

# HR Server Woes 1

50

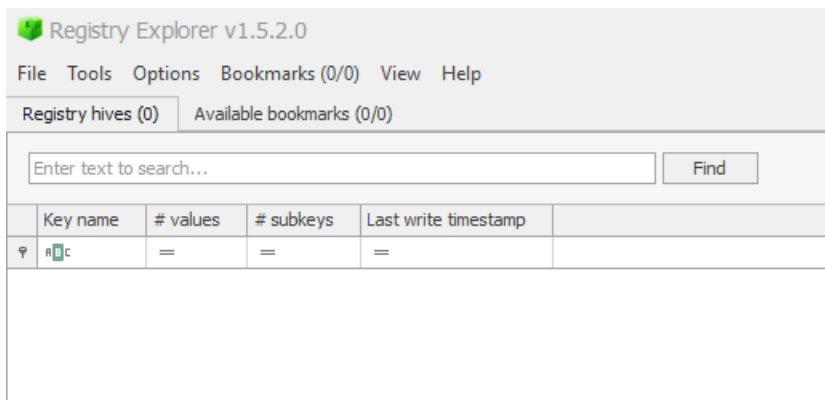
Use the files you download to examine the suspicious host. What is the hostname of this machine? [Link](#)

With using Zimmerman's tools to look in to a bunch of these items here is a link to install them:

<https://ericzimmerman.github.io/#!index.md>

The Registry Hive is in the extracted folder under VSS1\Windows\system32\config

For this one we will use Registry Explorer to look at the registry key for the active computer name:



Load the system hive:

C:\Users\John\Downloads\CTF\may\hr\VSS1\Windows\system32\config\SYSTEM			
Associated deleted records	0	0	
ROOT	0	15	2018-07-11 23:40:03
ActivationBroker	0	1	2018-02-02 19:39:11
ControlSet001	0	6	2018-05-07 13:54:53
ControlSet002	0	6	2018-02-02 19:38:58
DriverDatabase	3	4	2018-05-01 15:04:23
HardwareConfig	2	2	2018-07-11 23:40:04
Keyboard Layout	0	2	2018-02-02 19:39:13
Maps	0	1	2018-02-02 19:39:13
MountedDevices	5	0	2018-05-07 14:03:56
ResourceManager	2	4	2018-02-02 19:39:13
ResourcePolicyStore	0	2	2018-02-02 19:39:13
RNG	2	0	2018-07-11 23:40:04
Select	4	0	2018-02-02 19:39:13
Setup	11	8	2018-07-11 23:40:16
Software	0	1	2018-02-02 19:39:13
WPA	0	16	2018-08-01 16:44:10
Unassociated deleted records	0	0	
Unassociated deleted values	182	0	

Go to Root/ControlSet001/Control/Computername/Computername

ActivationBroker	0	1	2018-02-02 19:39:11
ControlSet001	0	6	2018-05-07 13:54:53
Control	10	101	2018-07-11 23:40:13
{7746D80F-97E0-4E26-9543-26B41FC22F79}	1	6	2018-02-02 20:04:17
ACPI	1	0	2018-02-02 19:39:13
AppID	0	2	2018-02-02 19:39:13
AppReadiness	1	0	2016-07-16 13:24:05
Arbiters	0	3	2018-02-02 19:39:13
BackupRestore	0	3	2018-02-02 19:39:13
CI	0	2	2018-02-02 19:39:13
Class	0	109	2018-02-02 19:40:17
CMF	2	4	2018-05-01 21:56:17
CoDeviceInstallers	0	0	2018-02-02 19:39:13
COM Name Arbiter	1	0	2018-02-02 20:03:13
CommonGlobUserSettings	0	1	2018-02-02 19:39:13
Compatibility	0	1	2018-02-02 19:39:13
ComputerName	0	1	2018-07-11 23:40:11
ComputerName	2	0	2018-05-01 21:55:44

We see the ComputerName key and our answer:

Drag a column header here to group by that column					
	Value Name	Value Type	Data	Value Slack	Is Deleted
▼	ntfs	ntfs	ntfs	ntfs	
▶	(default)	RegSz	mmsrvc	DC-00-00-00	
	ComputerName	RegSz	WIN-29U41M70JCO	88-1D-42-00	

Flag: WIN-29U41M70JCO

## 50

Unlock Hint for 10 points

From here we can see the version of the operating system.

