Case 1 Web Server Investigation

FOR-480 Forensics Practicum

February, 2 2023

Investigation Conducted By: Noah Beckman

Table of Contents

Objectives

The idea of this lab is to generate a supertimeline 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
EvtxECmd
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

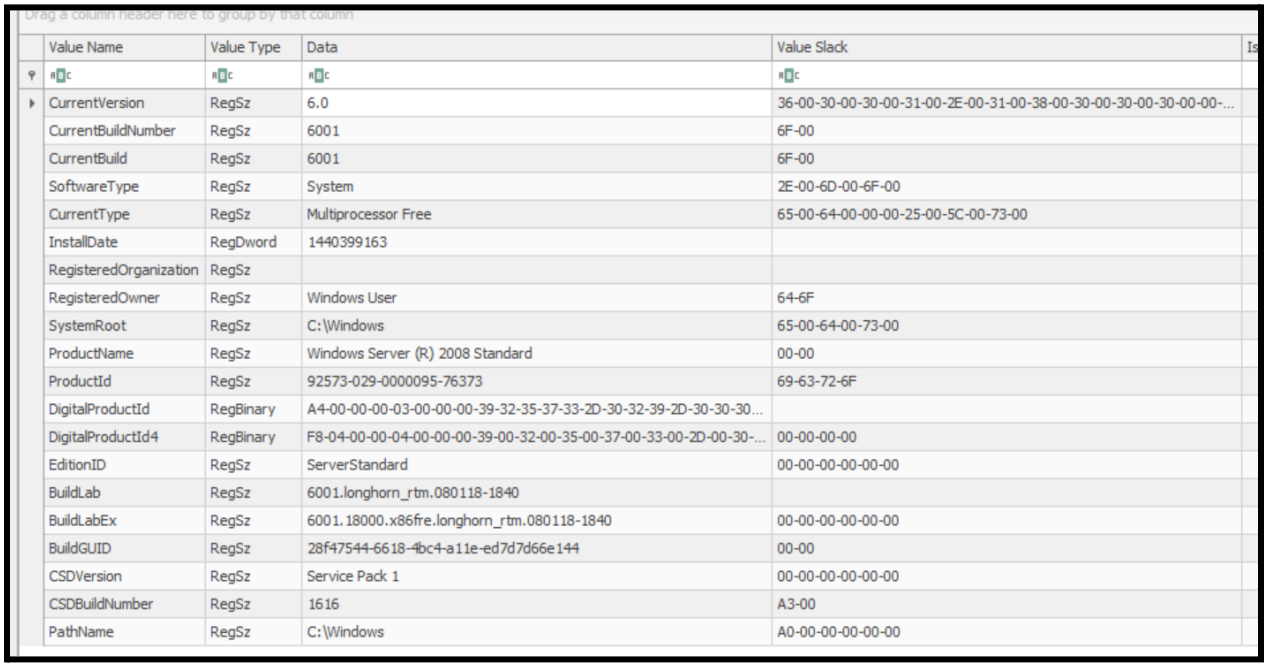
Windows Artifacts
- Prefetch
- Recycle Bin
- Lnk Files
- Jump Lists
- Shell Bags
- Windows Registry
- Windows Event Logs

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



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

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

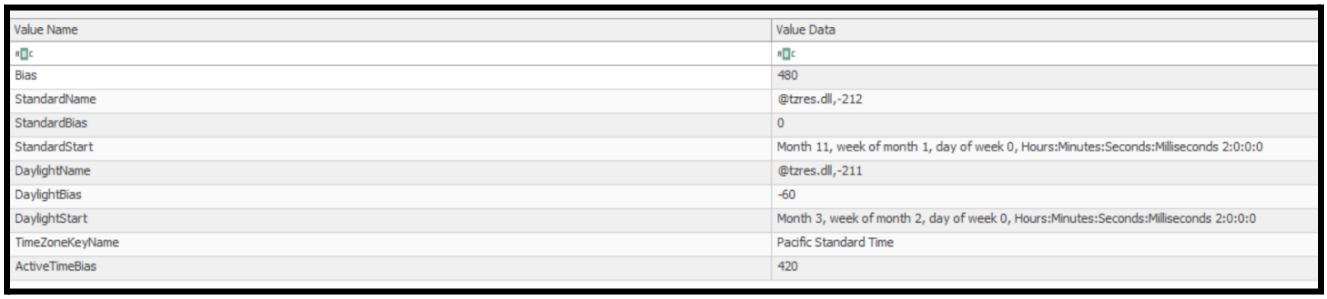
(default)	RegSz	mnmsrvc
ComputerName	RegSz	WIN-L0ZZQ76PMUF

The computer name of the E01 image is: WIN-L0ZZQ76PMU

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 being applied during the acquisition of the system.



