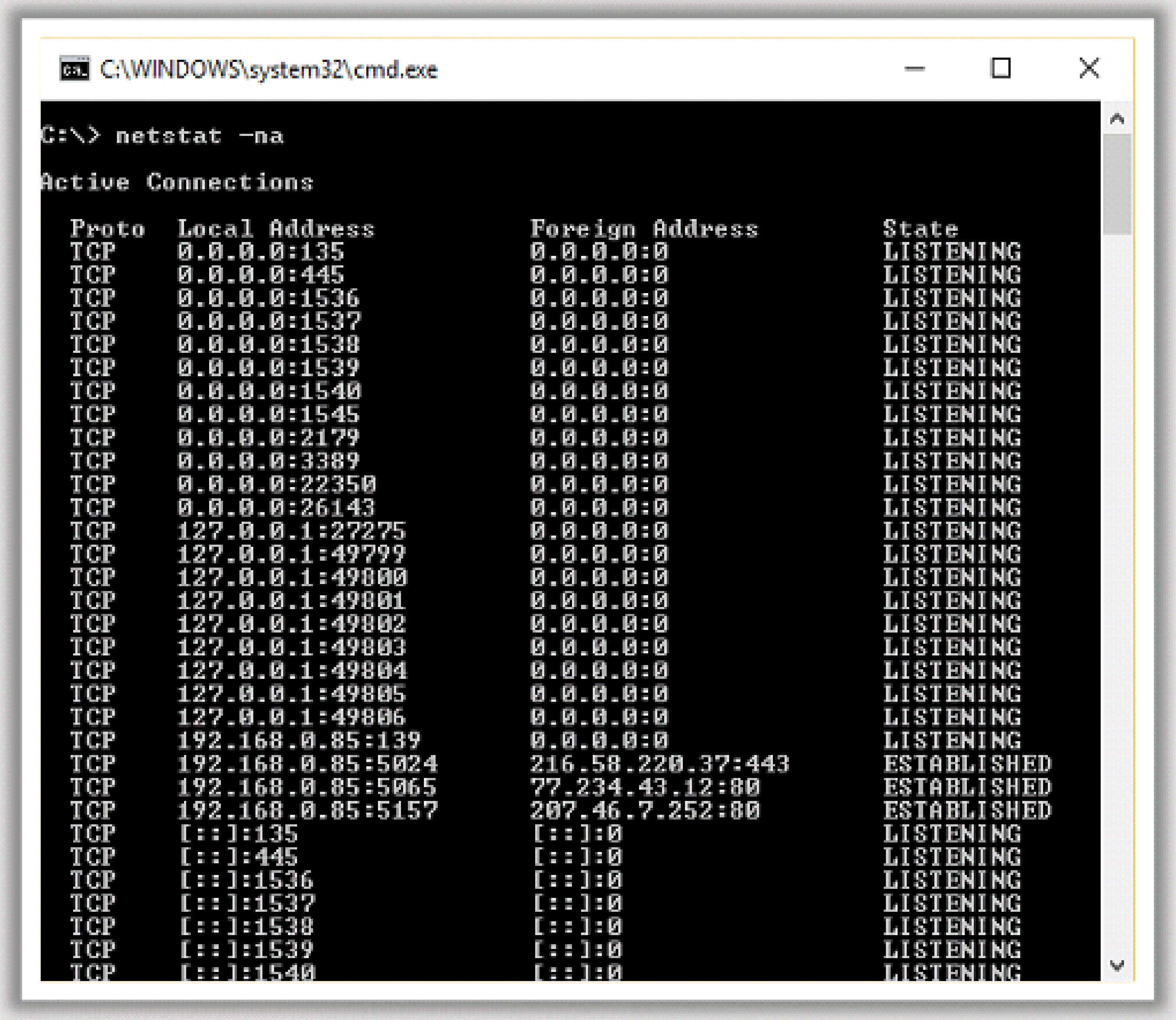
  `C:\> nbtstat -S`

- Find if TCP and UDP ports have unusual listening

  `C:\> netstat -na`

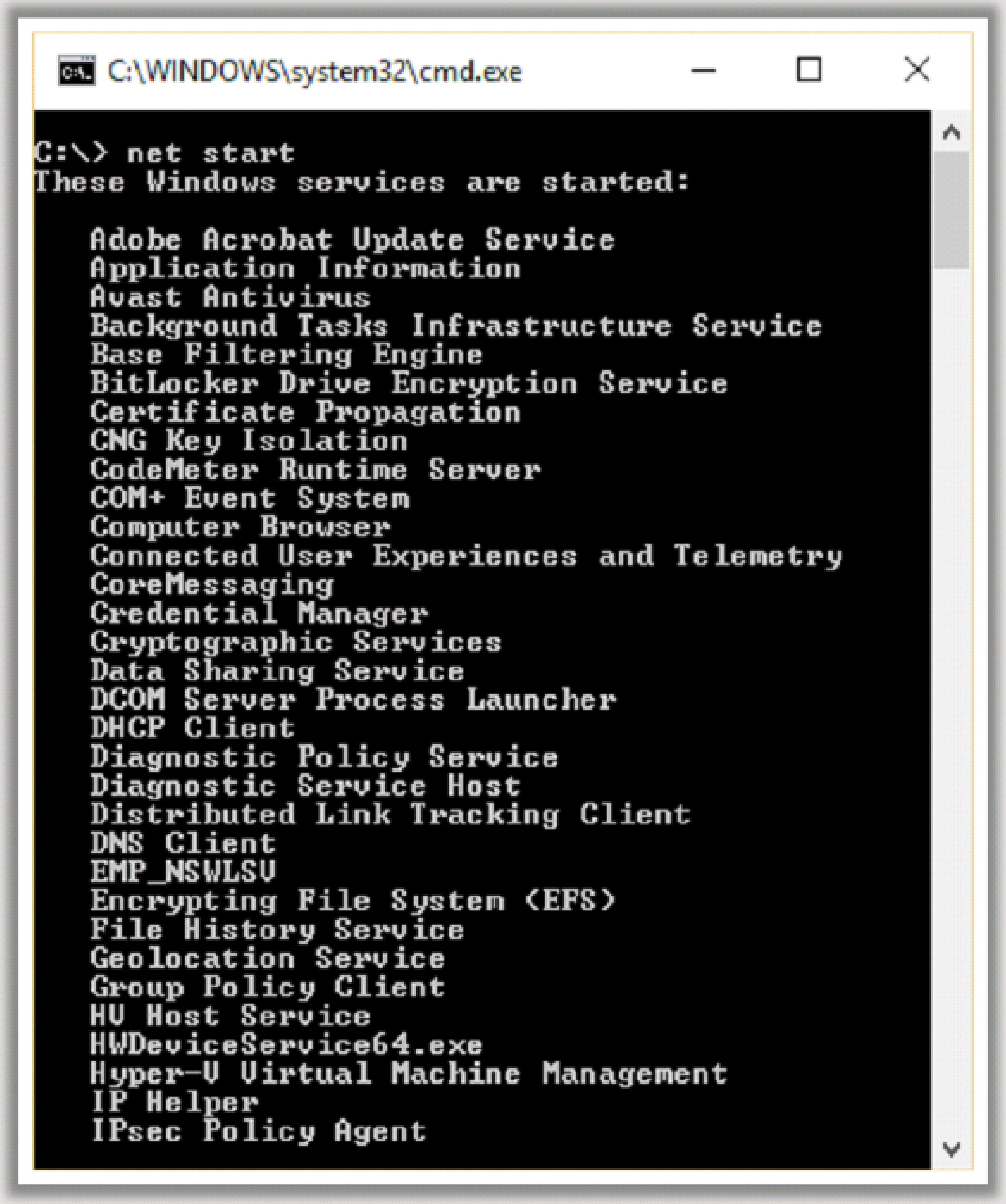


```
C:\WINDOWS\system32>net session

Computer               User name            Client Type       Opens Idle time

-------------------------------------------------------------------------------

\\[::1]                Admin                                      0 00:14:46
\\[fe80::7462:70a6:8...Admin                                      0 00:14:46
The command completed successfully.


C:\WINDOWS\system32>
```



```
C:\> netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1536           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1537           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1538           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1539           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1540           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1545           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2179           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:22350          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:26143          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:27275        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49799        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49800        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49801        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49802        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49803        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49804        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49805        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49806        0.0.0.0:0              LISTENING
  TCP    192.168.0.85:139       0.0.0.0:0              LISTENING
  TCP    192.168.0.85:5024      216.58.220.37:443      ESTABLISHED
  TCP    192.168.0.85:5065      77.234.43.12:80        ESTABLISHED
  TCP    192.168.0.85:5157      207.46.7.252:80        ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:1536              [::]:0                 LISTENING
  TCP    [::]:1537              [::]:0                 LISTENING
  TCP    [::]:1538              [::]:0                 LISTENING
  TCP    [::]:1539              [::]:0                 LISTENING
  TCP    [::]:1540              [::]:0                 LISTENING
```

