המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

Reverse Engineering Course

Static Analysis

Barak Gonen

```
call   2084
jmp    15CA
call   17B4
mov    si,7160
xor    di,di
mov    es,[7686]
mov    bx,000F
xor    cx,cx
mov    bp,0001
mov    dx,ds
```

Lesson 1 – Assembly to C Code

Hex View

- http://data.cyber.org.il/reversing/BreakMe.exe
- Open BreakMe exercise with Hex View
  - Neo Hex Editor
  - HXD
  - Etc
- Study as much as you can
  - Code / Data / Imports sections
  - Strings

IDA- Basic

- Interactive Dis-Assembly
- Basic operations:
    - Sections
    - Memory / Graph views
    - Strings view
    - Show machine code
    - Click / Esc
    - Change names
    - Insert comments
    - Convert string -> data -> string

BreakMe

Riddle1

- https://data.cyber.org.il/reversing/riddles.zip
- Convert riddle1.exe to C

Reversing Techniques

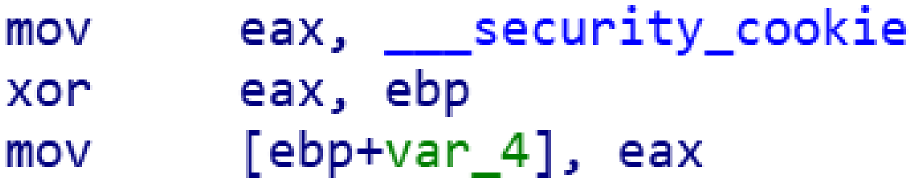
- Focus on the important things- attempting to figure every line is wasteful
- Three steps:
    - 1: Identify main
    - 2: Disregard compiler stuff
    - 3: Identify signatures of functions

Step 1 - Tactics for finding Main

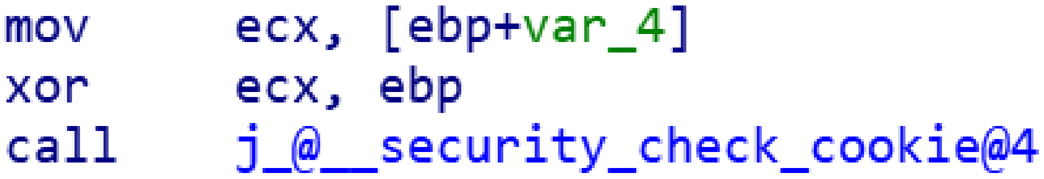
- Use functions graph
- One step before exit routines
- Look for unique argv-argc-envp sequence
- Xref to strings, then go up
- Recognize the compiler ☺
- Find main (riddle 1)

Step 2 - Canary

- Compilers add instructions to verify the stack is untouched
  - Push value and pop it before return
  - Make sure ESP untouched
- Identify by finding matching patterns at func start/end



```
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
```



```
mov     ecx, [ebp+var_4]
xor     ecx, ebp
call    j_@__security_check_cookie@4
```

Step 2 - Other Distractions

- Storing / restoring registers
- Initialization functions
    - CPU information
    - Thread information

Step 3 – Function Signatures

- Args – passed to the func
- Vars – locals
- Who clears the stack?
- Increase our knowledge over time

Practice

- Finish converting riddle 1 to C code

Practice

- Convert riddle2.exe to C

Homework

- Riddle 3, 4, 5

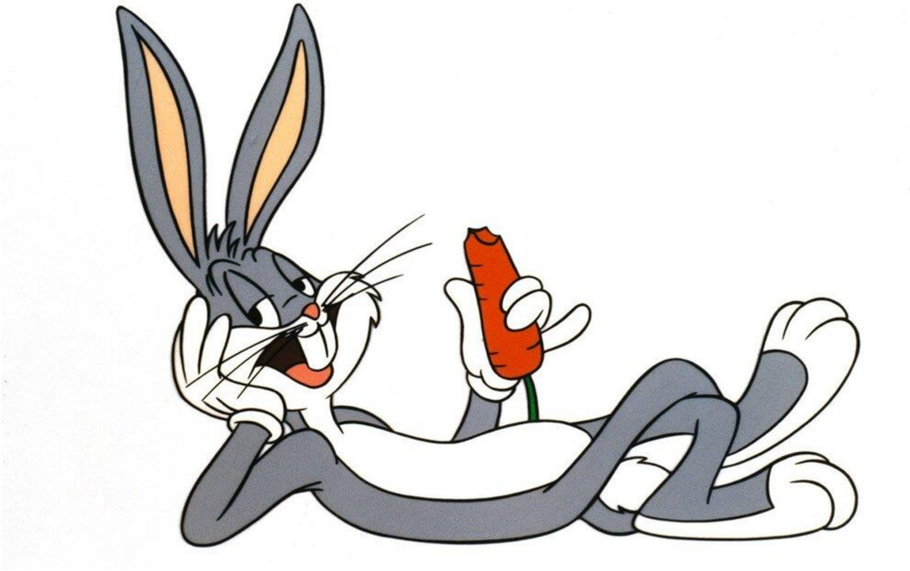
Lesson 2 – Patching, Practice

IDA – Play with Patching

- Patch and apply patches to BreakMe.exe:
  - Step 1: Accept all but correct password
  - Step 2: Accept all passwords
  - Step 3: Don’t even ask for a password
    - Hint: Rename memory location

Practice

- Carrot.exe



Homework

- Pixies.exe
- Vegas.exe