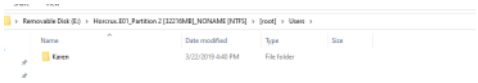
HireMe Lab (Cyber Defenders) - Walkthrough

Saturday, September 21, 2024 2:49 PM

Story:
Karen is a security professional looking for a new job. A company called "TAAUSAI" offered her a position and asked her to complete a couple of tasks to prove her technical competency. As a soc analyst Analyze the provided disk image and answer the questions based on your understanding of the cases she was assigned to investigate.

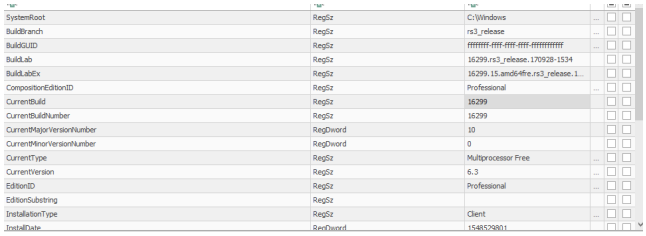
Q1: What is the administrator's username?

- 'Karen' is the only available account on the OS



Q2: What is the OS's build number?

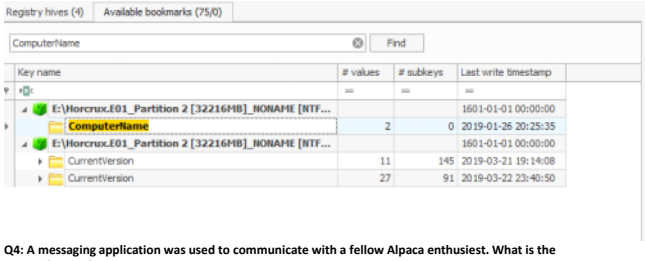
- **I loaded the 'Software' HIVE to 'Registry Explorer' and navigated to '** SOFTWARE\Microsoft \Windows NT\CurrentVersion' to see the build number.



SystemRoot	RegSz	C:\Windows
BuildBranch	RegSz	rs3_release
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	RegSz	16299.rs3_release.170928-1534
BuildLabEx	RegSz	16299.15.amd64fre.rs3_release.1...
CompositionEditionID	RegSz	Professional
CurrentBuild	RegSz	16299
CurrentBuildNumber	RegSz	16299
CurrentMajorVersionNumber	RegDword	10
CurrentMinorVersionNumber	RegDword	0
CurrentType	RegSz	Multiprocessor Free
CurrentVersion	RegSz	6.3
EditionID	RegSz	Professional
EditionSubstring	RegSz	
InstallationType	RegSz	Client
InstallDate	RegDword	1548529801

Q3: What is the hostname of the computer?

- **I loaded the 'System' HIVE to 'Registry Explorer' and navigated to '** \CurrentControlSet\Control \Computername\ComputerName' to see the hostname.



Registry hives (4) | Available bookmarks (75/0)

ComputerName | Find

Key name	# values	# subkeys	Last write timestamp
E:\Horcrux.E01_Partition 2 [32216MB]_NONAME [NTF...			1601-01-01 00:00:00
ComputerName	2	0	2019-01-26 20:25:35
E:\Horcrux.E01_Partition 2 [32216MB]_NONAME [NTF...			1601-01-01 00:00:00
CurrentVersion	11	145	2019-03-21 19:14:08
CurrentVersion	27	91	2019-03-22 23:40:50

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Re...
(default)	RegSz	mnmsrvc	DC-00-00...		
ComputerName	RegSz	TOTALLYNOTAHACK	69-00-70...		

Q4: A messaging application was used to communicate with a fellow Alpaca enthusiest. What is the name of the software?

- Great question! I checked the Chrome history and identified that the user downloaded Skype. Additionally, you can check the registry key **Microsoft\Windows\CurrentVersion\App Path**s to see which applications are installed on the OS.

2017-09-29 13:48:39	setup.exe		
2019-02-09 20:52:56	SKYPESERVER.EXE	C:\Program Files (x86)\Microsoft Office\Root\Office16\SkypeSrv\SKYPESERVER.EXE	C:\Program Files (x86)\Microsoft Office\Root\Office16\SkypeSrv\
2017-09-29 14:43:12	SnippingTool.exe	%SystemRoot%\system32\SnippingTool.exe	
2017-09-29 13:48:39	table30.exe		
2017-09-29 14:43:12	TabTip.exe	%CommonProgramFiles%\microsoft shared\ink\TabTip.exe	
2019-02-09 20:51:17	vstoee.dll		