Investigating Web Attacks in Windows-Based Servers (Cont'd)



```
C:\> net start
These Windows services are started:

   Adobe Acrobat Update Service
   Application Information
   Avast Antivirus
   Background Tasks Infrastructure Service
   Base Filtering Engine
   BitLocker Drive Encryption Service
   Certificate Propagation
   CNG Key Isolation
   CodeMeter Runtime Server
   COM+ Event System
   Computer Browser
   Connected User Experiences and Telemetry
   CoreMessaging
   Credential Manager
   Cryptographic Services
   Data Sharing Service
   DCOM Server Process Launcher
   DHCP Client
   Diagnostic Policy Service
   Diagnostic Service Host
   Distributed Link Tracking Client
   DNS Client
   EMP_NSWLSV
   Encrypting File System (EFS)
   File History Service
   Geolocation Service
   Group Policy Client
   HV Host Service
   HWDeviceService64.exe
   Hyper-V Virtual Machine Management
   IP Helper
   IPsec Policy Agent
```

Find scheduled and unscheduled tasks on the local host

```
C:\> schtasks.exe
```

Check for creation of new accounts in administrator group

```
C:\> lusrmgr.msc
```

See if any unexpected processes are running in Task Manager

```
Start -> Run -> taskmgr -> OK
```

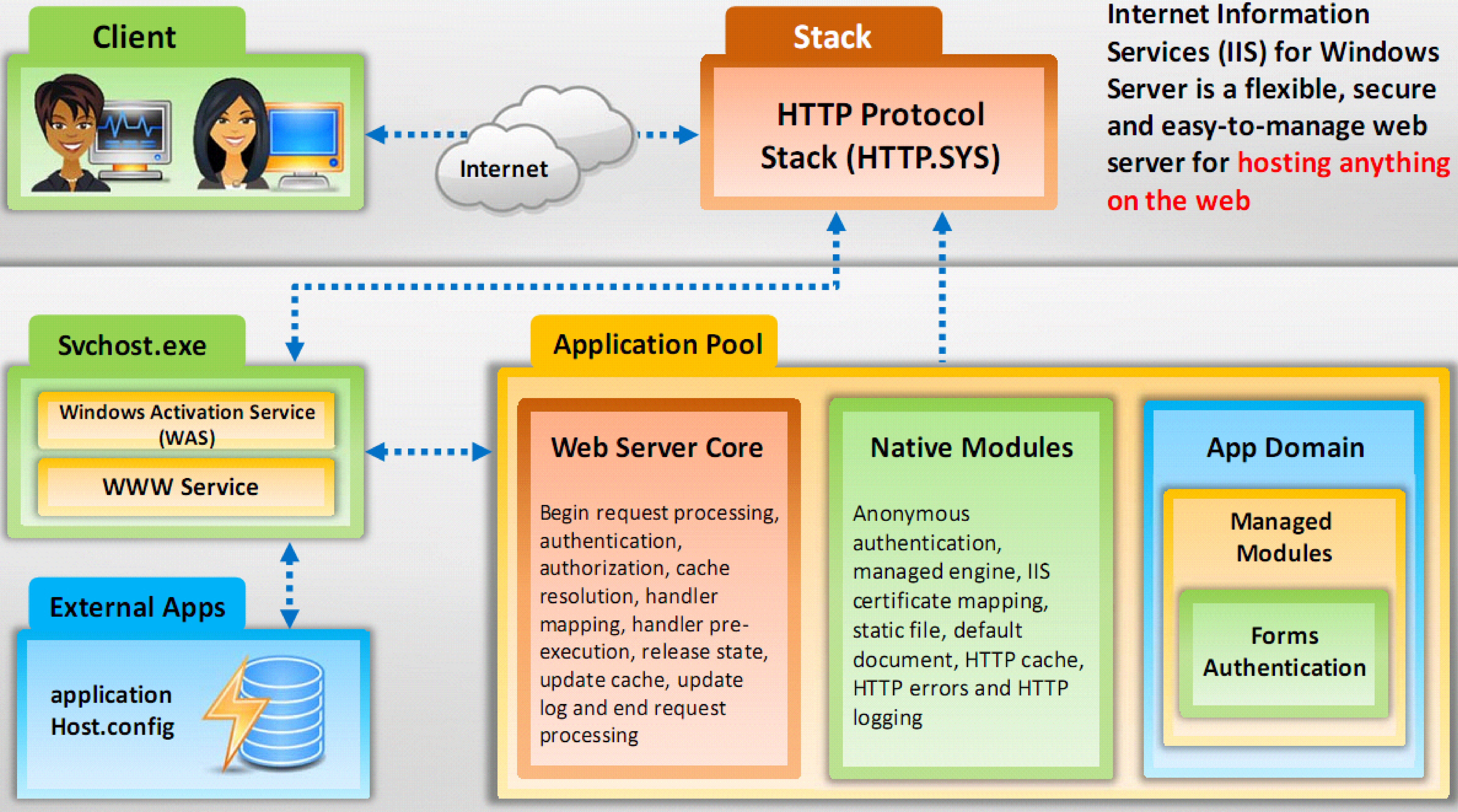
Look for unusual network services

```
C:\> net start
```

Check file space usage to look for a sudden decrease in free space

```
C:\> dir
```

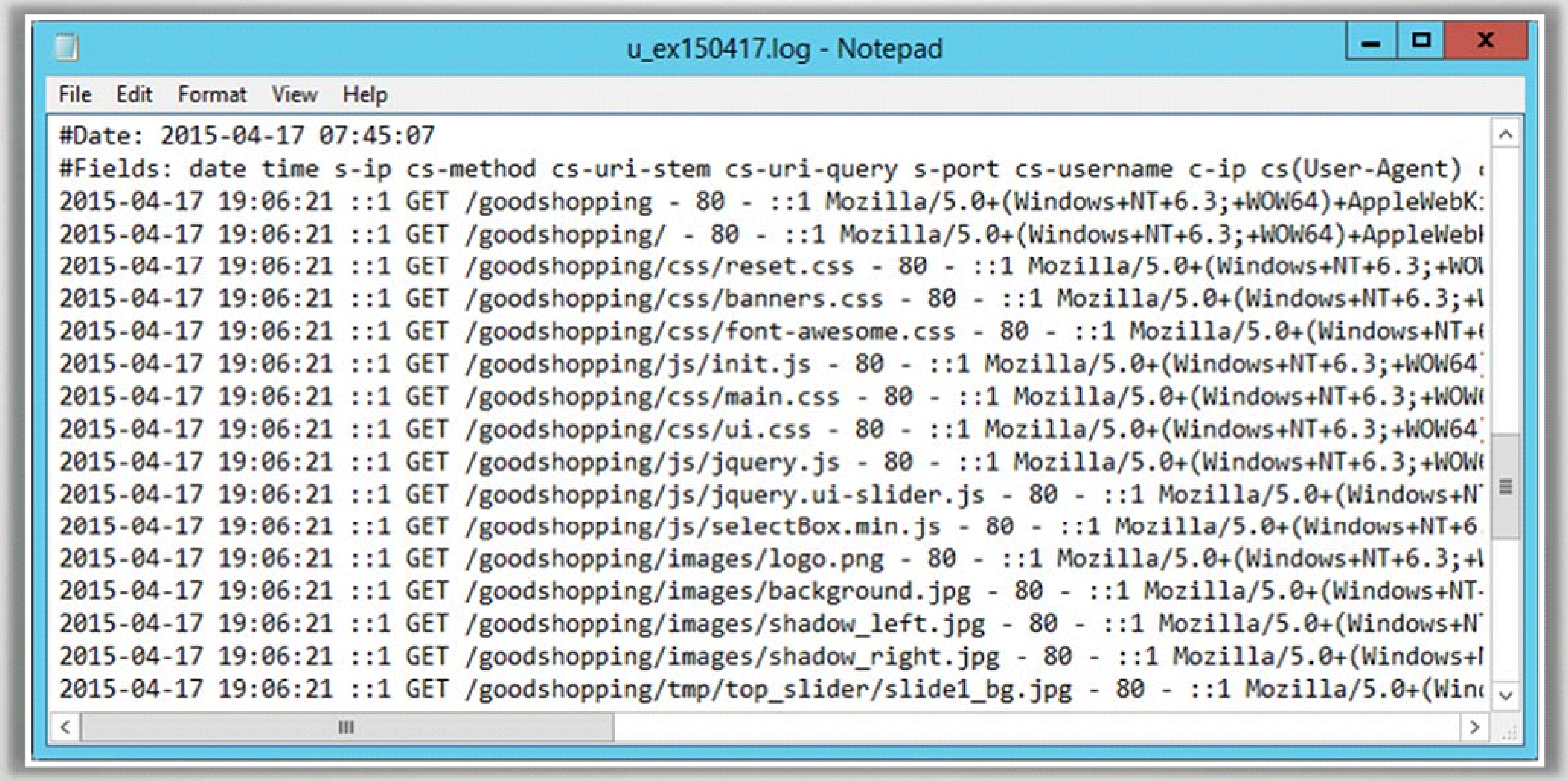
IIS Web Server Architecture


Client
Internet
Stack
HTTP Protocol Stack (HTTP.SYS)
Svchost.exe
Windows Activation Service (WAS)
WWW Service
External Apps
application Host.config
Application Pool
Web Server Core
Begin request processing, authentication, authorization, cache resolution, handler mapping, handler pre-execution, release state, update cache, update log and end request processing
Native Modules
Anonymous authentication, managed engine, IIS certificate mapping, static file, default document, HTTP cache, HTTP errors and HTTP logging
App Domain
Managed Modules
Forms Authentication