Value Name	Value Data
▯c	▯c
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

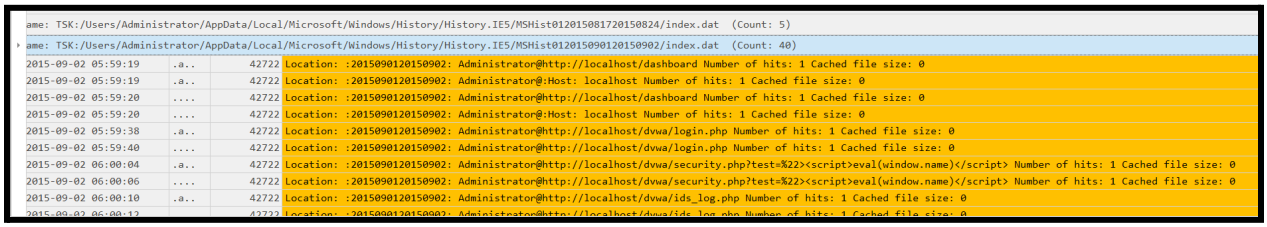
Investigation Findings

Do a thorough investigation and report back your findings.

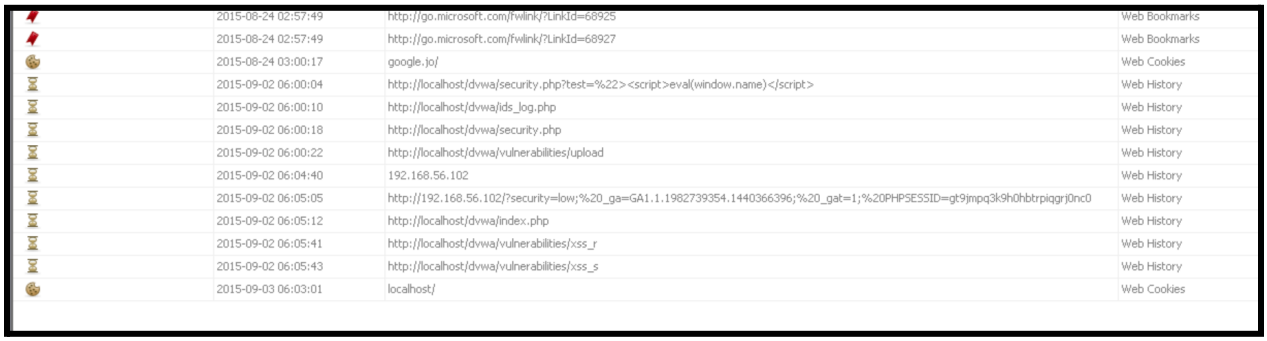
The web-server has been hit with an attack, what is it?

Attack 1: Cross Site Scripting (XSS Attack)

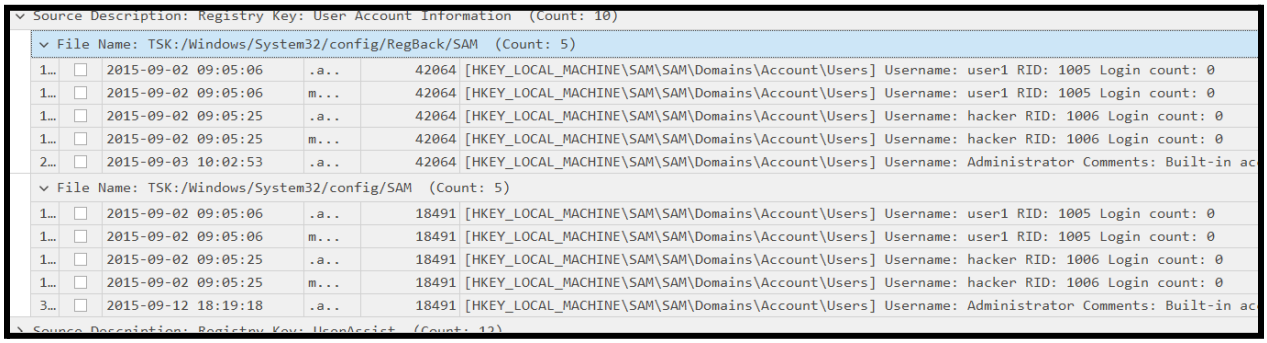
One of the main attacks on the system can be seen in the following logs from the image. The provided filtered log files reveals two XSS attack attempts on **2015-09-02 06:00:04** and **06:00:06**



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.

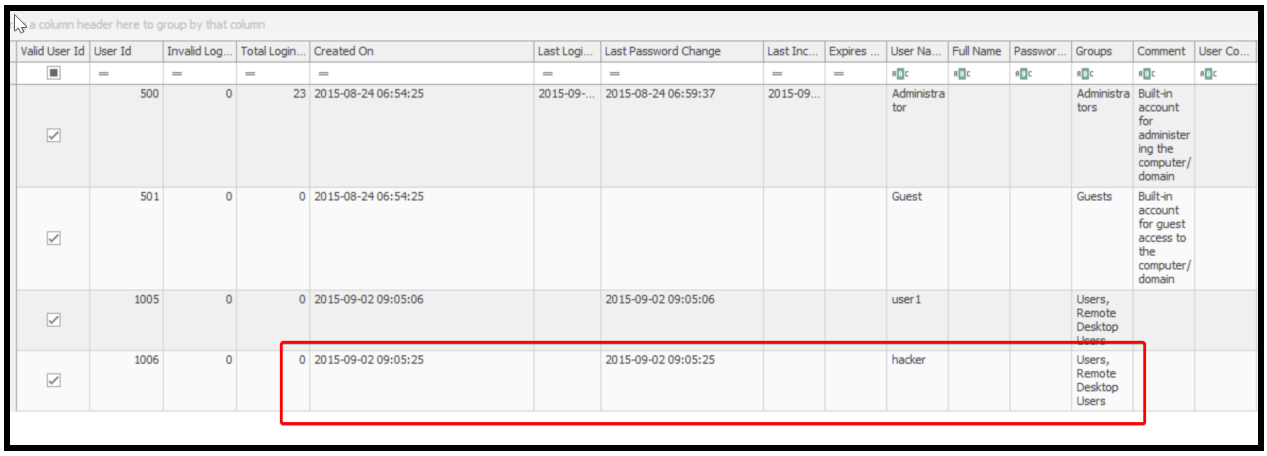


A few minutes later, a new user was created on the system named hacker. This can be seen under the TSK logs. Additional logs can be found in the SAM registry hive. This occurred at **2015-09-02 09:05:25**



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.