Flag: Windows Server 2016 Datacenter

Flag: Windows Server 2016 Datacenter

## HR Server Woes 3

50

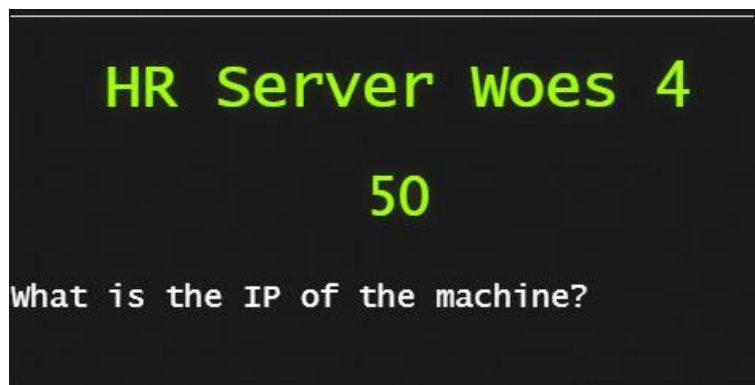
What is the timezone of the machine?  
Answer should be three letters.

We will go back to the CurrentControlSet from the hostname question, but instead go to \ControlSet001\Control\TimeZoneInformation

TabletPC	0	1	2018-02-02 19:39:13
Terminal Server	19	13	2018-07-11 16:42:54
<b>TimeZoneInformation</b>	10	0	2018-05-01 22:55:19
...	75	0	2018-02-02 19:39:13

[illegible]

Flag: pst



For this one we will go move to a different key:

`\CurrentControlSet\Services\Tcpip\Parameters\Interfaces`

Here we see there are three interfaces but only one has IP information

Tcpip	13	5	2018-02-02 19:39:13
Linkage	3	0	2018-05-01 22:00:23
Parameters	10	6	2018-07-11 23:40:12
Adapters	0	2	2018-05-01 22:00:23
DNSRegisteredAdapters	0	0	2018-02-02 19:39:21
Interfaces	0	3	2018-05-01 22:00:23
{22a461ff-64fe-48a0-b486-1feecf41a56e}	3	0	2018-02-02 19:39:28
{a942f1a4-0850-11e8-b7e6-806e6f6e6963}	0	0	2018-02-02 19:39:18
{d640cc3b-357e-40f1-9f24-192946fb909a}	20	0	2018-08-06 23:42:25
NsiObjectSecurity	0	0	2016-07-16 13:24:04

DhcpIPAddress	RegSz	74.118.139.108	00-00-60-3C-8F-00
DhcpSubnetMask	RegSz	255.255.255.0	34-00-00-00-6D-00-61-00
DhcpServer	RegSz	204.16.247.14	35-00-00-00-46-00-34-00

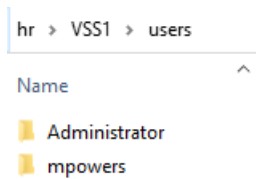
Flag: 74.118.139.108

# HR Server Woes 5

80

What are the names of the users on this system? Flag format: acct1,acct2,... (no spaces). Do not include the account "Default"

For this one we can just browse the file system under the vss1\users folder



Flag: Administrator,mpowers

# HR Server Woes 6

80

What is the file name that represents  
MFT Entry 168043?