Internet Information Services (IIS) for Windows Server is a flexible, secure and easy-to-manage web server for hosting anything on the web

IIS Logs

- IIS logs all server **visits** in log files
- **IIS logs** provide useful **information** regarding the activity of various **Web applications**, such as connection time, IP address, user account, page URLs and actions
- The IIS server generates **ASCII text-based** log files
- On Windows Server 2012, the log files are stored by default in the *%SystemDrive%\inetpub\logs\LogFiles*



```
#Date: 2015-04-17 07:45:07
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent)
2015-04-17 19:06:21 ::1 GET /goodshopping - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+WOW64)+AppleWebK
2015-04-17 19:06:21 ::1 GET /goodshopping/ - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+WOW64)+AppleWeb
2015-04-17 19:06:21 ::1 GET /goodshopping/css/reset.css - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+WO
2015-04-17 19:06:21 ::1 GET /goodshopping/css/banners.css - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+
2015-04-17 19:06:21 ::1 GET /goodshopping/css/font-awesome.css - 80 - ::1 Mozilla/5.0+(Windows+NT+
2015-04-17 19:06:21 ::1 GET /goodshopping/js/init.js - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+WOW64
2015-04-17 19:06:21 ::1 GET /goodshopping/css/main.css - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+WOW
2015-04-17 19:06:21 ::1 GET /goodshopping/css/ui.css - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+WOW64
2015-04-17 19:06:21 ::1 GET /goodshopping/js/jquery.js - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+WOW
2015-04-17 19:06:21 ::1 GET /goodshopping/js/jquery.ui-slider.js - 80 - ::1 Mozilla/5.0+(Windows+N
2015-04-17 19:06:21 ::1 GET /goodshopping/js/selectBox.min.js - 80 - ::1 Mozilla/5.0+(Windows+NT+6
2015-04-17 19:06:21 ::1 GET /goodshopping/images/logo.png - 80 - ::1 Mozilla/5.0+(Windows+NT+6.3;+
2015-04-17 19:06:21 ::1 GET /goodshopping/images/background.jpg - 80 - ::1 Mozilla/5.0+(Windows+NT
2015-04-17 19:06:21 ::1 GET /goodshopping/images/shadow_left.jpg - 80 - ::1 Mozilla/5.0+(Windows+N
2015-04-17 19:06:21 ::1 GET /goodshopping/images/shadow_right.jpg - 80 - ::1 Mozilla/5.0+(Windows+
2015-04-17 19:06:21 ::1 GET /goodshopping/tmp/top_slider/slide1_bg.jpg - 80 - ::1 Mozilla/5.0+(Win
```

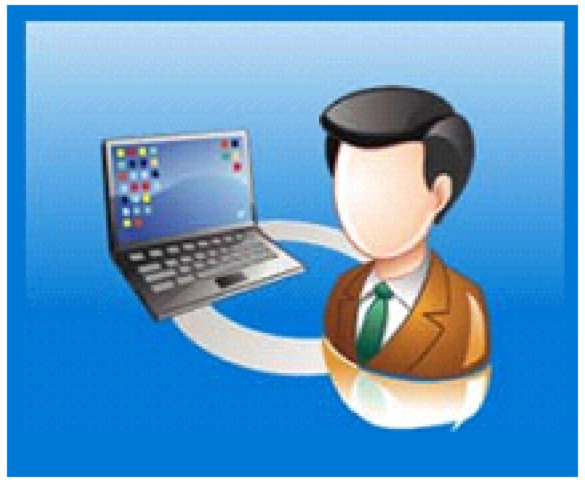
Investigating IIS Logs

- **Example of IIS log file entry as viewed in a text editor:**

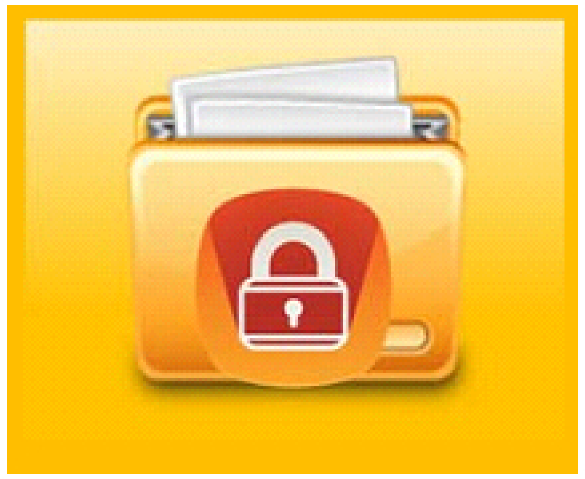
```
2016-02-10 06:11:41
192.168.0.10 GET
/images/content/bg_body_
1.jpg - 80 - 192.168.0.27
Mozilla/5.0+(Windows+NT+
6.3;+WOW64)+AppleWebKi
t/537.36+(KHTML,+like+Gec
ko)+Chrome/48.0.2564.103
+Safari/537.36
http://www.moviescope.co
m/css/style.css 200 0 0 365
```

Field	Appear As	Description
Date	**03/06/2015**	Log file entry was made on June 03, 2015
Time	**8:45:30**	Log life entry was recorded at 8:45 A.M
Server IP	**172.15.10.30**	IP address of the server
Client IP address	**192.168.100.150**	IP address of the client
cs-method	**GET**	The user issued a GET or download command
cs-uri-stem	**/images/content/bg_body_1.jpg**	The user wanted to download the bg_body_1.jpg file from the Images folder
cs-uri-query	**-**	The URI query did not occur (URI queries are necessary only for dynamic pages, such as ASP pages, so this field usually contains a hyphen for static pages.)
s-port	**80**	The server port
cs-username	**-**	The user was anonymous
c-ip	**192.168.0.27**	The IP address of the client
cs(User-Agent)	**Mozilla/5.0+(Windows+NT+6.3;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/48.0.2564.103+Safari/537.36**	The type of browser that the client used, as represented by the browser
cs(Referer)	**http://www.moviescope.com/css/style.css**	The Web page that provided the link to the Web site
sc-status	**200**	The request was fulfilled without error
time-taken	**365**	The action was completed in 365 milliseconds

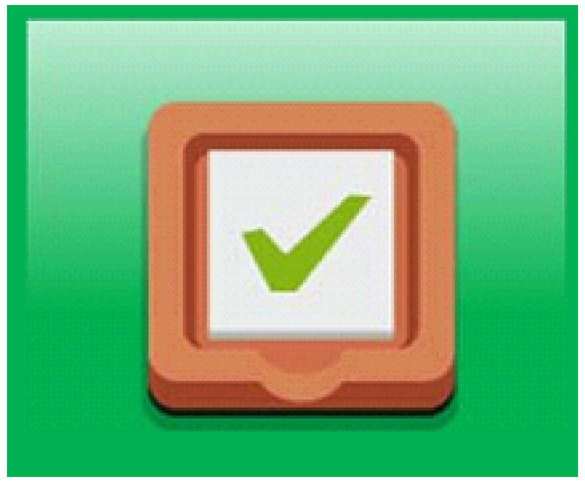
Maintaining Credible IIS Log Files



- Investigators must ask themselves certain questions before presenting IIS logs in court as evidence of web attack. This includes:
  - **What would happen if the credibility of the IIS logs was challenged in court?**
  - **What if the defense claims the logs are not reliable enough to be admissible as evidence?**



- An investigator must **secure the evidence** and ensure that it is accurate, authentic and accessible.



- In order to prove that the log files are valid, the investigator needs to present them as **acceptable and dependable sources** by providing convincing arguments, which makes them valid evidences.

