Advanced Windows Security Course for 2020

Module 6: Cheating on Windows, Fuzzing and Buffer Overflow: Attack Scenarios and Protection Methods

January 14th, 2020

COURE

Cheating on Windows, Fuzzing and Buffer Overflow: Attack Scenarios and Protection Methods

Adrian Denkiewicz

CQURE: Cybersecurity Expert

CQURE Academy: Trainer

OSCE, OSCP, OSWP

@YetAnotherTruth; adrian@cqure.pl

/adenkiewicz

Artur Wojtkowski

CQURE: Cybersecurity Expert

CQURE Academy: Trainer

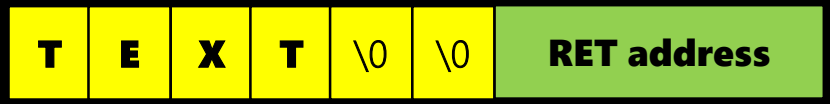
OSCE, OSCP, CISSP

@arturwojtkowski; artur@cqure.pl

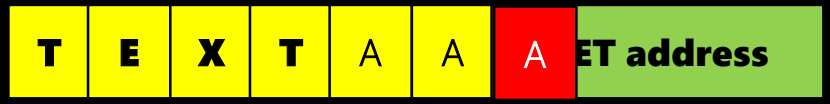
What is an exploit?

Buffer Overflow

Normal execution: function is called with "TEXT" as an argument

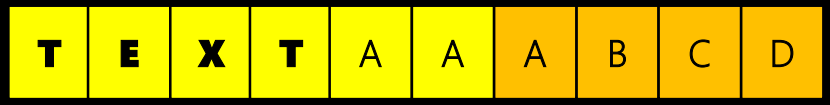


One byte overflow: function is called with "TEXTAAA" as an argument



Execution hijack: function is called with "TEXTAAABCD" as an argument.

ABCD becomes new RET address.



