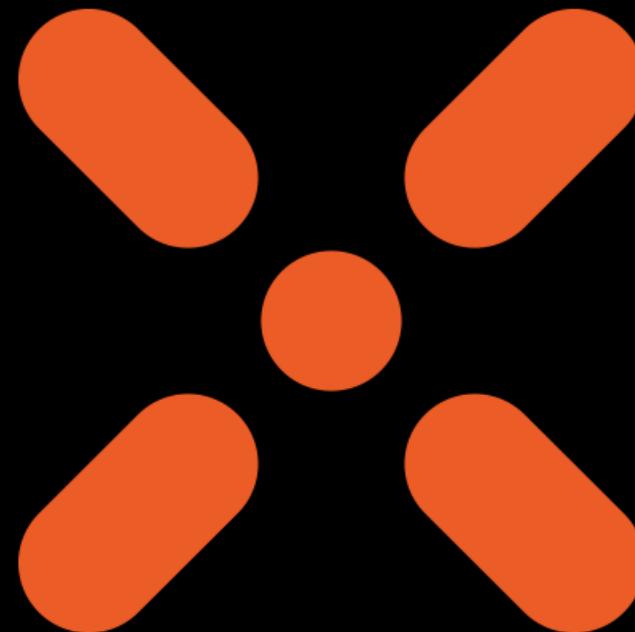


# Advanced Windows Security Course for 2020

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



January 14th, 2020

CQURE

# 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@cquire.pl](mailto:adrian@cquire.pl)

 /adenkiewicz



## Artur Wojtkowski

**CQURE:** Cybersecurity Expert

**CQURE Academy:** Trainer

OSCE, OSCP, CISSP

 @arturwojtkowski; [artur@cquire.pl](mailto:artur@cquire.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.



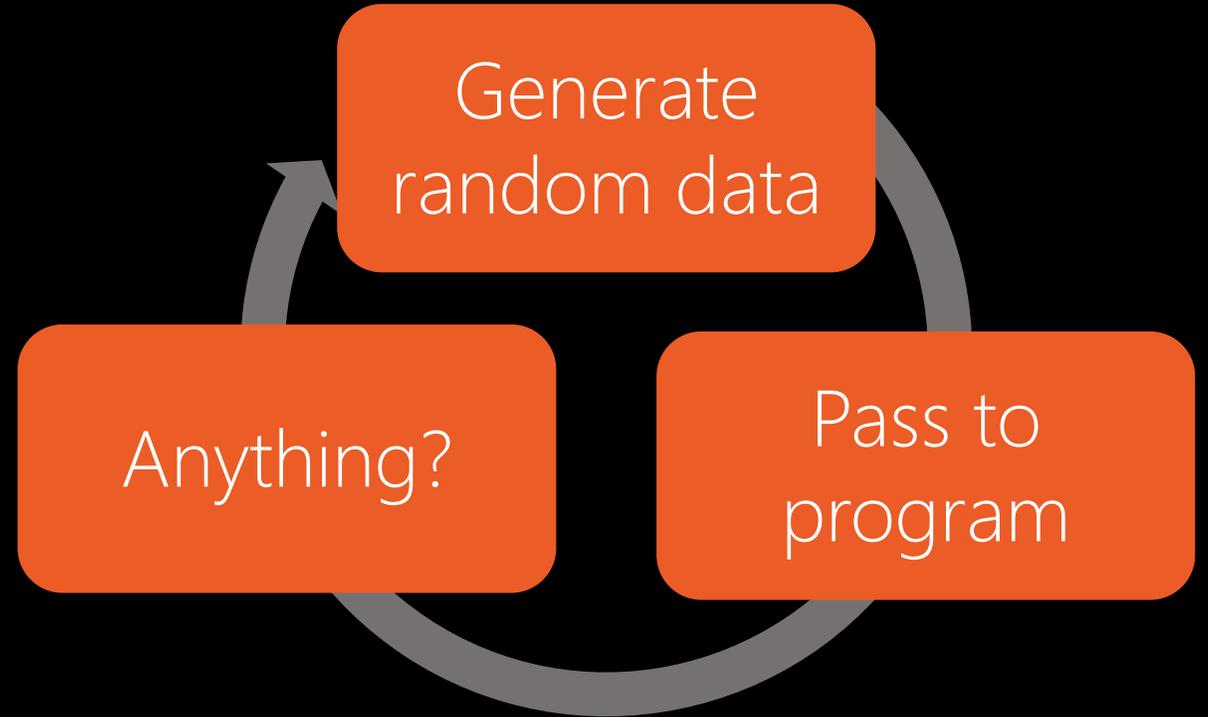
ABCD becomes new RET address.