Investigating IIS Logs: Best Practices

While handling IIS logs, the investigators must treat them carefully and consider these files as evidences

- IIS logs, in combination with other logs, such as firewall logs, IDS logs, and even TCPdump can provide more log credibility when used as an evidence
- Configure the IIS logs to record all the available fields
- Capture events with a accurate timestamp
- Maintain continuity in the logs
- Ensure IIS logs are not altered in any way from the time they have been originally recorded

Coordinated Universal Time (UTC)

IIS records logs using UTC

It helps in solving the synchronization issues when running servers in multiple time zones

Windows offsets the value of the system clock with the system time zone to calculate UTC

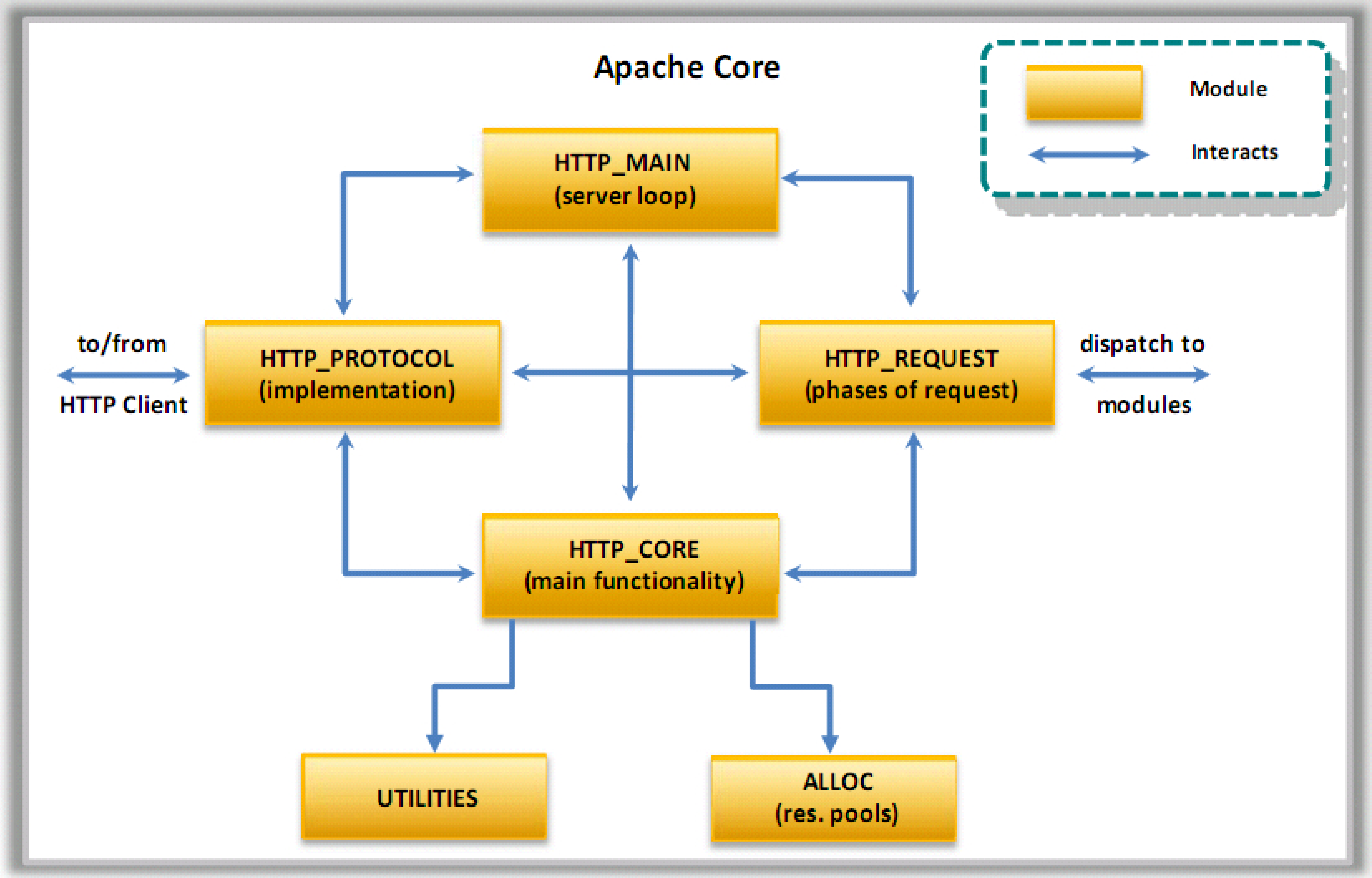
To check whether the UTC is correct, a network administrator must ensure accurateness of the local time zone setting

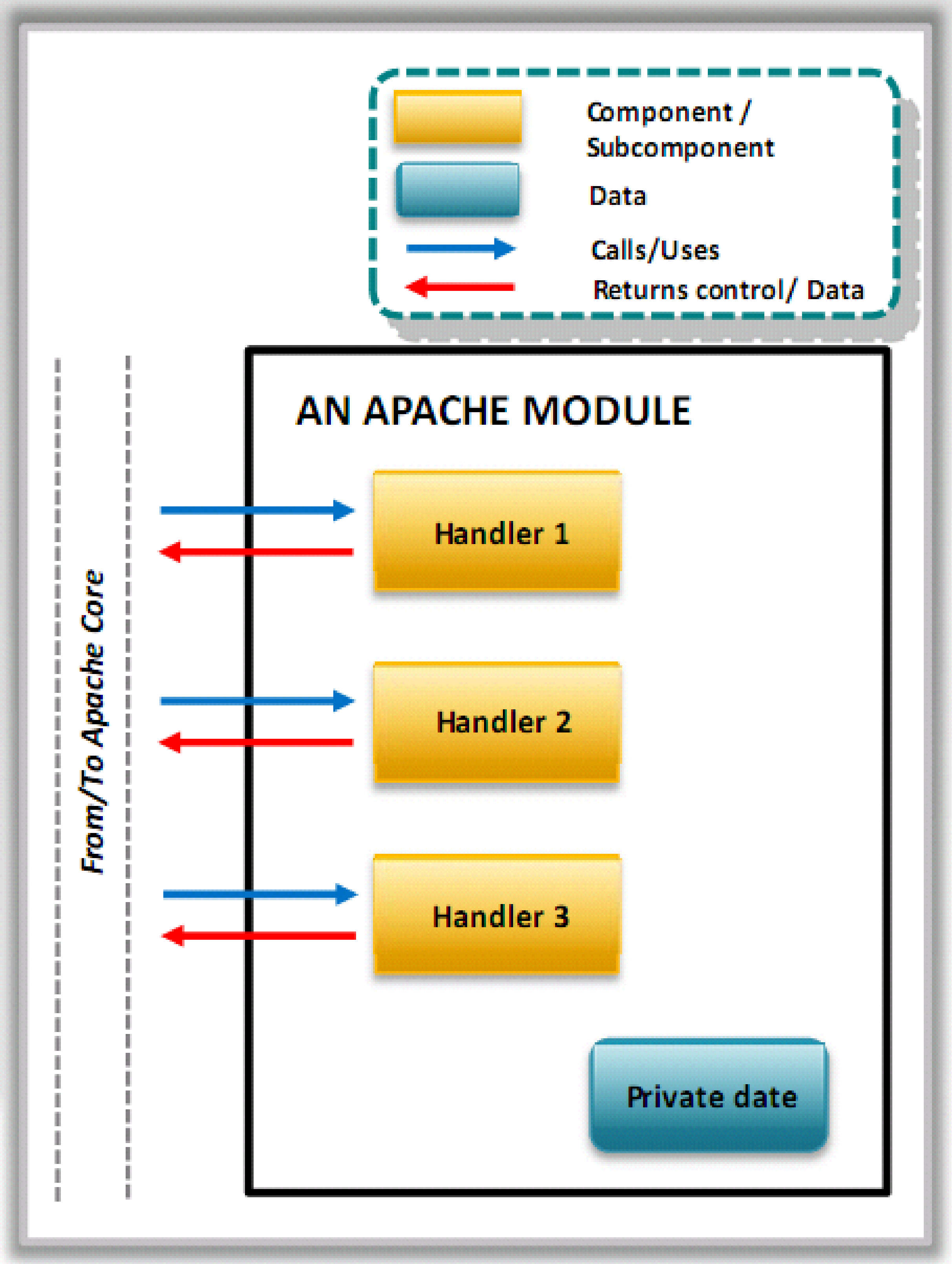
The network administrator must verify that during the process, the IIS is set to roll over logs using local time

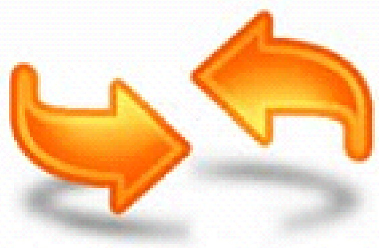
A network administrator can verify a server's time zone setting by looking at the first entries in the log file.

If the server is set to UTC -06:00, then the first log entries should appear around 18:00 (00:00 - 06:00 = 18:00).

