Sig•Mal

Meeting 10

Types of Security

CTF Advice

Sig•Mal++

Types of Security

There are multiple “types” of cybersecurity:

- General → Utilizes a mix of offensive and defensive tac
- Offensive → Proactive approach through use of ethical hacking “Red-teaming”
- Defensive → Reactive approach that focuses on prevention, detection, and response to attacks “Blue-teaming”

CTF Advice / Security

+ Command Line Tools > GUIs
+ Code more (you don’t need to be amazing, but the skill will carry over and you will be a coding unit)
+ Read up about common vulnerabilities (and see if there is documentation on how to exploit them)
+ Read write-ups (you’ll pick up interesting techniques used by others)

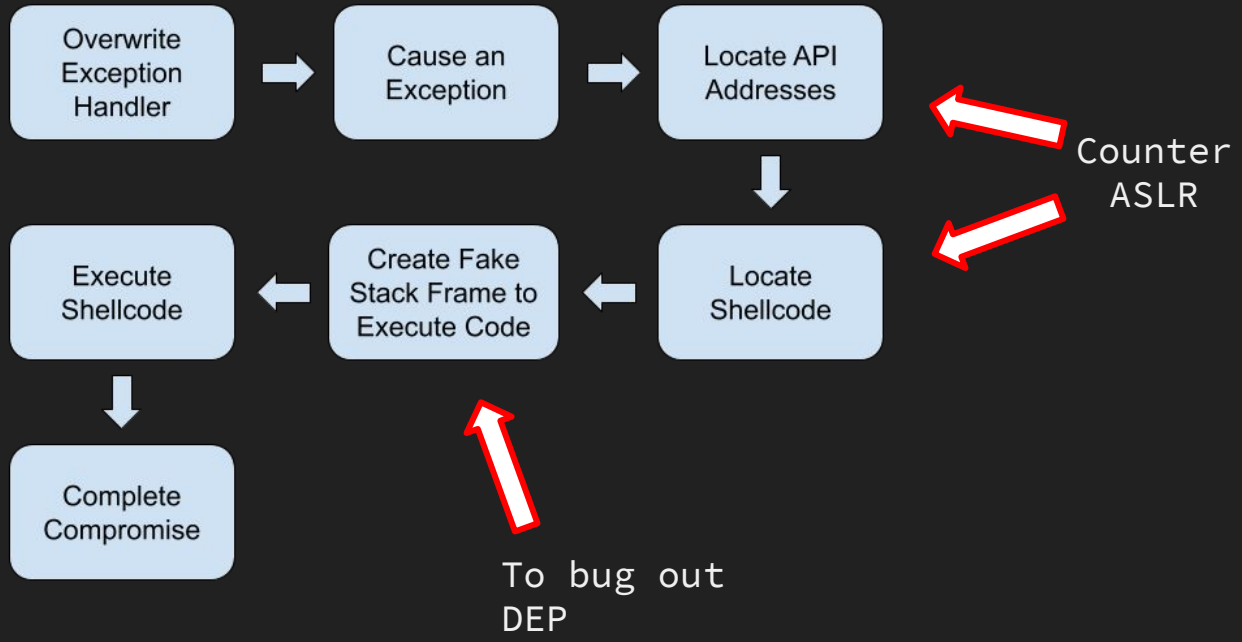
History of Exploits

Exploiting a Stack Overflow: 1996

Exploiting a Stack Overflow: 2003
(Stack Cookies “Stack Canaries”)

History of Exploits

Exploiting a Stack Overflow: 2007
(DEP Data Execution Prevention + ASLR)



Build Tools

Build Tools (before and if you are gonna be heavily testing something)

If I know that I will need to interact with big numbers and crack RSA for a good percentage of.

If you are doing binary exploitation, then maybe a simple script may or may not be good.

Good (To write before)	Not Good (To write before)
Buffer overflow a certain amount of characters	Specific areas, timing and placement

Build Tools

For example:

```
buff = lambda x, y: print(“A”*x+y)
```

Would be a dope technique for an extremely simple and weak buffer overflow. But doesn’t have nearly enough flexibility for a more advanced challenges. (This is where you have to use creativity (and more advanced code) to break it)

+ Sometimes you need to add “\n” to string in order for it to be read.

HAC Server vs Powerful Machine

One of the things I learned recently:

- Don’t worry about having a powerful machine running Kali. More portable to have a server that is stealthy and “slaps”.

  → You can ssh into a machine and have everything there.

- I’ll bring a cool {ATTAC} space with a new server in the coming weeks

Sources

- Types of CyberSec
- Trail of Bits CTF Guide