973cc0f6-4ac7-4857-b92e-794c80c68996	C:\Users\Karen\Downloads\alpy.png	C:
2eee9d77-e56b-4441-bc0d-777c887c2d56	C:\Users\Karen\Downloads\Alpaca-Care-for-...	C:
187f6172-3124-4702-90bc-34a3ef18a097		C:
45909c70-9476-4ca5-854f-1c6e55093740	A:\PAssist_Std.exe	A:
f808ed1f-c450-430b-bbf0-7bb16669457d	A:\timestomp.exe	A:
187e1870-42c1-454c-9c59-29efc7599db2	A:\HashTab_v6.0.0.34_Setup.exe	A:
5cc93d0c-89cc-4376-8584-16c96f9a435e	A:\Skype-8.41.0.54.exe	A:
b71665d1-be44-4cfa-b9bc-32075002e579	C:...	C:
c07ab7a4-35d3-4d1e-8094-1b66151c06d9		
5322ac5c-0fbf-474b-afa4-b381fd495a14		
bb7a04e1-f022-495d-a655-1e99b5b3ce1a	C:\Users\Karen\Pictures\haircuts1.jpg	C:
cac91e2b-a4a1-424f-a1ac-2352bd260b75	A:\antimalwaresetup.exe	A:
dc1ade17-ead9-4811-b86b-6eb8f10c0b22	A:\7z1900-x64.exe	A:

Q5: What is the zip code of the administrator's post?

- To address this question, I considered looking for the answer in the email headers using the OST viewer.
  While checking the Google Chrome history, I found that 'Karen' uploaded a post to a job requests website.
  After loading the 'Webdata' into DBSqlite, I discovered that the zip code is '19709'.

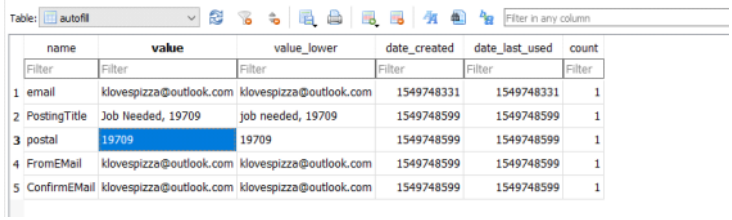


Table: autofill | Filter in any column

	name	value	value_lower	date_created	date_last_used	count
1	email	klovespizza@outlook.com	klovespizza@outlook.com	1549748331	1549748331	1
2	PostingTitle	Job Needed, 19709	job needed, 19709	1549748599	1549748599	1
3	postal	19709	19709	1549748599	1549748599	1
4	FromEMail	klovespizza@outlook.com	klovespizza@outlook.com	1549748599	1549748599	1
5	ConfirmEMail	klovespizza@outlook.com	klovespizza@outlook.com	1549748599	1549748599	1

Q6: What are the initials of the person who contacted the admin user from TAAUSAI?

I loaded the Outlook content of the user into OST Viewer and searched for emails from the mentioned sender, TAAUSAI.
I found an email with the sender's initials, 'M.S.'

Hello Ms. Karen,

We are attempting to reach out to you again to see if you'd still be interested in working with us. As we previously mentioned, this is a high paying technical job involving computers. That may sound scary, but all you need to know is how to turn a computer on. We'll provide you with resources about on how to do the rest.

Let us know if you're interested. We're willing to pay $150,000 USD upfront, and more at the completion of the job.

Feel free to reply to this email, or send us a message at taausai@gmail.com.

We look forward to hearing back from you soon!

Best,
M.S.

Q7: How much money was TAAUSAI willing to pay upfront?

- We are able to see how much money TAAUSAI willing above (150,000$)

Q8: What country is the admin user meeting the hacker group in?

- I reviewed the email correspondence between Karen and 'taausai' and found that the attacker sent Karen a location: "Meet us here: 27°22'50.10"N, 33°37'54.62"E." This location is situated in **Egypt.**

We have been conducting an investigation on Bob Redliubeht (the CEO of Alpacamybags Luxury Alpaca handbags) and we believe he's been mistreating some of his Alpacas. We have heard complaints that he refuses to provide Alpacas with scarfs and beanies during the winter!

What we need you to do is gain his trust and then hack his machine. We will give you more information about this in person. Meet us here "27°22'50.10"N, 33°37'54.62"E"

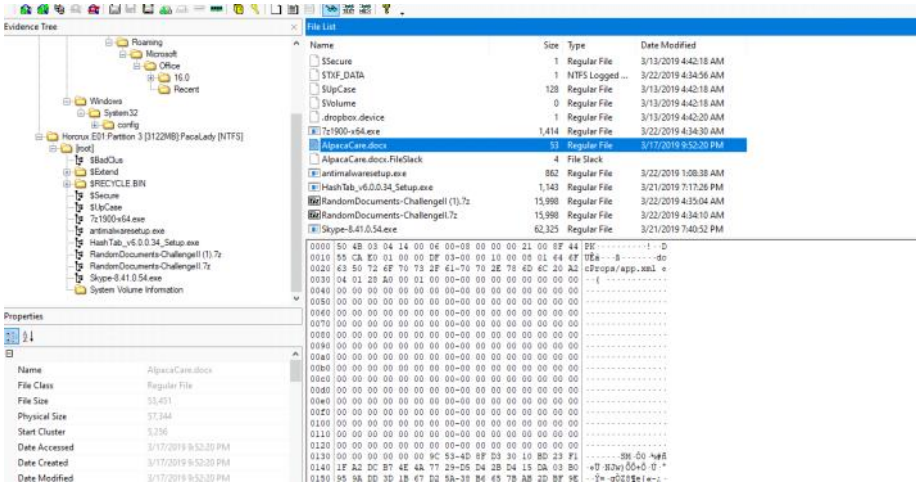
Q9: What is the machine's timezone? (Use the three-letter abbreviation)

- To address this question, I loaded the 'SYSTEM' hive into Registry Explorer and searched for the key 'TimezoneInformation' located at 'ControlSet001\Control\TimeZoneInformation.'
  The answer is **UTC**.