We will open up an Administrator PowerShell and will use this to convert the \$MFT file into a CSV file to find the entry we need.

```
debug          Show debug information during processing
trace         Show trace information during processing

Examples: MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out" --csvf MyOutputFile.csv
MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out"
MFTECmd.exe -f "C:\Temp\SomeMFT" --json "c:\temp\out"
MFTECmd.exe -f "C:\Temp\SomeMFT" --body "c:\temp\out" --bdl c
MFTECmd.exe -f "C:\Temp\SomeMFT" --de 3-5

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

-f is required. Exiting
PS C:\Users\John\Downloads\CTF\Get-ZimmermanTools> .\MFTECmd.exe -f '..\may\hr\VSS1\$MFT' --csv ..\may\hr\mft.csv
MFTECmd version 0.5.0.0
Author: Eric Zimmerman (saeericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f ..\may\hr\VSS1\$MFT --csv ..\may\hr\mft.csv
Warning: Administrator privileges not found!
File type: MFT

MFTECmd version 0.5.0.0
Author: Eric Zimmerman (saeericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

-f          File to process ($MFT | $J | $logFile | $boot | $DOS). Required
-jsonf      Directory to save JSON formatted results to. This or --csv required unless --de or --body is specified
-file       File name to save JSON formatted results to. When present, overrides default name
-csv        Directory to save CSV formatted results to. This or --json required unless --de or --body is specified
-csvf       File name to save CSV formatted results to. When present, overrides default name
-body       Directory to save bodyfile formatted results to. --bdl is also required when using this option
-bodyf      File name to save bodyfile formatted results to. When present, overrides default name
-bdl        Drive letter (C, D, etc.) to use with bodyfile. Only the drive letter itself should be provided
-bif        When true, use lf vs CRlf for newlines. Default is FALSE
-dd         Directory to save exported file records. --de is also required when using this option
-do         Offset of the file record to dump as decimal or hex. Ex: 5120 or 0x1400 Use --de or --v 1 to see offsets
-de         Dump full details for entry/sequence #. Format is 'entry' or 'entry-Seq' as decimal or hex. Example: 5, 624-5 or 0x270-0x5.
-rs         When true, displays contents of directory specified by --de. Ignored when --de points to a file
-ds         Dump full details for Security id as decimal or hex. Example: 624 or 0x270
-dt         The custom date/time format to use when displaying time stamps. Default is: yyyy-MM-dd HH:mm:ss.ffffff
-sh         Include DOS file name types. Default is FALSE
-at         When true, include all timestamps from 0x30 attribute vs only when they differ from 0x30. Default is FALSE
-vss        Process all Volume Shadow Copies that exist on drive specified by -f. Default is FALSE
dedupe      Deduplicate -f & VSCs based on SHA-1. First file found wins. Default is FALSE
debug       Show debug information during processing
trace       Show trace information during processing

Examples: MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out" --csvf MyOutputFile.csv
MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out"
MFTECmd.exe -f "C:\Temp\SomeMFT" --json "c:\temp\out"
MFTECmd.exe -f "C:\Temp\SomeMFT" --body "c:\temp\out" --bdl c
MFTECmd.exe -f "C:\Temp\SomeMFT" --de 3-5

Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

--csv, --json, --body, --de, or --v is required. Exiting
PS C:\Users\John\Downloads\CTF\Get-ZimmermanTools>
```

.\Get-ZimmermanTools\MFTECmd.exe -f '..\may\hr\VSS1\\$MFT' --csv ..\may\hr\mft.csv



20200519202257\_MFTECmd\_\$MFT\_Output.csv

5/19/2020 3:23 PM

Microsoft Excel Commi

We open the excel file and we can browse for the entry to get the file name for the flag

199399	1					.pyc	185
199400	1					.pyc	437
199401	1						0
199402	1					.txt	98
199403	1					.txt	1110
199404	1						2859
199405	1						44644
199406	1					.txt	4
199407	1						116
199408	1					.exe	102743
199409	168042	1	TRUE	167052	1	.\Python3\pip3.exe	102743
199410	168043	1	TRUE	167052	1	.\Python3\pip3.7.exe	102743

Flag: pip3.7.exe



# HR Server Woes 7

80

What is the MFT Entry number of the following file?

`\xampp\mysql\bin\mysql.exe`

Inside this excel file we will search again for this file. We cannot search for the full path as the mysql.exe is separated to another column.