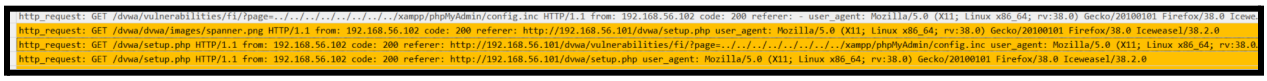


Valid User Id	User Id	Invalid Log...	Total Login...	Created On	Last Logi...	Last Password Change	Last Inc...	Expires ...	User Na...	Full Name	Passwor...	Groups	Comment	User Co...
☑	500	0	23	2015-08-24 06:54:25	2015-09-...	2015-08-24 06:59:37	2015-09...		Administrator			Administrators	Built-in account 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		

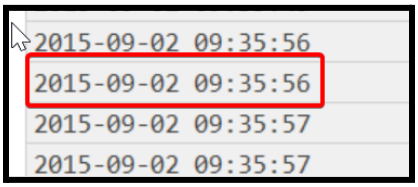
The creation date can be confirmed to be **2015-09-02 09:05:25.**

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.

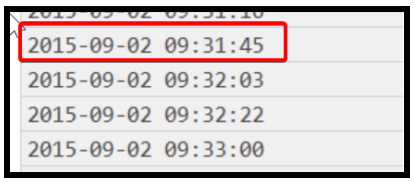


Directory Traversal 1



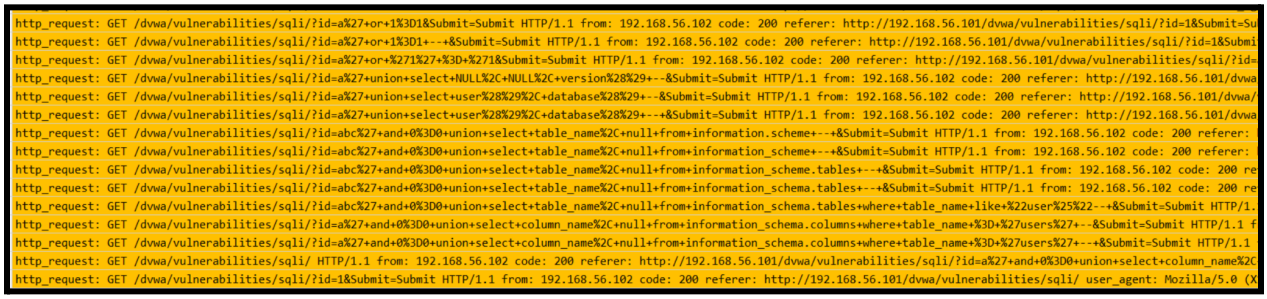
Time of attack

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.

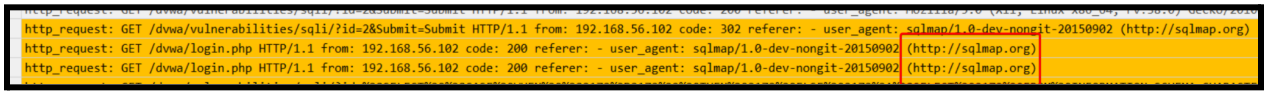


Attack 3: SQL Mapping for SQL injection

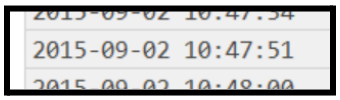
SQL mapping is an attack technique that automates the process of exploiting SQL injection flaws to gain access to databases. This type of attack is very noisy and a portion of the logs from the attack can be seen below. Within the screenshot the various sql commands can be seen trying to manipulate the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



We can confirm this is a sql mapping attack by looking at the end of the lines. The attacker is using sqlmap.org.