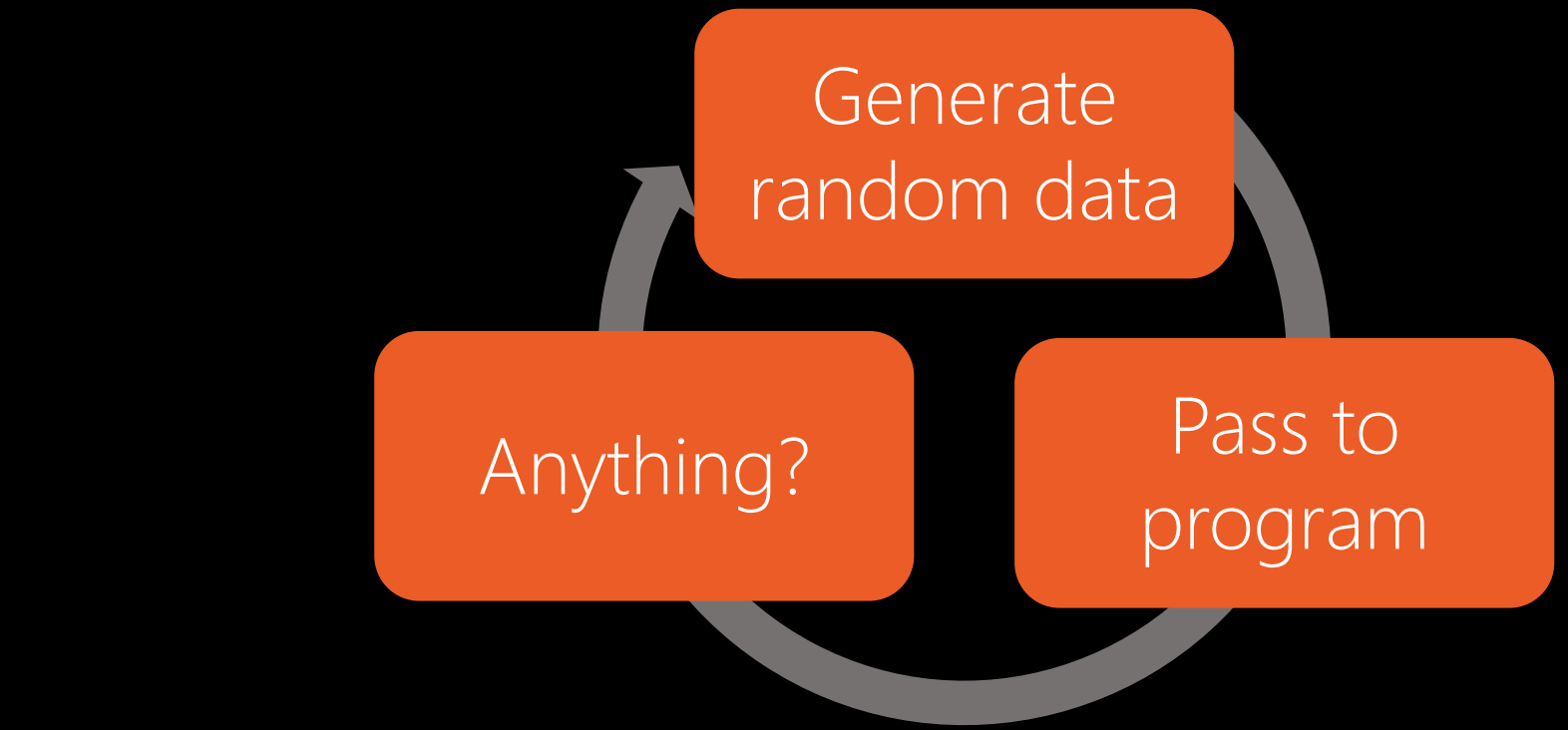
Other popular vulnerabilities

- Integer overflows
- Format string attacks
- NULL pointer dereference
- Double free
- Use after free
- Code reuse