The screenshot shows an Excel spreadsheet with a 'Find and Replace' dialog box open. The dialog box is set to search for '\xampp\mysql\bin' in the 'Find what' field. The 'Find Next' button is highlighted. The spreadsheet contains columns for file names and their extensions, with 'mysql.exe' listed in the final row.

File Name	Extension
mysql_tzinfo_to_sql.exe	.exe
myisampack.exe	.exe
mysql_upgrade_service.exe	.exe
mysql_install_db.exe	.exe
mysqldadmin.exe	.exe
mysqlshow.exe	.exe
replace.exe	.exe
aria_dump_log.exe	.exe
perror.exe	.exe
aria_ftdump.exe	.exe
echo.exe	.exe
mysql_plugin.exe	.exe
myisamlog.exe	.exe
my_print_defaults.exe	.exe
mysqlbinlog.exe	.exe
mysql.exe	.exe

Flag: 115322

# HR Server Woes 8

100

What is the MFT Attribute ID of the named \$J data attribute for the MFT Entry with a file name of \$UsnJrnl?

Sticking with the CSV file we can search for \$j

140345	Find and Replace				?	×
140346	Find				Replace	
140347	Find what: \$j					
140348						
140349					Options >>	
140350	Find All				Find Next	Close
140351	108606	2	TRUE	11	2: (Windows\Parame	
140352	108606	2	TRUE	11	11: \.\$Extend	
140353	108606	2	TRUE	11	11: \.\$Extend	
140354						
140355					viostor.sys	.sys 48712
140356					History	0
140357					Temporary Internet Files	0
					Temporary Internet Files	0
					Documents and Settings	0
					diagwrn.xml	.xml 18344
					MainQueueOnline0.que	.que 28812
					setup.exe	0
					setupact.log	.log 325845
					setuperr.log	.log 0
					setupinfo	102656
					\$UsnJrnl	3.66E+08
					\$UsnJrnl:\$J	3.66E+08

We can take this and look in MFT Explorer to view the attributes.

So browse to \$extend\.\$UsnJrnl

	Image Icon	Name	Parent Path	Is Dir	Is Deleted	SI_Created On	FN_Created
	No image data	#C	#C			=	=
		\$RmMetad...	.\\$Extend	✓		2018-05-01 22:52:51.80934...	
		\$ObjId	.\\$Extend			2018-05-01 22:52:51.80934...	
		\$Quota	.\\$Extend			2018-05-01 22:52:51.80934...	
		\$Reparse	.\\$Extend			2018-05-01 22:52:51.80934...	
		\$UsnJrnl	.\\$Extend			2018-05-01 21:55:24.13800...	