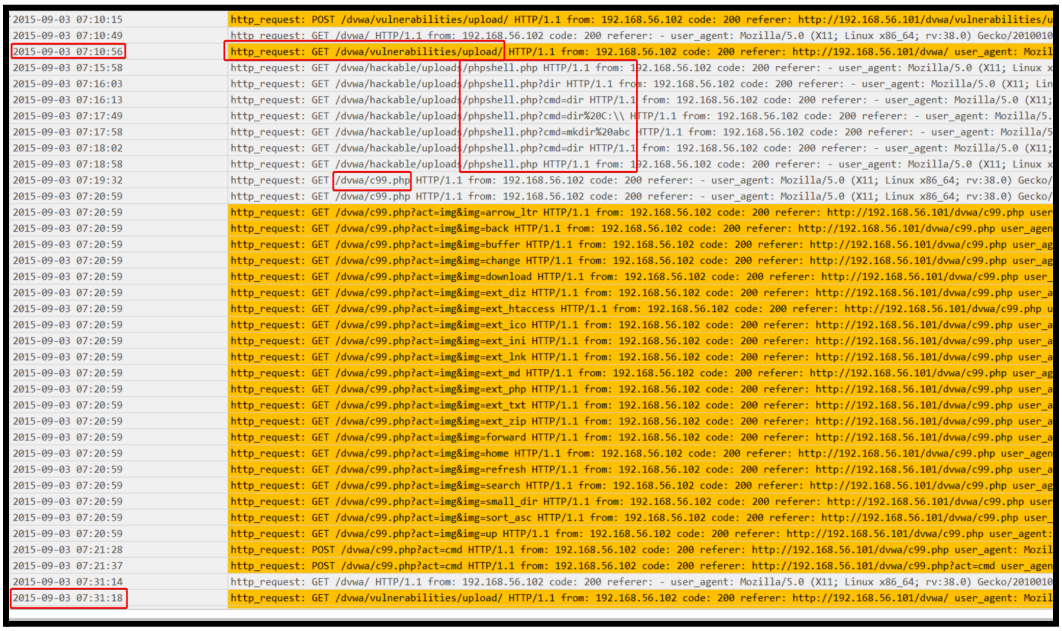


These attacks occurred over the course of time starting at **2015-09-02 10:47:51**

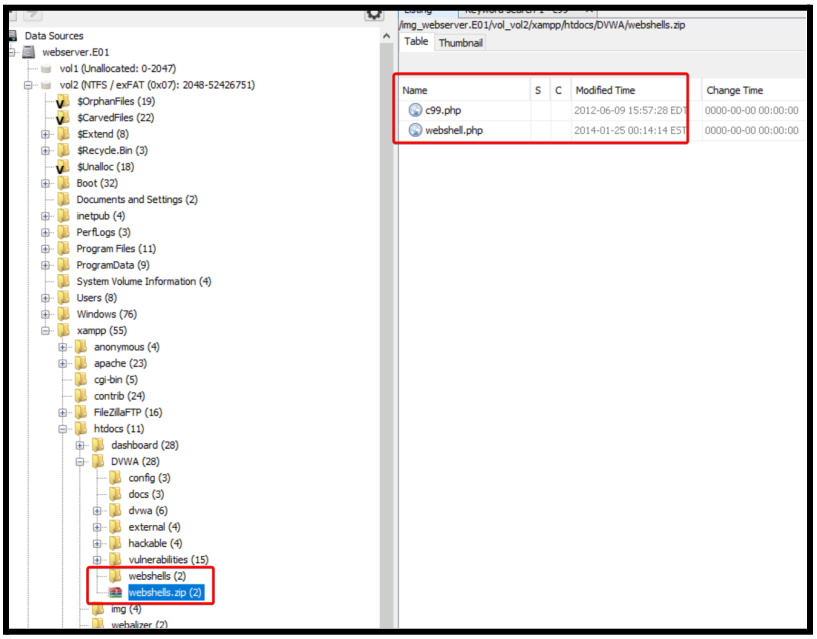


Attack 4: File Upload Vulnerability

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.

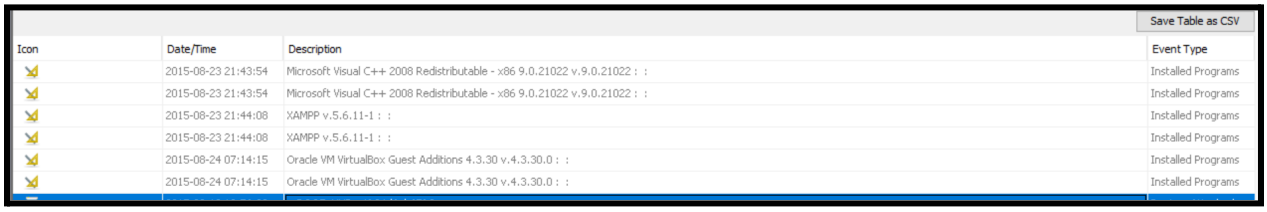


The webshell.php file accessed in the logs above can be seen in the file system below to further prove its upload and existence.



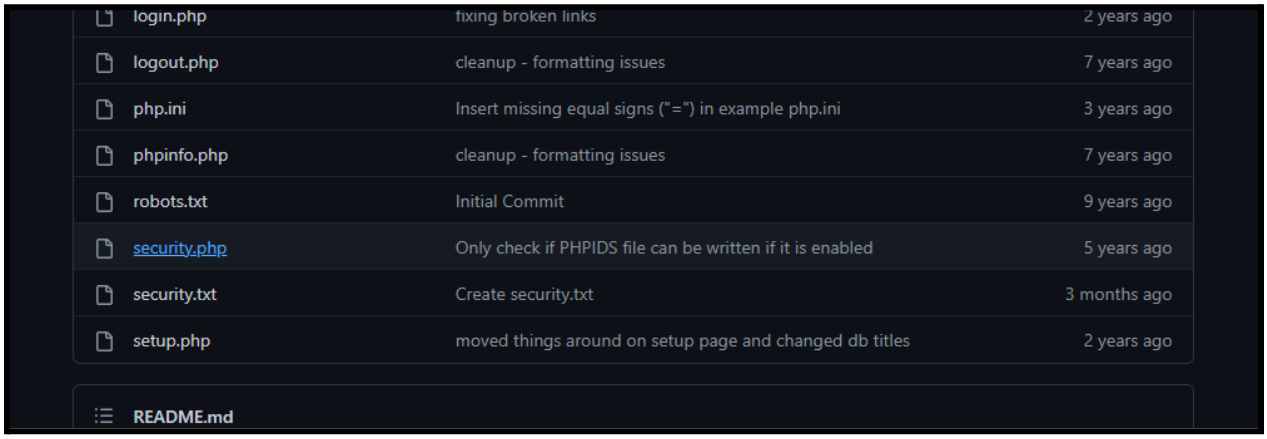
What software has been installed on the server by the threat actor?

