SP Lab 1 Optional: Memory Corruption

School of Informatics, University of Edinburgh

Classic Buffer Overflow (Set-UID version)

Checkpoint 1. What countermeasures are implemented in morden operating system to make buffer overflow attack difficult?

Checkpoint 2. What is a shellcode and what can I shellcode do?

Checkpoint 3. What is the meaning of the execstack options and no-stack-protector options for gcc compiler?

Checkpoint 4. Briefly describe the vulnerability for the strcpy function used in the vulnerable program.

Checkpoint 5. Why is it necessary to change the ownership of the vulnerable program to **root** and enable **SET-UID** bit to allow an attacker to gain root privilege?

Checkpoint 6. Briefly explain your exploit.

Checkpoint 7. Recall the SET-UID lab, what is the countermeasures for dash against privilege escalation?

Checkpoint 8. What is address randomization and how it helps to defend buffer overflow attack?

Checkpoint 9. What is StackGuard and how it helps to defend buffer overflow attack?

Checkpoint 10. What is Non-executable Stack Protection and how it helps to defend buffer overflow attack?