Exercise 1

1. Disables the This will install... Do you wish to continue? prompt at the beginning of Setup.
/SILENT, /VERYSILENT
Instructs Setup to be silent or very silent.
/SUPPRESSMSGBOXES
Instructs Setup to suppress message boxes.
/LOG
Causes Setup to create a log file in the user's TEMP directory.
/LOG="filename"
Same as /LOG, except it allows you to specify a fixed path/filename to use for the log file.
/NOCANCEL
Prevents the user from cancelling during the installation process.
/NORESTART
Prevents Setup from restarting the system following a successful installation, or after a Preparing to Install failure that requests a restart.
/RESTARTEXITCODE=exit code
Specifies a custom exit code that Setup is to return when the system needs to be restarted.
/CLOSEAPPLICATIONS
Instructs Setup to close applications using files that need to be updated.
/NOCLOSEAPPLICATIONS
Prevents Setup from closing applications using files that need to be updated.
/RESTARTAPPLICATIONS
Instructs Setup to restart applications.
/NORESTARTAPPLICATIONS
Prevents Setup from restarting applications.
/LOADINF="filename"
Instructs Setup to load the settings from the specified file after having checked the command line.
/SAVEINF="filename"

There are several strings that say things like “Disables the This will install... Do you wish to continue? prompt at the beginning of Setup.” and “Instructs Setup to suppress message boxes”. This means that the program will run silently in the background. You can also see /LOG="filename", so you know that the prgram will be loggging to a file.

2. c027ce33c293f925324ba5477031e937
Several detection engines detect that this sample is a key logger.
The sample also attempts to contact several domains. It was successful for two of those.

SecureAge APEX	Malicious	Arcabit	Application.Keylogger.QQJ
Avast	Win32:ActualSpy-Q [PUP]	AVG	Win32:ActualSpy-Q [PUP]
BitDefender	Application.Keylogger.QQJ	Bkav	W32.AIDetectVM.malware1
Comodo	Malware@#1uj4pojiwtpvw	Cybereason	Malicious.3c293f
DrWeb	Program.ActualSpy.4	Emsisoft	Application.Keylogger.QQJ (B)
eScan	Application.Keylogger.QQJ	ESET-NOD32	Multiple Detections
FireEye	Application.Keylogger.QQJ	Fortinet	Riskware/Generic
GData	Application.Keylogger.QQJ	K7AntiVirus	Password-Stealer (0055dec41)
K7GW	Password-Stealer (0055dec41)	Kaspersky	Not-a-virus:HEUR:Monitor.Win32.Generic
Malwarebytes	RiskWare.ActualKeyLogger	MAX	Malware (ai Score=82)
Microsoft	Trojan:Win32/Wacatac.B!ml	Qihoo-360	HEUR/QVM06.1.13AA.Malware.Gen

3.

```
[austinsbrown@inspiron5567 lab12]$ sha256sum keylogger.exe
a4ffe3da00780acc018da4527fc5277338bb4a33516f27683dd2bed9f04fb488  keylogger.exe
[austinsbrown@inspiron5567 lab12]$
```

```
[austinsbrown@inspiron5567 lab12]$ sha512sum keylogger.exe
45236458b9dac4dbc4d371a7900bc4c8a51579cee5f912e685594f34c1746b333fe4477178a89ba9428431469c33d5663c379d5e66a43c4c3c3146acd4a1b23b  keylogger.exe
[austinsbrown@inspiron5567 lab12]$
```

Exercise 2

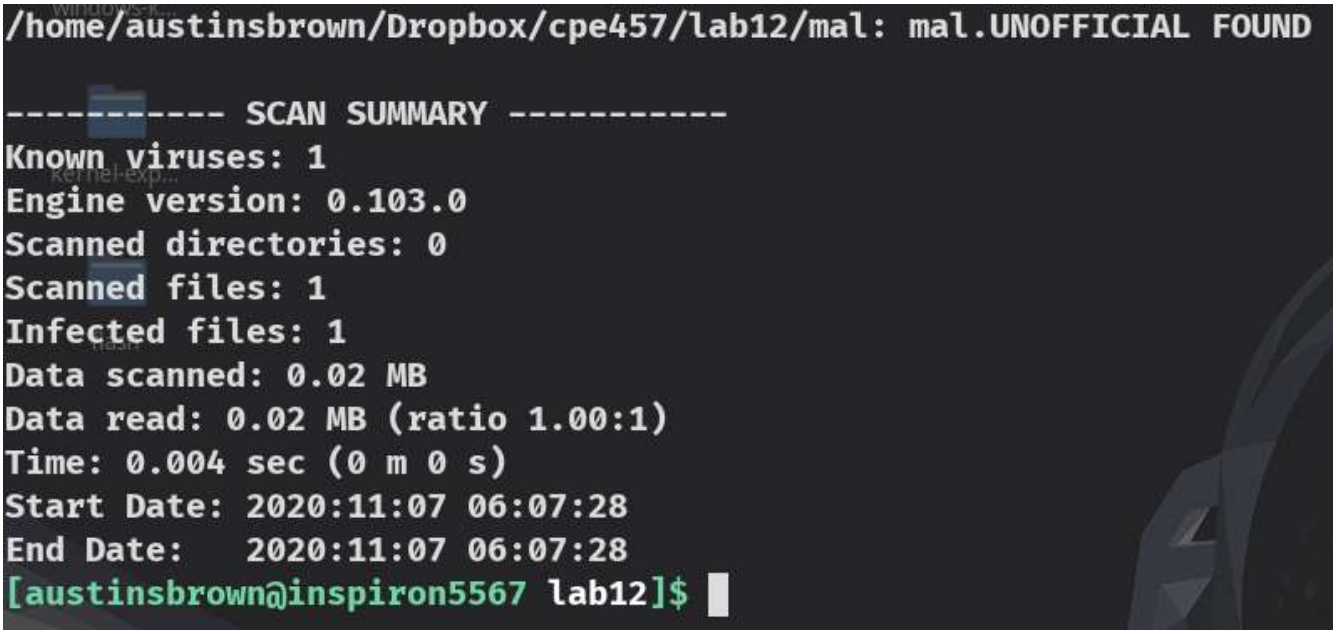
1.

```c
#include <stdio.h>

int main()
{
    printf("This file is malicious.\nConsider your files stolen.\n");
    return 0;
}
```

database.ndb

```
1  mal:*:*:6D616C6963696F7573
```


/home/austinsbrown/Dropbox/cpe457/lab12/mal: mal.UNOFFICIAL FOUND
---------- SCAN SUMMARY ----------
Known viruses: 1
Engine version: 0.103.0
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.02 MB
Data read: 0.02 MB (ratio 1.00:1)
Time: 0.004 sec (0 m 0 s)
Start Date: 2020:11:07 06:07:28
End Date: 2020:11:07 06:07:28
[austinsbrown@inspiron5567 lab12]$