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.



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.



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

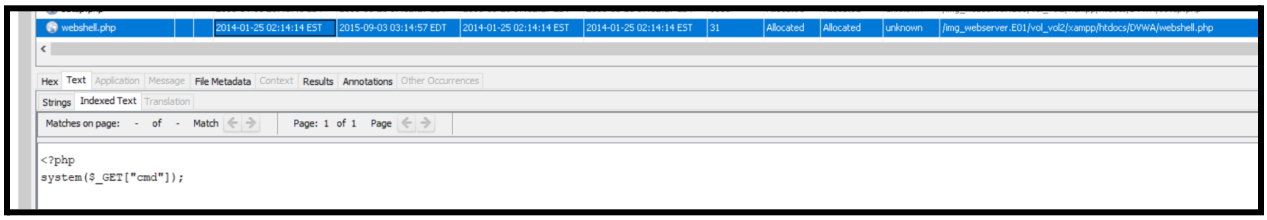
Name of File	Time	File Size	File Hash — SHA256
webshell.php	Modified Time 2014-01-25 00:14:14 EST	31 bytes	794F25B47B4773F6749B0F607F906E5181545ECA7835A927C9A197C94C3FD74B
webshells.zip	Access Time 2015-09-03 03:14:48 EDT	42095 bytes	BDAE3070D4D9A483A8F08DB4D16C9100723DEA6FBA3A7E53CBF249851BAD99EE
c99.php	Modified Time 2012-06-09 15:57:28 EDT	153275 bytes	4320d95cc2fe61e0b862756f8c4ffb251c7d1391e2f6841887c3dc765ba0369c
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	08245EEB54A5D973B20A82E03D82556A693F5C63310E01A2F492B78DDA132A99
phpshell2.php	Created Time 2015-09-03 03:31:30 EDT	945 bytes	2E77D2DB6FFBA49BE0CCF3850EE23DE61B289D1E2DFEE5B79E4D04563C42A1F7

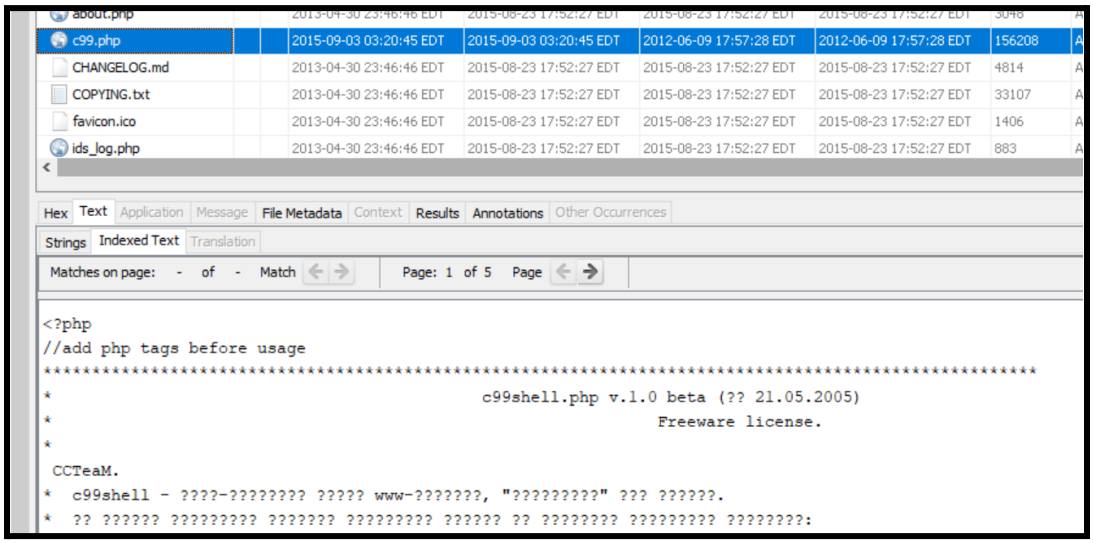
Malicious File Contents

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**

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



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.