Apache Web Server Architecture







Apache Web Server Logs

Apache HTTP Server

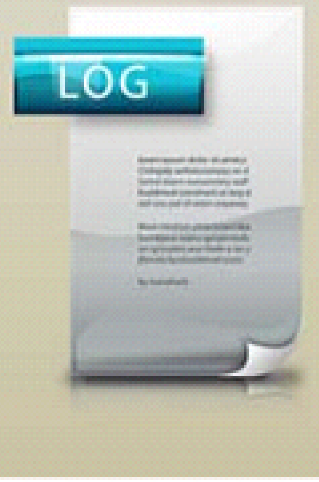
- Apache HTTP Server is a web server that supports many operating systems, such as Unix, GNU, FreeBSD, Linux, Solaris, Novell NetWare, AmigaOS, Mac OS X, Microsoft Windows, OS/2 and TPF

Apache Log Information

- Apache logs provide **information about web application** activities, such as:
  - **IP address of the client**
  - **Ident of client machine**
  - **User ID of client**
  - **Time**
  - **Request line from client**
  - **Status code**
  - **Size of the object returned to the client**

Apache Log Format

- Common Apache log format :
  - LogFormat "%h %l %u %t \"%r\" %>s %b" common
  - CustomLog “logs/access_log” common



Investigating Apache Logs

Error Log

- The Apache server saves **diagnostic information** and error messages that it encounters while processing requests in the error logs
- It is an important piece of **evidence** from an investigator's point of view
- The default location of error logs:

  RHEL/Red Hat/CentOS/Fedora Linux: `/var/log/httpd/error_log`

  Debian/Ubuntu Linux: `/var/log/apache2/error.log`

  FreeBSD: `/var/log/httpd-error.log`

Access Log

- It contains requests processed by the **Apache server**
- The default location of error logs:

  RHEL/Red Hat/CentOS/Fedora Linux: `/var/log/httpd/access_log`

  Debian/Ubuntu Linux: `/var/log/apache2/access.log`

  FreeBSD Linux: `/var/log/httpd-access.log`

Check the following locations for Apache configuration file to find the exact location of the log files:

- RHEL/Red Hat/CentOS/Fedora Linux: `/usr/local/etc/apache22/httpd.conf`
- Debian/Ubuntu Linux: `/etc/apache2/apache2.conf`
- FreeBSD: `/etc/httpd/conf/httpd.conf`

Investigating Apache Logs (Cont'd)

Access log/ Common Log format

```
"%h %l %u %t \"%r\" %>s %b"
```

Example of Apache access log file entry, as viewed in a text editor:

```
10.10.10.10 - jason [17/Aug/2016:00:12:34 +0300] "GET /images/content/bg_body_1.jpg
HTTP/1.0" 500 1458
```

Apache Log Fields		
%a - RemoteIPOrHost	%r - Request	%X - ConnectionStatus
%A - LocalIPOrHost	%>s - HttpStatusCode	%{Referer}i - Referer
%b or %B - Size	%t - eventTime	%{User-agent}i - UserAgent
%D - RequestTimeUs (microseconds)	%T - RequestTimeSeconds	%{UNIQUE_ID}e - UniqueId
%h - RemoteIPOrHost	%u - RemoteUser	%{X-Forwarded-For}i - XForwardedFor
%k - KeepAliveRequests	%U - UrlPath	%{Host}i - Host
%l - RemoteLogname	%v - VirtualHost	

Investigating Apache Logs (Cont'd)

Example of Apache error log file entry as viewed in a text editor:

```
[Mon Sep 16 14:25:33.812856 2016] [core:error] [pid 12485:tid 8589745621] [client
10.10.255.14] File does not exist: /images/content/bg_body_1.jpg
```

[First element] - Day, month, date, time, and year of the log

[Second element] - Severity of the error

[Third element] - Process ID and its corresponding thread ID

[Fourth element] - IP address of the client that generated the error

[Fifth element] - Message itself (In this example, the message shows that the "File does not exist")

Severity	Description	Example
emerg	Emergencies — system is unusable	"Child cannot open lock file. Exiting"
alert	Immediate action required	"getpwuid: couldn't determine user name from uid"
crit	Critical conditions	"socket: Failed to get a socket, exiting child"
error	Error conditions	"Premature end of script headers"
warn	Warning conditions	"child process 1234 did not exit, sending another SIGHUP"
notice	Normal but significant condition	"httpd: caught SIGBUS, attempting to dump core in ..."
info	Informational	"Server seems busy..."
debug	Debug-level messages	"opening config file ..."
trace1-8	Trace messages	"proxy: FTP: ... "

Investigating Cross-Site Scripting (XSS)

- Common XSS attacks use HTML tags, such as <script></script>, <IMG>, <INPUT>, <BODY>, etc.

- Attackers use various obfuscation techniques to avoid detection by application firewalls and IDS/IPS systems
  - Hex encoding
  - In-line comment
  - Char encoding
  - Toggle case
  - Replaced Keywords
  - White space manipulation

- For example, all the scripts below mean the same:
  <script>alert("XSS")</script>
  <sCRipT>alert("XSS")</ScRiPt>…………………………………………………(**Toggle case**)
  %3cscript%3ealert("XSS")%3c/script%3e>……………………………………(Hex encoding)
  %253cscript%253ealert(1)%253c/script%253e…………………………(Double encoding)

- Investigators can use regex search to find **HTML tags**, other XSS signature words and their equivalents in web access logs to check for XSS attacks

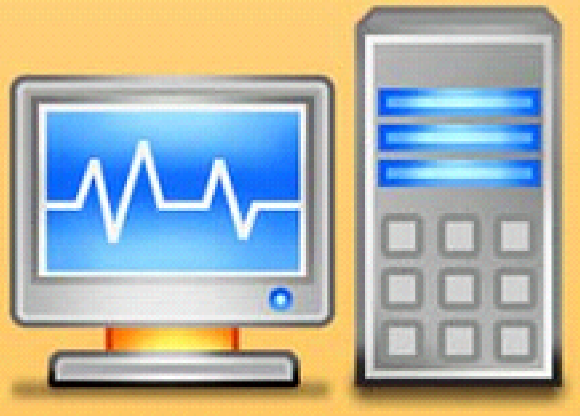
Investigating XSS: Using Regex to Search XSS Strings

- The regular expression below checks for attacks that may contain **HTML opening and closing tags** (<>) with any text inside, along with their hex and double encoding equivalents

- `/((\%3C)|(\%253C)|<)((\%2F)|(\%252F)|\/)*[a-zA-Z0-9\%]+((\%3E)|(\%253E)|>)/ix`
  - `((\%3C)|(\%253C)|<)` - Checks for opening angle bracket, its hex or double-encoded hex equivalent
  - `((\%2F)|(\%252F)|\/)*` - Checks for forward slash for a closing tag, its hex or double-encoded hex equivalent
  - `[a-zA-Z0-9\%]+` - Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation
  - `((\%3E)|(\%253E)|>)` - Checks for closing angle bracket, hex or double-encoded hex equivalent

Investigating SQL Injection Attacks

- Look for SQL injection attack incidents in these locations:
  - IDS log files
  - Database server log files
  - Web server log files



- The SQL injection attack signature in Web server log files may look as follows:

```
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah’ or 1=1 –
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah’ or )1=1 (--
12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah’ or exec master..xp_cmdshell 'net user test testpass  --
```

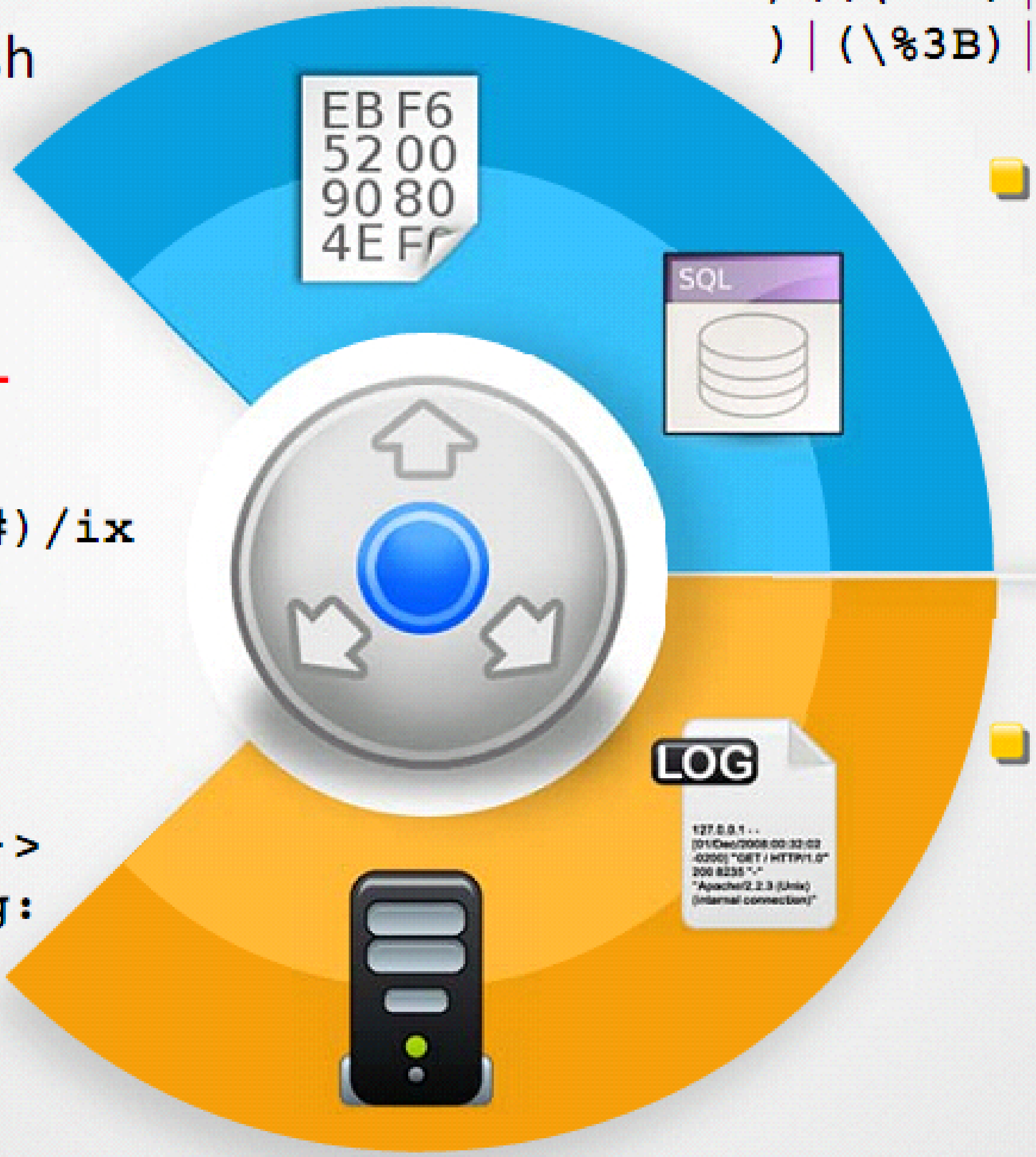
Investigating SQL Injection Attacks (Cont'd)