Value Name	Value Data	Value Data Raw
▯c	▯c	▯c
Bias	0	0
DaylightBias	0	0
DaylightName	@tzres.dll,-931	@tzres.dll,-931
DaylightStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-932	@tzres.dll,-932
StandardStart	Month 0, week of month 0, day of week 0, Hours:Minutes:Seconds:Milliseconds 0:0:0:0	00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	UTC	UTC
ActiveTimeBias	0	0

Q10: When was AlpacaCare.docx last accessed?

- To address this question, firstly, I tried to parse the MFT file but the file wasn't there.
  FTK Imager have the ability to see the modification and the accesses times.



Q11: There was a second partition on the drive. What is the letter assigned to it?

- To address this question, I searched for the key 'MountDevice' to identify the mounted disks.
  I found three disks: 'A', 'C', and 'D.' Upon reviewing the downloads performed by Google Chrome, I discovered that the files were downloaded to the **'A' drive.'**

Q12: What is the answer to the question Company's manager asked Karen?

- We backed to the OST Viewer, I accessed to the email correspondence between them I found Karen answer

Re: Interested in the job
Alpaca Activists<taausai@gmail.com> Thu 03/21/2019 18:55 PM
To: "Karen Alice" <klovespizza@outlook.com>

Hi Michael,

The answer is TheCardCriesNoMore

-Karen

From: Alpaca Activists <taausai@gmail.com>

Q13: What is the job position offered to Karen? (3 words, 2 spaces in between)

- I accessed to the email correspondence between them I found the job position.

Karen,

WOW! That was quick! I have confirmed with my manager that that answer is correct. We didn't expect you to know the answer, but were really testing you on your ability to quickly learn new things that may be a bit out of your comfort zone.

The job position we think you'll be an awesome fit for is an entry level cyber security analysts. We want someone who's willing to learn and don't really care about what you know coming in. We'll be in touch with more information about what this job entails (and the set up involved with getting you payed), but wanted to give you some material to study in the mean time.

Q14: When was the admin user password last changed?

- To address this question,I used Registry Explorer to export the key 'HKEY_LOCAL_MACHINE \SAM \SAM\Domains\Account\Users' from the SAM hive and opened it with TimelineExplorer.exe.

Valid User Id	User Id	Invalid Login Count	Total Login Count	Created On	Last Login Time	Last Password Change	Last Incorrect Password	Expires On	User Name	Full
☐	=	=	=	=	=	=	=			
☑	500	0	0	2019-01-26 …					Administrator	
☑	501	0	0	2019-01-26 …					Guest	
☑	503	0	0	2019-01-26 …					DefaultAccount	
☑	504	0	0	2019-01-26 …		2019-01-26 19:07:03			WDAGUtilityAccount	
☑	1001	0	32	2019-01-26 …	2019-03-22 23:22…	2019-03-21 19:13:09	2019-03-21 19:14:49		Karen	
☑	1000	0	2	2019-01-26 …	2019-01-26 19:10…	2019-01-26 19:09:41			defaultuser0	

Q15: What version of Chrome is installed on the machine?

- By accessing the 'Uninstall' key located at HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft \Windows\CurrentVersion\Uninstall, we can view the versions of the installed programs.

2017-09-29 14:41…	DXM_Runtime							
2017-09-29 13:48…	Fontcore							
2019-03-13 05:20…	Google Chrome	Google Chrome	72.0.3626.121	Google Inc.	20190312		C:\Program Files (x86)\Google\Chrome\Application	"C:\Program Files (x86)\Google\Chrome\Application\72.0.3626.121\Installer\setup.exe" --uninstall --system-level --verbose-logging

Q16: What is the URL used to download Skype?

- I tried to find the download URL via Google Chrome artifacts without success.
  I used the HINT, and of course, ADS can show us the downloaded URL.
  I parsed the MFT file and check the Zone ID contents:

Zone Id Contents
[ZoneTransfer] ZoneId=3 ReferrerUrl=https://www.skype.com/en/get-skype/ HostUrl=https://download.skype.com/s4l/download/win/Skype-8.41.0.54.exe

Q17: What is the domain name of the website Karen browsed on Alpaca care that the file AlpacaCare.docx is based on?

- To address this question, I opened the DOCX file and searched for any links that could lead me to their domain, and I found several.