To do the math here is what we need to find the offset

$$108606 * 1024 = 111212544$$

Convert to hex: 111212544 == 6A0F800

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F		Overview	Details
00000000	46	49	4C	45	30	00	03	00	A2	CA	67	42	00	00	00	00	FILE0... €ËgB....		
00000010	02	00	01	00	38	00	05	00	E0	01	00	00	00	04	00	00	... 8... à.....		Flags: Hidden[System]Archive[SparseFile, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x101, Quota Charged: 0x0
00000020	00	00	00	00	00	00	00	00	0C	00	00	00	3E	A8	01	00	..... >.....		Update Sequence #: 0x0
00000030	6E	F5	D3	01	00	00	00	00	10	00	00	00	60	00	00	00	nðÖ.....		
00000040	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	..... H.....		Created On: 2018-05-01 21:55:24.1380099
00000050	03	3D	7D	18	97	E1	D3	01	03	3D	7D	18	97	E1	D3	01	. =)... äÖ. =)... äÖ.		Content Modified On: 2018-05-01 21:55:24.1380099
00000060	03	3D	7D	18	97	E1	D3	01	03	3D	7D	18	97	E1	D3	01	. =)... äÖ. =)... äÖ.		Record Modified On: 2018-05-01 21:55:24.1380099
00000070	26	02	00	00	00	00	00	00	00	00	00	00	00	00	00	00	&.....		Last Accessed On: 2018-05-01 21:55:24.1380099
00000080	00	00	00	00	01	01	00	00	00	00	00	00	00	00	00	00	.....		**** FILE NAME ****
00000090	00	00	00	00	00	00	00	30	00	00	00	70	00	00	00	00	..... 0... p....		Type: FileName, Attribute #: 0x1, Size: 0x70, Content size: 0x52, Name size: 0x0, Content offset: 0x18, Resident: True
000000A0	00	00	00	00	00	01	00	52	00	00	00	18	00	01	00	00	..... R.....		
000000B0	08	00	00	00	00	00	08	00	03	3D	7D	18	97	E1	D3	01	..... =)... äÖ.		File name: \$Jsn3m1 (Length: 0x8)
000000C0	03	3D	7D	18	97	E1	D3	01	03	3D	7D	18	97	E1	D3	01	. =)... äÖ. =)... äÖ.		Flags: Hidden[System]Archive, Name Type: Posix, Reparse Value: 0x0, Physical Size: 0x0, Logical Size: 0x0
000000D0	03	3D	7D	18	97	E1	D3	01	00	00	00	00	00	00	00	00	. =)... äÖ. =)... äÖ.		Parent Mft Record: Entry/seq: 0x8-0x8
000000E0	00	00	00	00	00	00	00	26	00	00	00	00	00	00	00	00	. =)... äÖ. =)... äÖ.		Created On: 2018-05-01 21:55:24.1380099
000000F0	08	00	24	00	55	00	73	00	6E	00	4A	00	72	00	6E	00	..... &.....		Content Modified On: 2018-05-01 21:55:24.1380099
00000100	6C	00	00	00	00	00	00	80	00	00	00	90	00	00	00	00	.. \$ . U . s . n . J . r . n .		Record Modified On: 2018-05-01 21:55:24.1380099
00000110	01	02	48	00	00	80	00	00	00	00	00	00	00	00	00	00	l.....		Last Accessed On: 2018-05-01 21:55:24.1380099
00000120	7F	5D	01	00	00	00	00	50	00	04	00	00	00	00	00	00	.. ]..... P.....		**** DATA ****
00000130	00	00	D8	15	00	00	00	80	98	D5	15	00	00	00	00	00	.. Ö..... " . Ö.....		Type: Data, Attribute #: 0x3, Size: 0x90, Content size: 0x0, Name size: 0x2, Name: \$J, Content offset: 0x0, Resident: False
00000140	80	98	D5	15	00	00	00	00	00	48	00	00	00	00	00	00	*. Ö..... H.....		Non Resident Data
00000150	24	00	4A	00	00	00	00	03	00	59	01	32	98	00	DF	00	\$ . J . ..... Y . 2 . . B		Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0x15D7F, Allocated Size: 0x15D80000, Actual Size: 0x15D598B0, Initialized Size: 0x15D598B0
00000160	10	01	31	68	58	BF	28	32	80	00	75	94	FE	32	80	00	.. 1h[ z+2... u. b2..		DataRun Entries
00000170	D6	40	FF	32	86	00	CF	72	08	31	4A	2F	F9	F5	32	80	Ö@21. l r. 1j / uö2..		Cluster offset: 0x0, # clusters: 0x15900
00000180	00	48	33	EE	32	80	00	D1	41	EA	32	80	00	AC	6A	1E	. K3l 2. . NÄe2. . "j .		Cluster offset: 0x110DF, # clusters: 0x98
00000190	00	00	00	00	00	00	00	80	00	00	00	40	00	00	00	00	.....		Cluster offset: 0x2B9F58, # clusters: 0x68
000001A0	00	04	18	00	00	00	08	00	20	00	00	00	20	00	00	00	.....		Cluster offset: 0xFEE9475, # clusters: 0x80
000001B0	24	00	40	00	61	00	78	00	00	40	00	00	00	00	00	00	\$ . M a . x . ) . . ©.....		Cluster offset: 0xFF40D6, # clusters: 0x80
000001C0	00	00	10	00	00	00	00	00	03	3D	7D	18	97	E1	D3	01	..... =)... äÖ.		Cluster offset: 0x872CF, # clusters: 0x86
000001D0	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	82	79	47	11	..... yyy. yG.		Cluster offset: 0xF9F92F, # clusters: 0x4A
000001E0	FF	FF	FF	FF	82	79	47	11	FF	FF	FF	FF	82	79	47	11	yyy. yG. yyy. yG.		Cluster offset: 0xEE3346, # clusters: 0x80
000001F0	00	00	10	00	00	00	00	00	03	3D	7D	18	97	E1	6E	F5	..... =)... änb		Cluster offset: 0xEA41D1, # clusters: 0x80
00000200	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	82	79	47	11	..... yyy. yG.		Cluster offset: 0x1E6AAC, # clusters: 0x80
00000210	22	80	00	A8	03	22	80	00	D6	03	22	80	00	7A	03	00	*. . . . . Ü. . . . . z. .		

