Pwning: Introduction

Mainack Mondal

CS60112
Spring 2023-24

What is pwning?

PWN

What does PWN mean?

PWN is hacker jargon meaning to conquer or dominate. In the context of online security, pwned often means that your account or system has been breached, and your passwords—user passwords or privileged passwords—have been compromised. The word originated in online gaming forums as a misspelling of “owned.”

But… isn’t this too generic?

PWN challenges are a type of CTF challenge that require you to exploit a binary typically running on a remote server. This can be done by exploiting a vulnerability in the binary, or by using a vulnerability in the binary to gain access to the system.

Often, PWN challenges will require you to gain access to a remote server, and then exploit the binary on that server. This is done by connecting to the server using a tool such as netcat, and then sending commands to the server.

https://lnwatson.co.uk/posts/pwn-challenges/

But…how do we exploit an entry to the system?

Outline

- Access control
- In practice: Unix access control
- Breaking access: memory attacks
  - Exploiting overflow
  - Return oriented programming (ROP)

Slide courtesy: Matteo Maffei, TU Wien