CHFI Computer Hacking Forensic Investigator

- The regular expression mentioned below **checks for attacks** that may contain SQL specific meta-characters, such as the single-quote (') or the double-dash (--) with any text inside and their hex equivalents

- **Regular expression for detection of SQL meta-characters:**
  - `/(\%27)|(\')|(\-\-)|(\%23)|(#)/ix`

- **Snort signature**
  ```
  alert tcp $EXTERNAL_NET any ->
  $HTTP_SERVERS $HTTP_PORTS(msg:
  "SQL Injection - Paranoid";
  flow:to_server, established;
  uricontent:“.pl";pcre:"/
  (\%27)|(\')|(\-\-)|(%23)
  |(#)/i"; classtype:Web-
  application-attack;
  sid:9099; rev:5;)
  ```



- **Modified Regular expression for detection of SQL meta-characters:**
  - `/((\%3D)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/i`

- **Regular expression for typical SQL injection attack:**
  - `/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix`

- **Regular expression for detecting SQL injection with the UNION keyword:**
  - `/((\%27)|(\'))union/ix`

- **Regular expression for detecting SQL injection attacks on a MS SQL Server:**
  - `/exec(\s|\+)+(s|x)p\w+/ix`

Pen-Testing CSRF Validation Fields

C|HFI Computer Hacking Forensic Investigator

Test 1

- Confirm that the **validation field** is unique for each user

Test 2

- Make sure that another user cannot identify the validation field
- If the attacker can create the same validation field for another user, then creation of a new validation field becomes valueless
- The **validation field must be unique** for each site

Test 3

- Verify that the **validation field** is never sent on the query string, because this data could be leaked to the attacker in places like the HTTP referrer

Test 4

- Verify that the **request fails** if the validation field is missing

Investigating Code Injection Attack

1. Intrusion detection systems (IDS) and a series of sandbox execution environments provided by the OS helps in detection of code injection attacks

2. When the IDS finds a series of executable instructions in the network traffic, it transfers the suspicious packet's payload to the execution environment matching the packet's destination

3. The proper execution environment is determined with the help of the destination IP address of the incoming packets

4. The packet payload is then executed in the corresponding monitored environment, and a report of the payload's OS resource usage is passed to the IDS

5. If the report contains evidence of OS resource usage, the IDS alerts the user that the incoming packet contains malicious data

Investigating Cookie Poisoning Attack

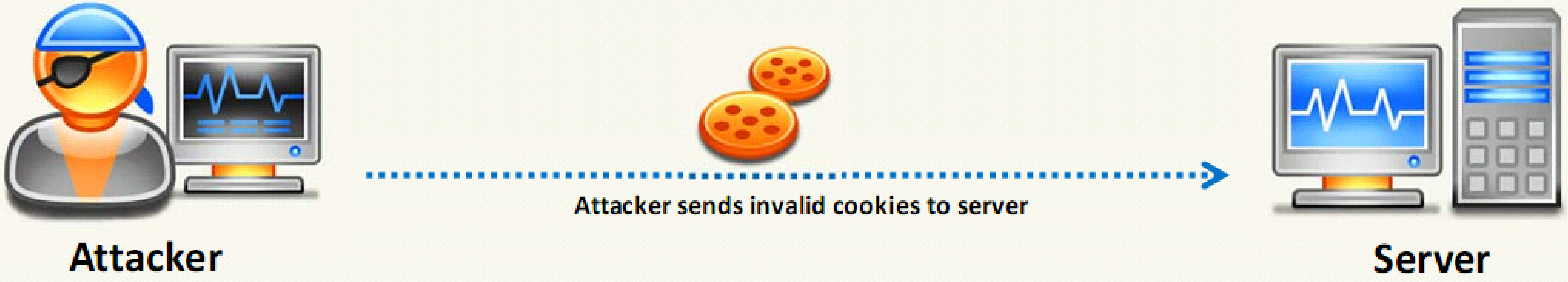
I Intrusion prevention products help in detecting cookie poisoning attacks

II These products trace the cookie's set command given by the Web server

III For every set command, information such as cookie name, cookie value, IP address, time, and the session to which the cookie was assigned is stored

IV After this, the intrusion prevention product catches every HTTP request sent to the Web server and compares any cookie information sent with all stored cookies

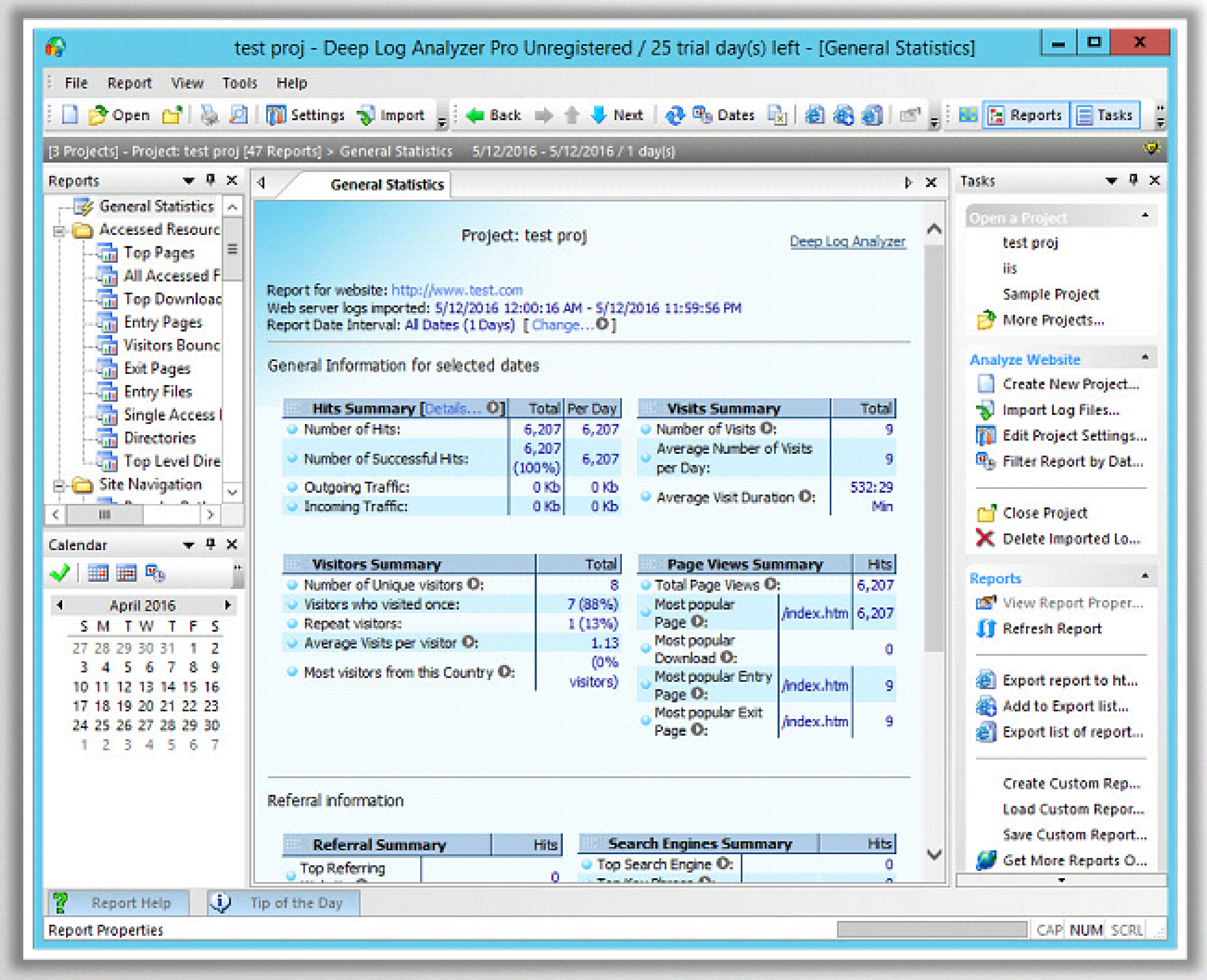
V If an attacker changes the cookie's contents, they will not match up with the stored cookies, and the intrusion prevention product will determine the occurrence of an attack



Web Log Viewers

Deep Log Analyzer

It is a web analytics solution that enables you to analyze logs from web servers, such IIS on Windows, Apache or Nginx on Unix/Linux and more



S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Project: test proj

Deep Log Analyzer

Report for website: http://www.test.com
Web server logs imported: 5/12/2016 12:00:16 AM - 5/12/2016 11:59:56 PM
Report Date Interval: All Dates (1 Days) [Change...]