Type: Data, Attribute #: 0x3, Size: 0x90, Content size: 0x0, Name size: 0x2, Name: \$J, Content offset: 0x0, Resident: False

Flag: 3

# HR Server Woes 9

## 100

At 2018-08-08 18:10:38.554 (UTC) what was the IP address of the the client that attempted to access SMB via an anonymous logon?

We will run the Zimmerman tools to correlate all the event logs together with EvtxExplorer. (Make sure you are on the E Drive).

```


Metrics (including dropped events)
Event Id      Count
300           10
400           6
403           5
600          36

Processed 262 files in 29.0807 seconds

PS C:\Users\John\Downloads\CTF> .\Get-ZimmermanTools\EvtxExplorer\EvtxECmd.exe -d .\may\hr\E\Windows\system32\winevt\log
s\ --csv .\may\hr\

```

This will create a csv file we can browse and sort on.

	20200520142236_EvtxECmd_Output.csv	5/20/2020 9:23 AM	Microsoft Excel C...	31,964 KB
---	------------------------------------	-------------------	----------------------	-----------

We will need to create a table: select all -> insert table with headers. Filter on channel for the two SMB-Server channels, and convert the Time created field to long date format.

Next we need to go to 8/18/2018 @ 18:10 and find the record associated with that field.

[illegible]

Flag: 80.81.110.50

# HR Server Woes 10

80

What was the name of the batch file saved by mpowers? Answer should be the full path starting with C:\

We need to load the mpowers ntuser.dat hive into Registry Explorer and look at the following location for recent open/saved files:

Software\Microsoft\Windows\CurrentVersion\Explorer\Comdlg32\OpenSavePidMRU\bat

ComDlg32	0	3	2018-07-23 16:38:52
CIDSizeMRU	3	0	2018-07-23 17:55:21
LastVisitedPidMRU	2	0	2018-07-23 17:55:21
OpenSavePidMRU	0	4	2018-07-23 16:48:15
*	5	0	2018-07-23 17:55:21
bat	2	0	2018-07-23 16:48:15
exe	3	0	2018-07-23 17:37:37
ps1	2	0	2018-07-23 16:41:14
Nonexistent	0	0	2018-07-23 16:41:14

.. PàCØ è: i. 4Ø . +00. . /C \..... ^ 1. .... ÆL... PRCDU  
C~1.. F..... Ì 3/LV. ÆL... ã..... Ì ÖY. P. r. o. d. u. c. t  
. i. o. n. .... j. 2. J. ... ÆLý. . UPDATE~1. BAT. . N ..... Ì 3/Lä. ÆLä. .... ä....  
..... n. . . u. p. d. a. t. e. \_ . a. p. . . b. a. t. ....