Fuzzing

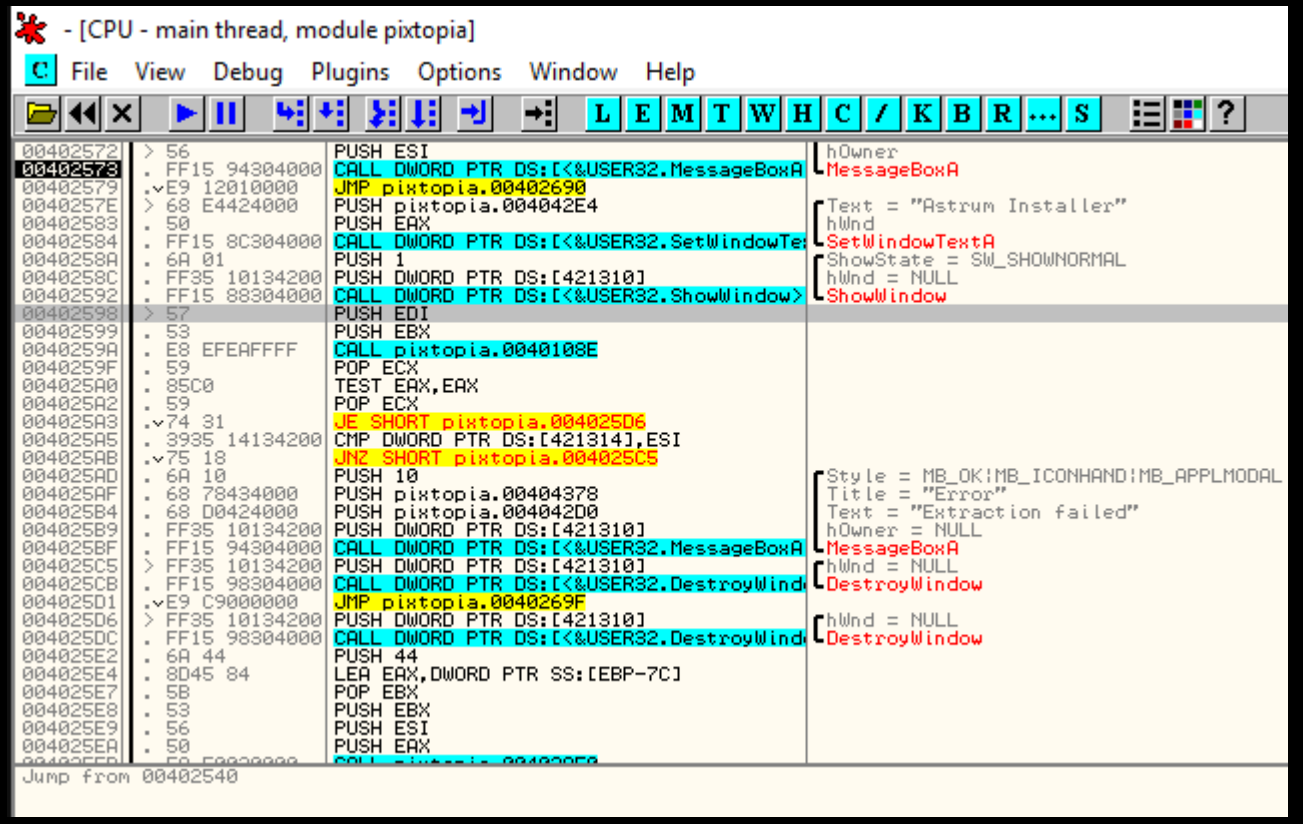
- Dumb
- Smart
- Evolutionary fuzzing

- Sanitizers
- Auto-triaging
- Fake sockets



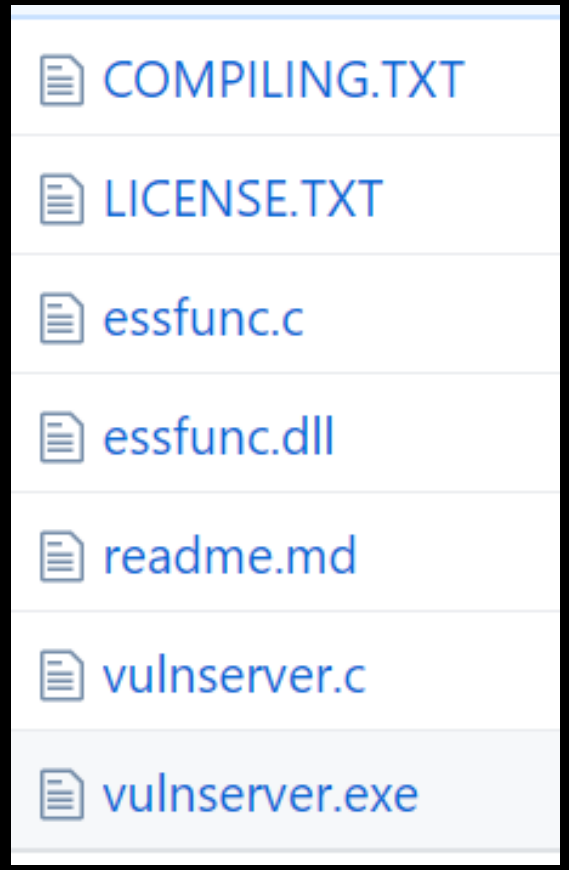
Debuggers

- OllyDbg
- Immunity
- X64dbg
- WinDbg



Vulnserv

"Vulnserver is a multithreaded Windows based TCP server that listens for client connections on port 9999 (by default) and allows the user to run a number of different commands that are vulnerable to various types of exploitable buffer overflows."