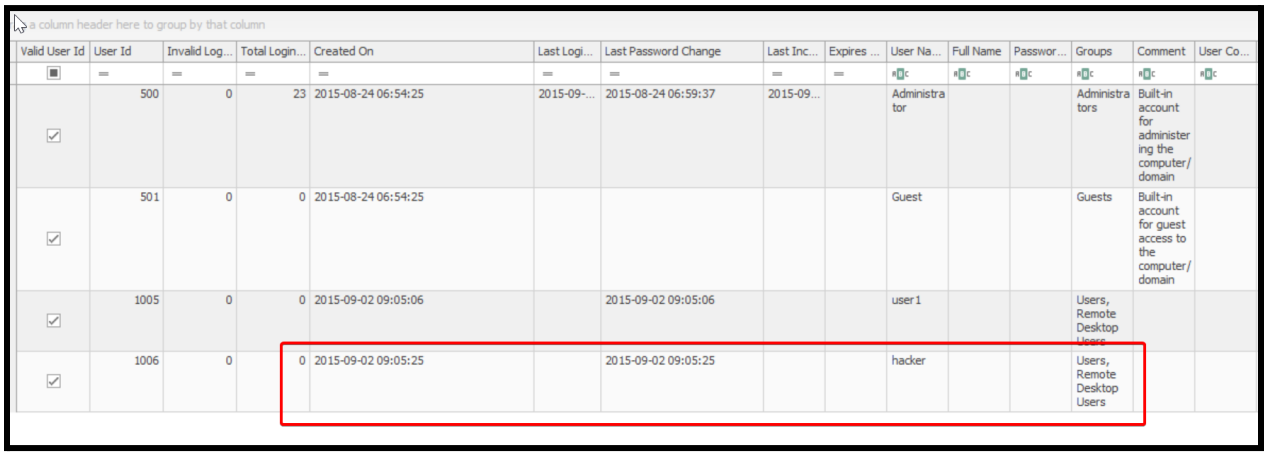


Google search result of c99.php

The screenshot below shows the contents of the phpshell2.php. This is a menu based php script for easier command execution.

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**



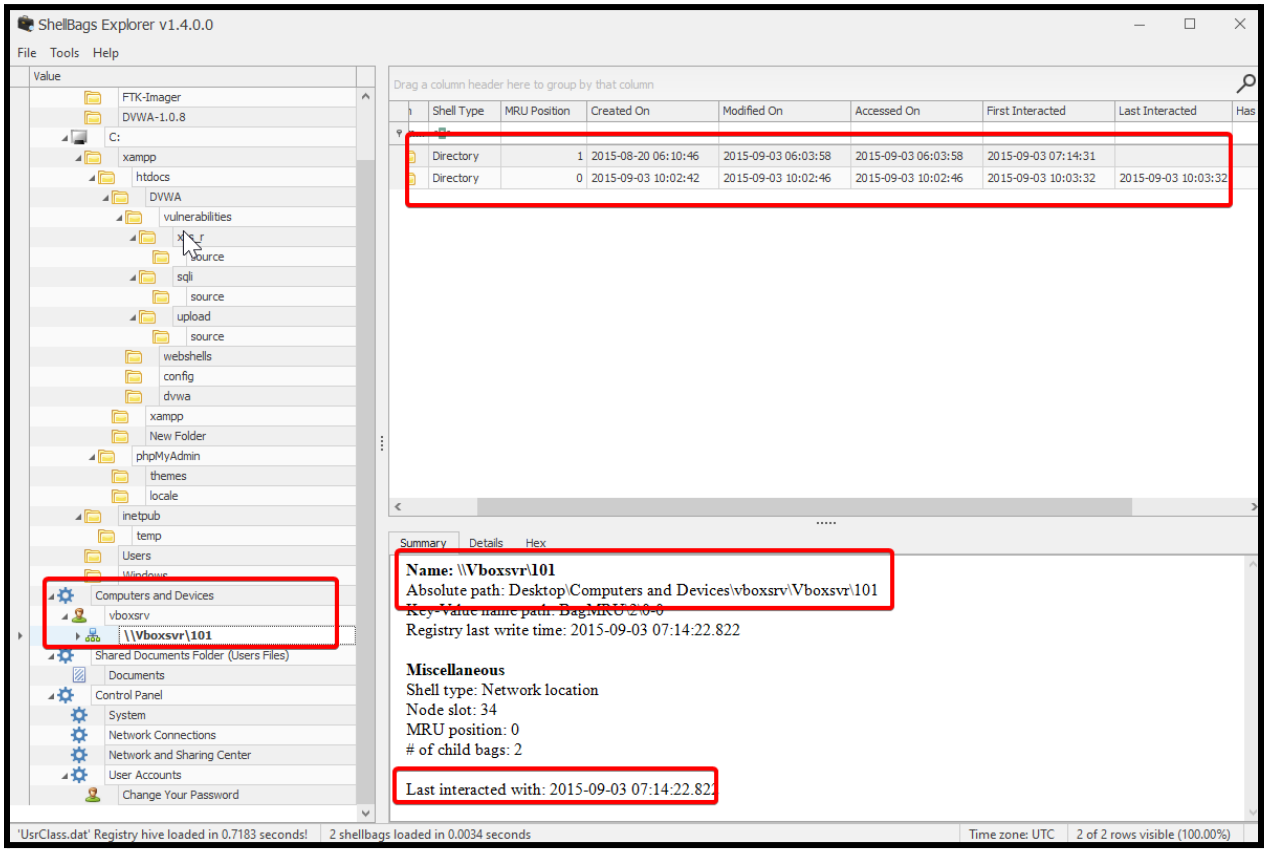
Valid User Id	User Id	Invalid Log...	Total Login...	Created On	Last Logi...	Last Password Change	Last Inc...	Expires ...	User Na...	Full Name	Passwor...	Groups	Comment	User Co...
☑	500	0	23	2015-08-24 06:54:25	2015-09-...	2015-08-24 06:59:37	2015-09...		Administrator			Administrators	Built-in account 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		

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.