From here we can see update\_app.bat was the bat files she saved under the c:\production folder

Flag: c:\production\update\_app.bat

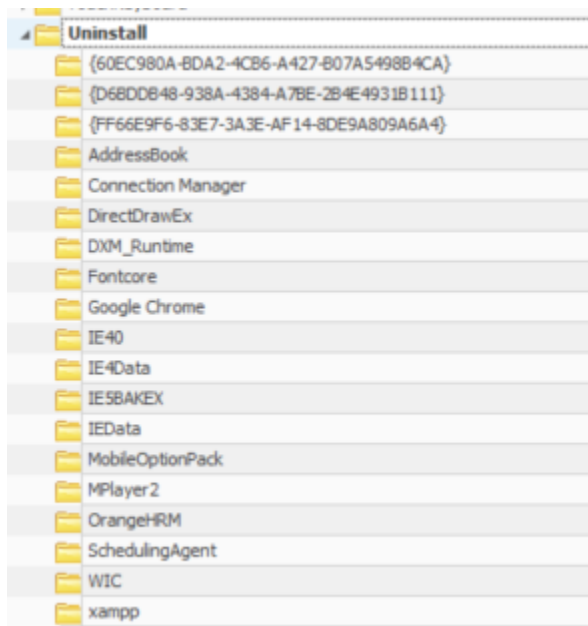
# HR Server Woes 11

80

What is the name of the hr management application that hosts a web server?

For this we will look at the Software registry hive and go the following location in order to find all the programs listed under the add/remove control panel:

Software\wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall



Here we see one program that has the HR in it as this could be the program we are looking for.

# OrangeHRM

Software company



[orangehrm.com](https://orangehrm.com)

OrangeHRM Inc. is a HR software company based in Secaucus, New Jersey. The company has developed a human resources management solution. The company offers an open-source, professional, & enterprise solution. The open-source solution is free while the professional and enterprise solutions are advanced hosted solutions. [Wikipedia](#)

Flag: OrangeHRM

# HR Server Woes 12

## 80

At 2018-07-30 22:31:33 UTC which user was logged in, what was the logon type (integer), and the remote IP? Format should be: TargetUserName-LogonType-IPAddress

We will run the Zimmerman tools to correlate all the event logs together with EvtxExplorer.

```
Processed 53 files in 57.0491 seconds
PS C:\Users\John\Downloads\CTF> .\Get-ZimmermanTools\EvtxExplorer\EvtxECmd.exe -d .\may\hr\VSS1\Windows\system32\winevt\logs\ --csv .\may\hr\
```

This will create a csv file we can browse and sort on.

20200519205704\_EvtxECmd\_Output.csv 5/19/2020 3:58 PM Microsoft Excel C... 68,140 KB

We can look into the event logs to get the information that we need. We can create a table out of the csv, Select All -> Insert Table -> My Table has headers

Under Column G we will filter on Security and Event ID 4624 for a successful Login attempts, this gives us only 79 Events to look at.

We will need to change the time created column to a time type data so we can see the timestamps

We see the answer here:

Monday, July 30, 2018	4624 Security	Successful logon	140 WORKGROUP\WIN-29U41M70JCO\$	WIN-29U41M70JCO (74.118.138.195)	Target: WIN-29U41M70JCO\mpowers	LogonType 10
Monday, July 30, 2018	4624 Security	Successful logon	140 WORKGROUP\WIN-29U41M70JCO\$	WIN-29U41M70JCO (74.118.138.195)	Target: WIN-29U41M70JCO\mpowers	LogonType 10

Flag: mpowers-10-74.118.138.195



# HR Server Woes 13

50

At 2018-07-27 02:42:43 (UTC), what is the name of the task that was started?

We will clear the filters for the event id and the channel that we used. We now need to look at the channel for Microsoft-Windows-Task\* to see if we can find our answer.

We go to the date and we find our answer in the Payload column:

516								7/27/2018 2:42:44 AM	
TimeCreated	EventId	Channel	MapDescription	Chun	ExecutableInfo	SourceFile	Payload		
Friday, July 27, 2018	107	Microsoft-Windows-TaskSched	20	C:\Users\Johnr [\"EventData\":{\"@Name\":\"TimeTriggerEvent\",\"Data\":{\"@Name\":\"TaskName\",\"#text\":\"\\Throw Taco\"},{\"@Name\":\"InstanceId\",\"#text\":\"937b509-b699-4441-b2fe-bb167784d470\"}}]]					

Flag: Throw Taco