General Information for selected dates

Hits Summary [Details...]	Total	Per Day
Number of Hits:	6,207	6,207
Number of Successful Hits:	6,207 (100%)	6,207
Outgoing Traffic:	0 Kb	0 Kb
Incoming Traffic:	0 Kb	0 Kb

Visits Summary	Total
Number of Visits :	9
Average Number of Visits per Day:	9
Average Visit Duration :	532:29 Min

Visitors Summary	Total
Number of Unique visitors :	8
Visitors who visited once:	7 (88%)
Repeat visitors:	1 (13%)
Average Visits per visitor :	1.13
Most visitors from this Country :	(0% visitors)

Page Views Summary		Hits
Total Page Views :		6,207
Most popular Page :	/index.htm	6,207
Most popular Download :		0
Most popular Entry Page :	/index.htm	9
Most popular Exit Page :	/index.htm	9

Referral information

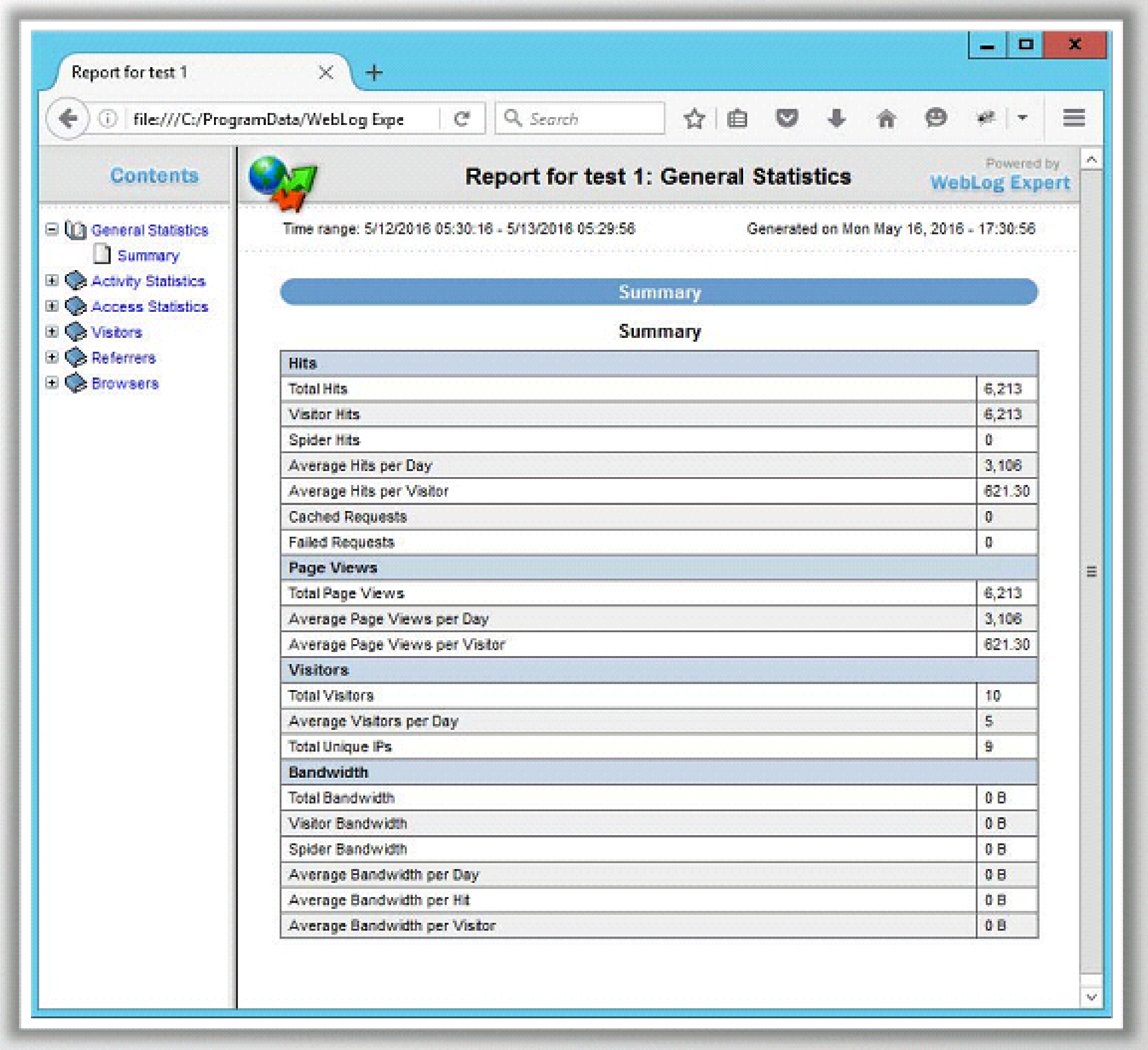
Referral Summary		Hits
Top Referring		0

Search Engines Summary		Hits
Top Search Engine :		0

http://www.deep-software.com

WebLog Expert

It is an access log analyzer that enables you to analyze logs of Apache, IIS and Nginx web servers



Report for test 1: General Statistics

Time range: 5/12/2016 05:30:16 - 5/13/2016 05:29:56

Generated on Mon May 16, 2016 - 17:30:56

Summary

Summary

Hits	
Total Hits	6,213
Visitor Hits	6,213
Spider Hits	0
Average Hits per Day	3,106
Average Hits per Visitor	621.30
Cached Requests	0
Failed Requests	0
Page Views	
Total Page Views	6,213
Average Page Views per Day	3,106
Average Page Views per Visitor	621.30
Visitors	
Total Visitors	10
Average Visitors per Day	5
Total Unique IPs	9
Bandwidth	
Total Bandwidth	0 B
Visitor Bandwidth	0 B
Spider Bandwidth	0 B
Average Bandwidth per Day	0 B
Average Bandwidth per Hit	0 B
Average Bandwidth per Visitor	0 B

https://www.weblogexpert.com

Web Log Viewers (Cont'd)