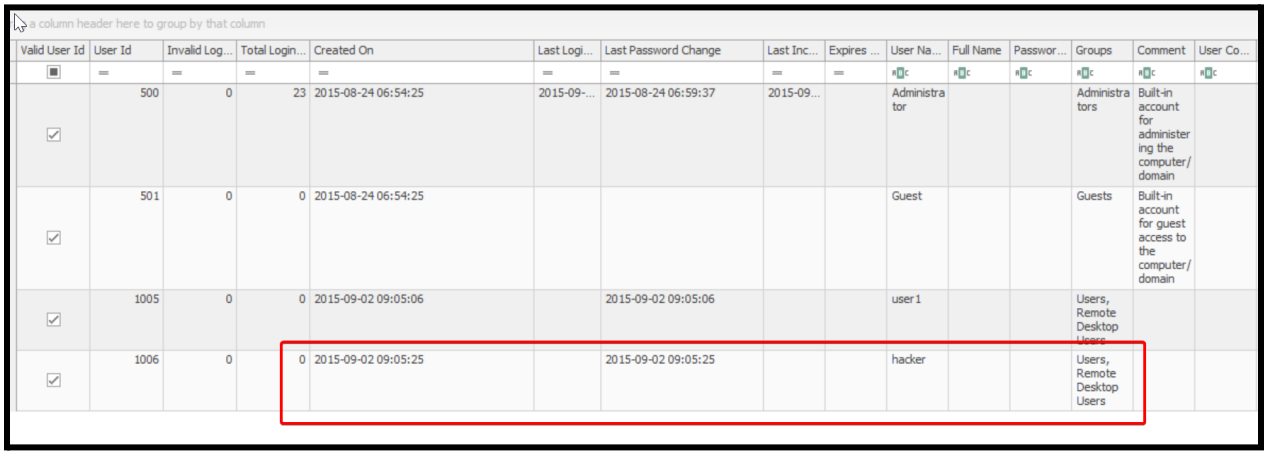
Shellbags

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.