# Other popular vulnerabilities

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

# Fuzzing

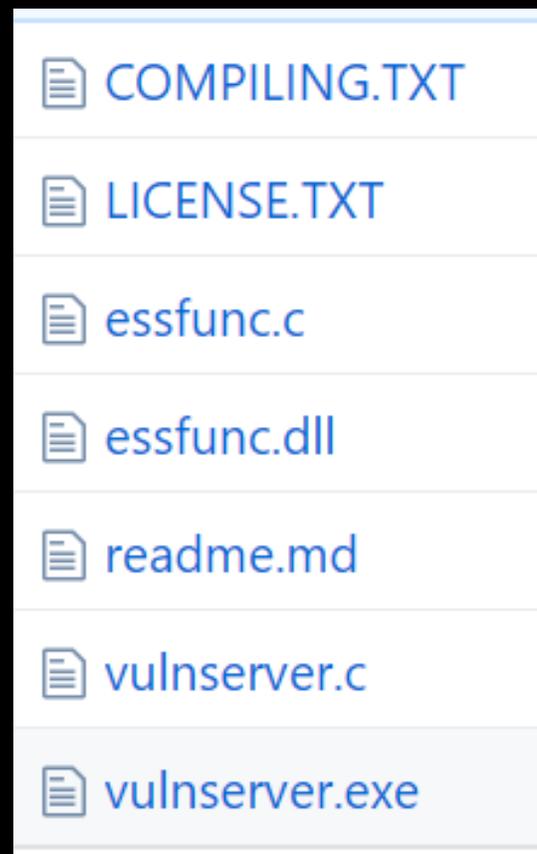
- Dumb
- Smart
- Evolutionary fuzzing
  
- Sanitizers
- Auto-triaging
- Fake sockets





# Vulnserver

“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.”