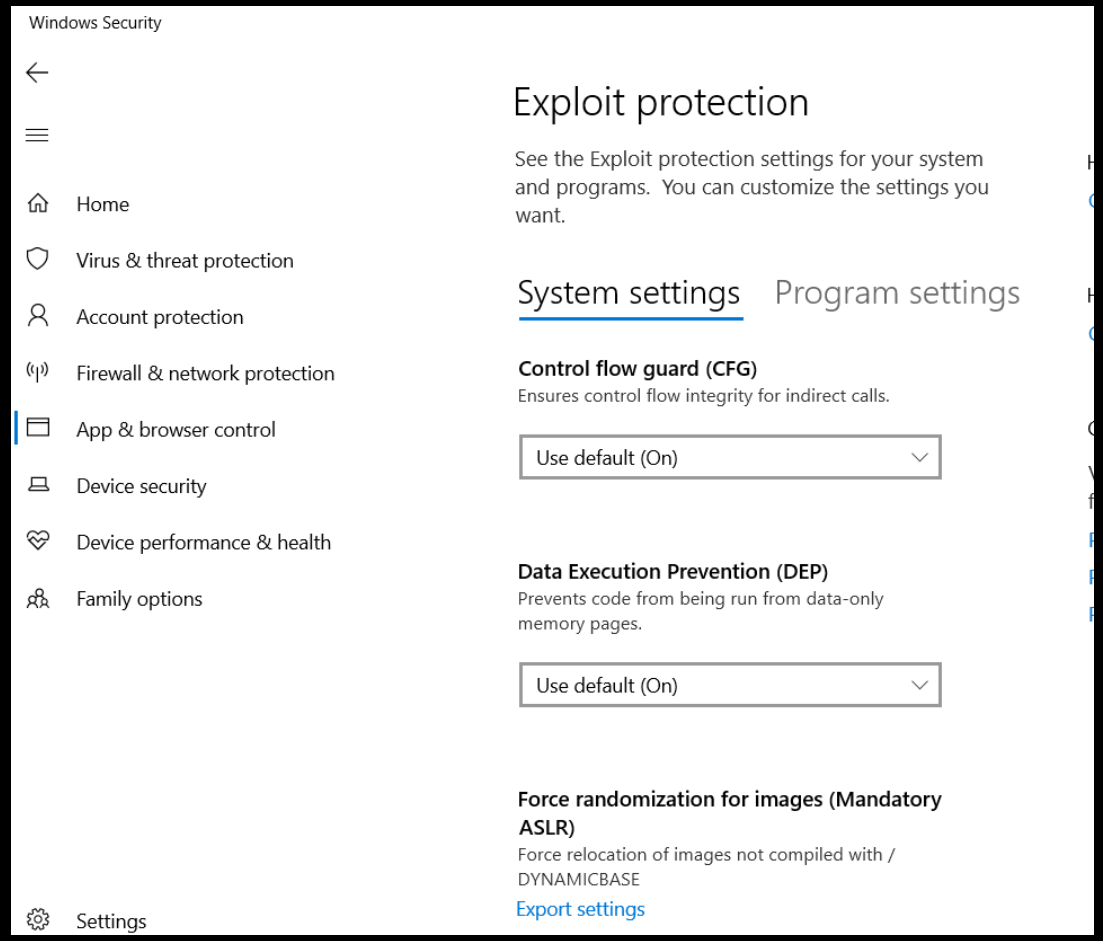


Exploitation demo

Exploitation prevention

- DEP
- ASLR
- Security canaries
- CFG
- Shadow Stacks

Exploit Guard



QUESTIONS?

Thank you!

- If you have questions email us at
  - info@cqureacademy.com

- You can also chat us up on the page
  - https://cqureacademy.com/

Cheating on Windows, Fuzzing and Buffer Overflow: Attack Scenarios and Protection Methods

Adrian Denkiewicz

CQURE: Cybersecurity Expert

CQURE Academy: Trainer

OSCE, OSCP, OSWP

@YetAnotherTruth; adrian@cqure.pl

/adenkiewicz

Artur Wojtkowski

CQURE: Cybersecurity Expert

CQURE Academy: Trainer

OSCE, OSCP, CISSP

@arturwojtkowski; artur@cqure.pl