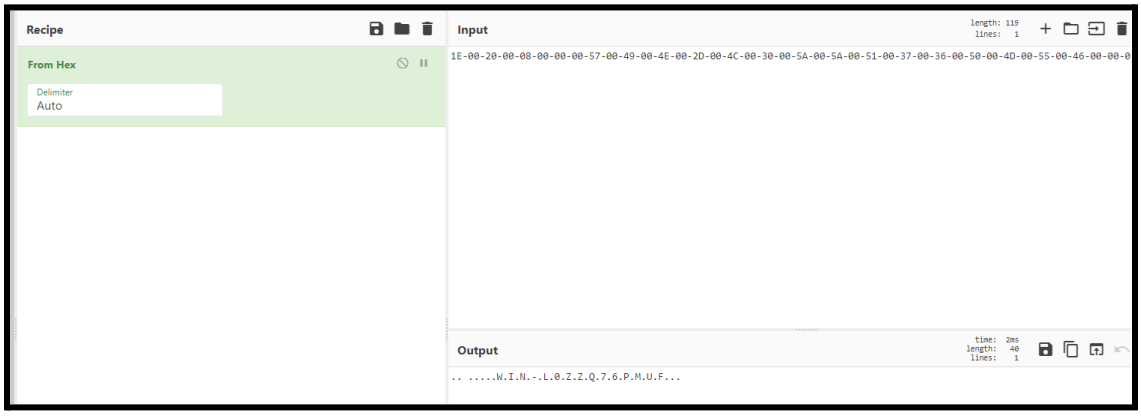
Registry Analysis

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**

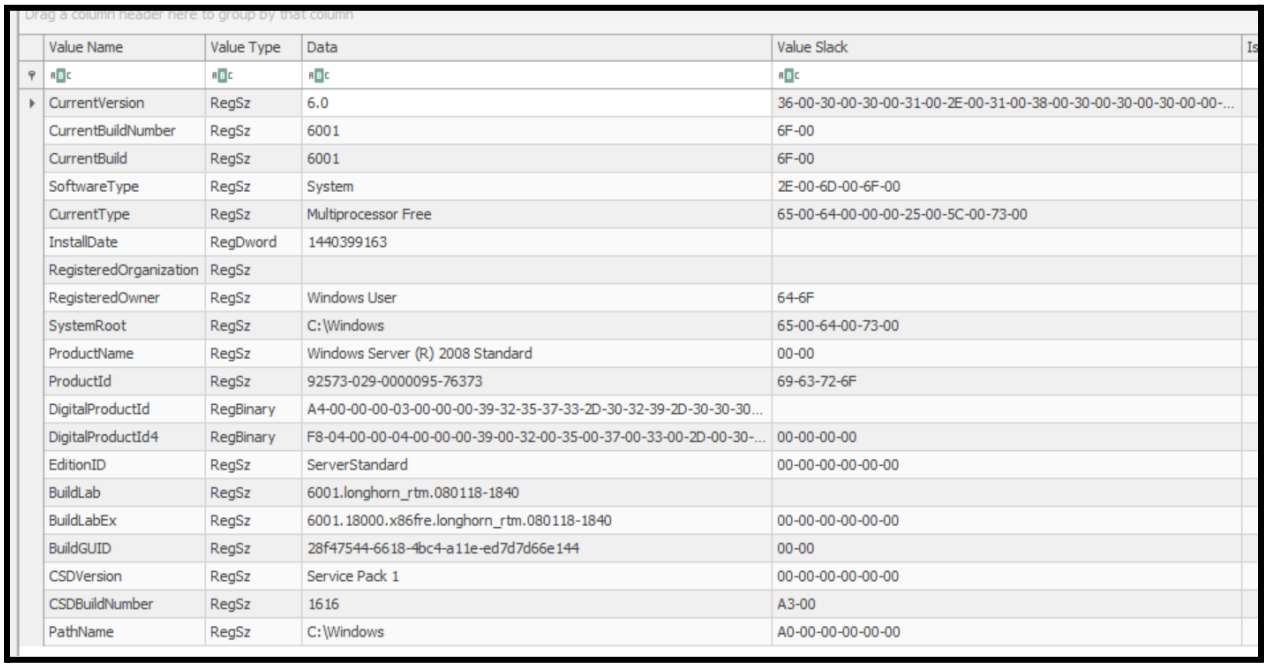


Valid User Id	User Id	Invalid Log...	Total Login...	Created On	Last Logi...	Last Password Change	Last Inc...	Expires ...	User Na...	Full Name	Passwor...	Groups	Comment	User Co...
☑	500	0	23	2015-08-24 06:54:25	2015-09-...	2015-08-24 06:59:37	2015-09...		Administrator			Administrators	Built-in account 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

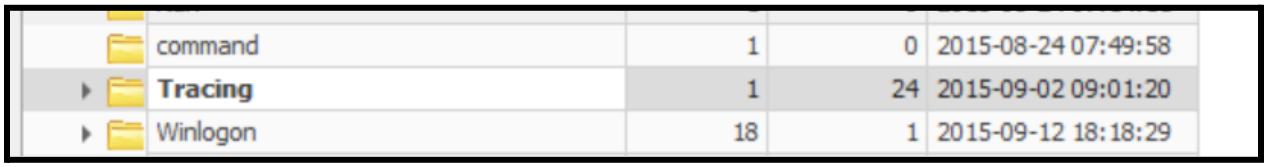


The next screenshot shows the system information for the image.



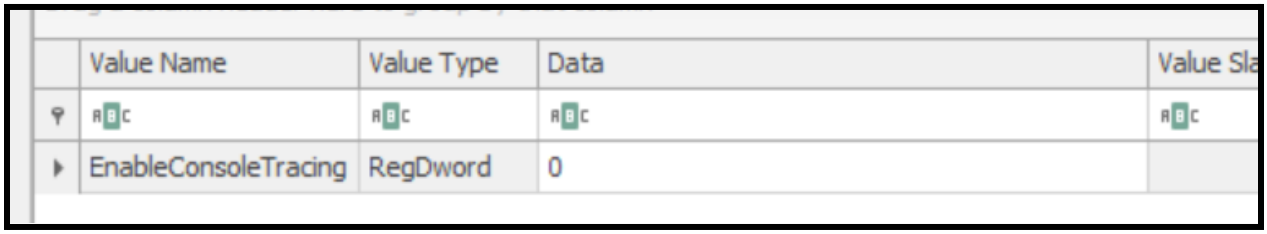
Value Name	Value Type	Data	Value Slack
CurrentVersion	RegSz	6.0	36-00-30-00-30-00-31-00-2E-00-31-00-38-00-30-00-30-00-30-00-00-...
CurrentBuildNumber	RegSz	6001	6F-00
CurrentBuild	RegSz	6001	6F-00
SoftwareType	RegSz	System	2E-00-6D-00-6F-00
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-25-00-5C-00-73-00
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.

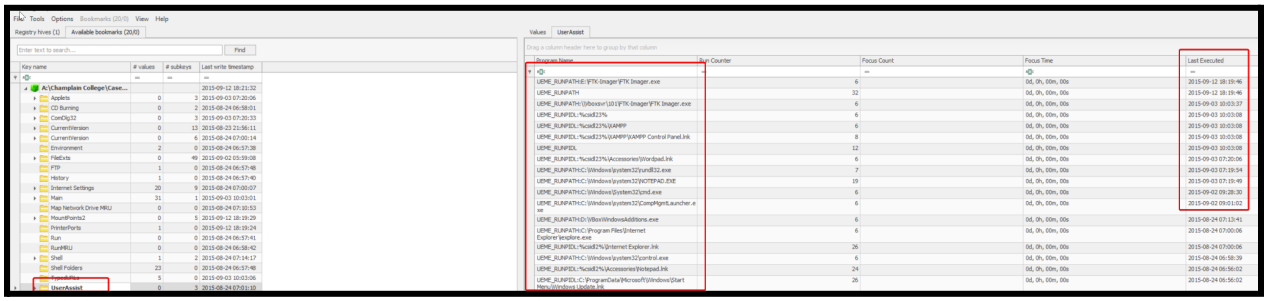


Value Name	Value Type	Data	Value Sla
EnableConsoleTracing	RegDword	0	

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	Slack
C:\xampp\phpMyAdmin	\vulnerabilities\sqli\source
C:\xampp	htdocs\DVWA\vulnerabilities\sqli\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