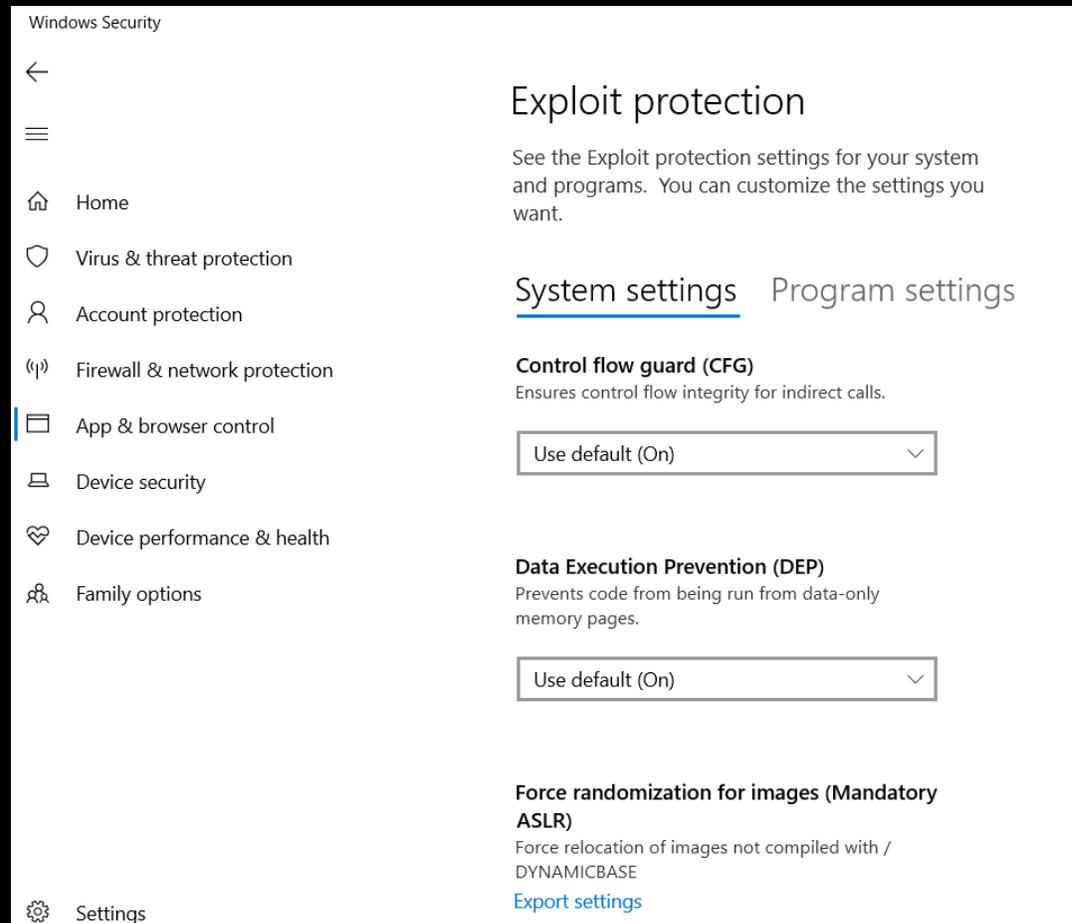
# Exploitation demo



# Exploitation prevention

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

# Exploit Guard



The screenshot shows the Windows Security application window. On the left is a navigation pane with the following items: Home, Virus & threat protection, Account protection, Firewall & network protection, App & browser control (highlighted with a blue bar), Device security, Device performance & health, and Family options. At the bottom of the pane is a gear icon labeled 'Settings'. The main content area is titled 'Exploit protection'. Below the title is a descriptive paragraph: 'See the Exploit protection settings for your system and programs. You can customize the settings you want.' There are two tabs: 'System settings' (which is selected and underlined) and 'Program settings'. Under 'System settings', there are three sections: 1. 'Control flow guard (CFG)' with the description 'Ensures control flow integrity for indirect calls.' and a dropdown menu set to 'Use default (On)'. 2. 'Data Execution Prevention (DEP)' with the description 'Prevents code from being run from data-only memory pages.' and a dropdown menu set to 'Use default (On)'. 3. 'Force randomization for images (Mandatory ASLR)' with the description 'Force relocation of images not compiled with /DYNAMICBASE' and a blue link labeled 'Export settings'.

Windows Security

←

☰

🏠 Home

🛡️ Virus & threat protection

👤 Account protection

🔒 Firewall & network protection

📁 App & browser control

📱 Device security

💓 Device performance & health

👨‍👩‍👧‍👦 Family options

⚙️ Settings

## Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

System settings Program settings

### Control flow guard (CFG)

Ensures control flow integrity for indirect calls.

Use default (On) ▾

### Data Execution Prevention (DEP)

Prevents code from being run from data-only memory pages.

Use default (On) ▾

### Force randomization for images (Mandatory ASLR)

Force relocation of images not compiled with /DYNAMICBASE

[Export settings](#)

QUESTIONS?



**Thank you!**

**If you have questions email us at  
[info@cquireacademy.com](mailto:info@cquireacademy.com)**

**You can also chat us up on the page  
<https://cquireacademy.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](mailto:adrian@cqure.pl)

 /adenkiewicz



## Artur Wojtkowski

**CQURE:** Cybersecurity Expert

**CQURE Academy:** Trainer

OSCE, OSCP, CISSP

 @arturwojtkowski; [artur@cqure.pl](mailto:artur@cqure.pl)