Apache Logs Viewer (ALV)
http://www.apacheviewer.com

AWStats
http://www.awstats.org

Nagios Log Server
https://www.nagios.com

Splunk
http://www.splunk.com

Web Log Storming
http://www.weblogstorming.com

LogCruncher
https://logentries.com

GoAccess
https://goaccess.io

HTTP-ANALYZE
http://http-analyze.org

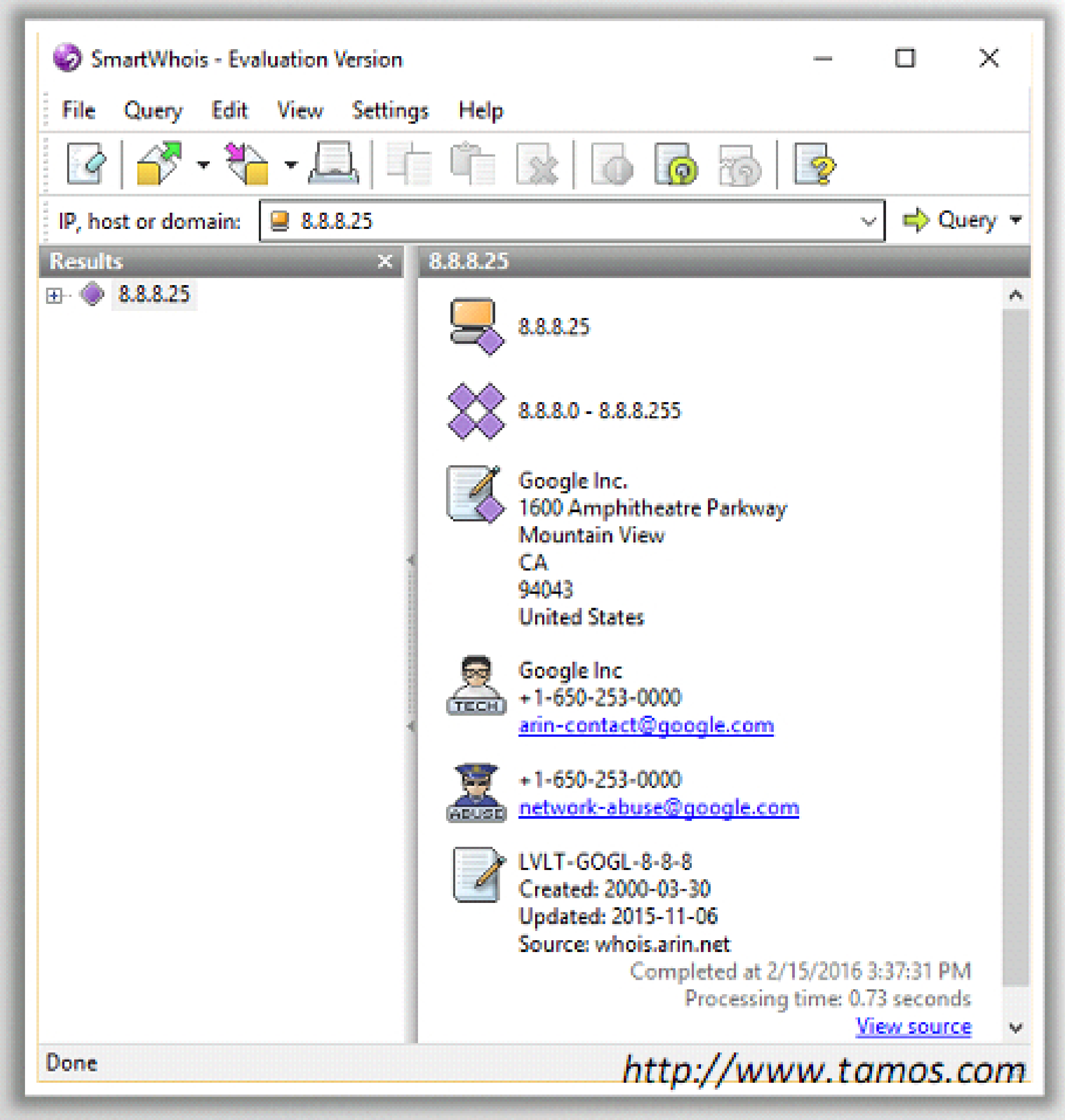
Active LogView
http://www.softcab.com

Webalizer
http://www.webalizer.org

IP Address Locating Tools

SmartWhois

- Network information utility that allows to look up for all the available information about an IP address, hostname or domain, including country, state or province, city, name of the network provider, administrator and technical support contact information


SmartWhois - Evaluation Version
File Query Edit View Settings Help
Results
8.8.8.25

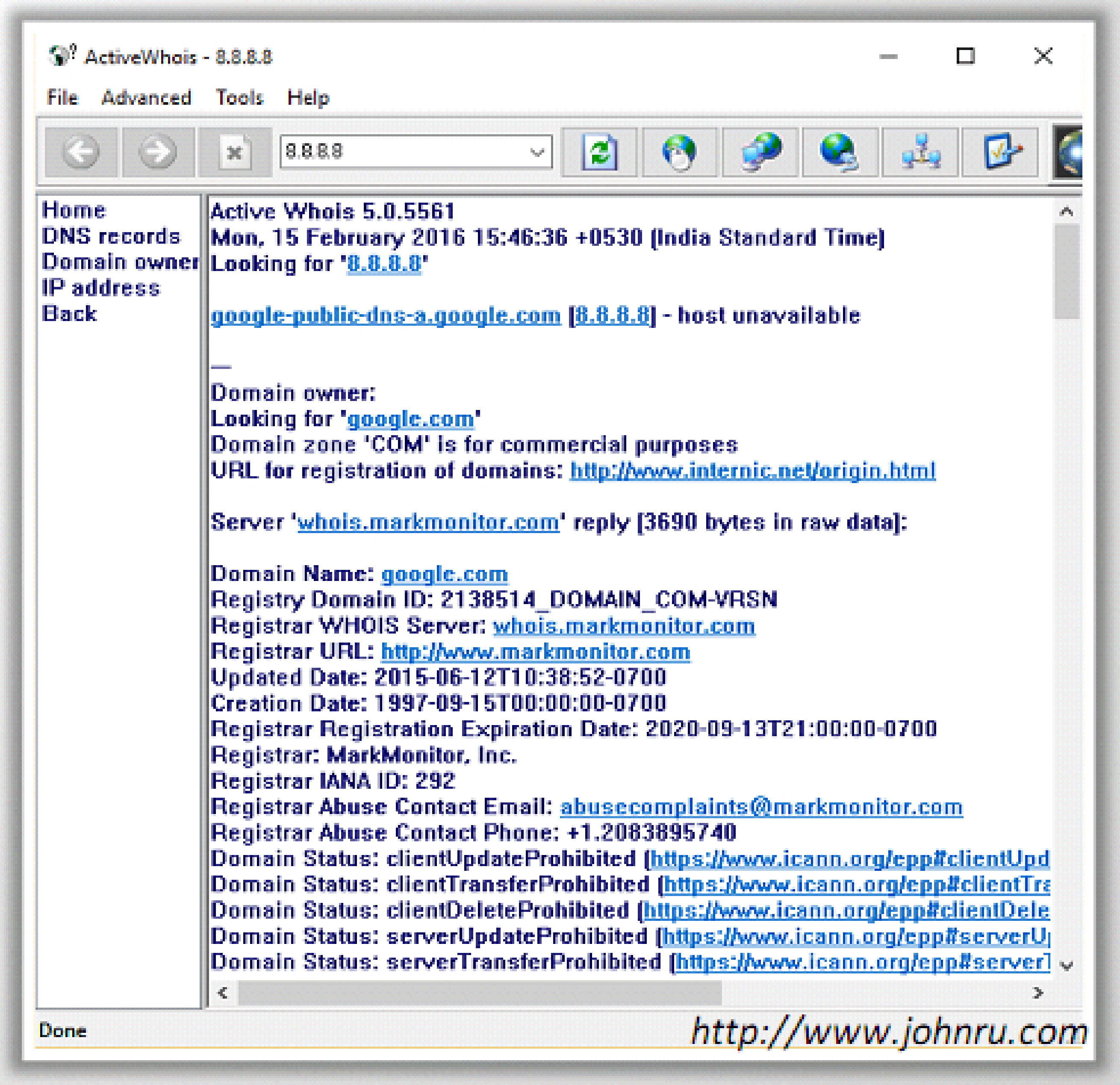
IP, host or domain: 8.8.8.25 Query

```
8.8.8.25

8.8.8.0 - 8.8.8.255

Google Inc.
1600 Amphitheatre Parkway
Mountain View
CA
94043
United States

Google Inc
+1-650-253-0000
arin-contact@google.com

+1-650-253-0000
network-abuse@google.com

LVLT-GOGL-8-8-8
Created: 2000-03-30
Updated: 2015-11-06
Source: whois.arin.net
                              Completed at 2/15/2016 3:37:31 PM
                                 Processing time: 0.73 seconds
                                                   View source
Done
```

http://www.tamos.com

ActiveWhois

- Network tool to find any information about the owners of IP address or Internet domain
- You can determine the country, personal and postal addresses of owner, and/or user of IP address and domains



```
Active Whois 5.0.5561
Mon, 15 February 2016 15:46:36 +0530 (India Standard Time)
Looking for '8.8.8.8'

google-public-dns-a.google.com [8.8.8.8] - host unavailable

—
Domain owner:
Looking for 'google.com'
Domain zone 'COM' is for commercial purposes
URL for registration of domains: http://www.internic.net/origin.html

Server 'whois.markmonitor.com' reply [3690 bytes in raw data]:

Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2015-06-12T10:38:52-0700
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpd
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTra
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDele
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverU
Domain Status: serverTransferProhibited (https://www.icann.org/epp#server1
Done
```

http://www.johnru.com

WHOIS Lookup Tools

LanWhoIs
http://lantricks.com

Batch IP Converter
http://www.networkmost.com

CallerIP
http://www.callerippro.com

Sobolsoft
http://www.sobolsoft.com

WhoIs Analyzer Pro
http://www.whoisanalyzer.com

HotWhoIs
http://www.tialsoft.com

ActiveWhoIs
http://www.johnru.com

WhoisThisDomain
http://www.nirsoft.net

SoftFuse Whois
http://www.softfuse.com

Whois
http://technet.microsoft.com

WHOIS Lookup Tools (Cont'd)

Domain Dossier
http://centralops.net

Whois
http://tools.whois.net

BetterWhois
http://www.betterwhois.com

DNSstuff
http://www.dnsstuff.com

Whois Online
http://whois.online-domain-tools.com

Network Solutions Whois
http://www.networksolutions.com

Web Wiz
http://www.webwiz.co.uk/domain-tools/whois-lookup.htm

WebToolHub
http://www.webtoolhub.com/tn561381-whois-lookup.aspx

Network-Tools.com
http://network-tools.com

UltraTools
https://www.ultratools.com/whois/home

Module Summary

CHFI Computer Hacking Forensic INVESTIGATOR

- ❑ Web applications provide an interface between the end users and web servers through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client Web browser
- ❑ An attack vector is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome
- ❑ Web defacement occurs when an intruder maliciously alters the visual appearance of a web page by inserting or substituting provocative and frequently offensive data
- ❑ Computer security logs contain information about the events occurring within an organization's systems and networks
- ❑ Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query
- ❑ Intrusion detection is the art of detecting inappropriate, incorrect or anomalous activity