Tutorial 03

Security

Contents

- Frequent mistakes in Exercise Sheet 2
- Quiz
- Canaries and Format String
- ROP Chain
- Time for Clarifications/Mistakes in Marking

Frequent Mistakes in Exercise Sheet 2

- E 2.2 (a)
  - Captured packets given. Which is the used TLS version in the communication?

- TLS Record Version
  - Version: TLS 1.0
  - This field shows minimum supported TLS version
- Extension: supported_versions
  - Supported Version: TLS 1.3
  - Supported Version: TLS 1.2
  - Values used by TLS 1.3 implementations

Frequent Mistakes in Exercise Sheet 2

- E 2.2 (d)
  - Captured packets given. Which is the Domain Name that the client attempts to connect to?

- Frequent answer: webuni.rz.uni-saarland.de
- Correct answer: www.uni-saarland.de or statistics.uni-saarland.de
- Show *Client Hello*

DNS queries to www.uni-saarland.de

16	1.952650509	192.168.5.192	192.168.5.1	DNS	90	Standard query 0x46a4 A www.uni-saarland.de OPT
17	1.952788554	192.168.5.192	192.168.5.1	DNS	90	Standard query 0xea6d AAAA www.uni-saarland.de OPT
18	1.971377845	192.168.5.1	192.168.5.192	DNS	130	Standard query response 0x46a4 A www.uni-saarland.de CNAME webuni.rz.uni-saarland.de A 134.96.7.179 OPT
19	1.975680959	192.168.5.1	192.168.5.192	DNS	157	Standard query response 0xea6d AAAA www.uni-saarland.de CNAME webuni.rz.uni-saarland.de SOA ns.rz.uni-saarland.de OPT
20	1.976333395	192.168.5.192	192.168.5.1	DNS	96	Standard query 0x99fc AAAA webuni.rz.uni-saarland.de OPT
21	1.993629509	192.168.5.1	192.168.5.192	DNS	139	Standard query response 0x99fc AAAA webuni.rz.uni-saarland.de SOA ns.rz.uni-saarland.de OPT
22	1.994458657	192.168.5.192	134.96.7.179	TCP	74	60736 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2881232836 TSecr=0 WS=128
23	2.017118379	134.96.7.179	192.168.5.192	TCP	66	443 → 60736 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1420 SACK_PERM=1 WS=128
24	2.017311607	192.168.5.192	134.96.7.179	TCP	54	60736 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
25	2.017868232	192.168.5.192	134.96.7.179	TLSv1.3	571	Client Hello
26	2.043978652	134.96.7.179	192.168.5.192	TCP	60	443 → 60736 [ACK] Seq=1 Ack=518 Win=30336 Len=0
27	2.045926780	134.96.7.179	192.168.5.192	TLSv1.3	1474	Server Hello, Change Cipher Spec, Application Data

- A and AAAA queries -> response
- Misleading DNS packet in original capture.

Quiz

Buffer-overflows that don't overwrite any pointers:

a. Don't exist.
b. Are insignificant.
c. Only matter on the stack.
d. Are just as dangerous.

Quiz

Buffer-overflows that don't overwrite any pointers:

a. Don't exist.
b. Are insignificant.
c. Only matter on the stack.
d. Are just as dangerous.

Quiz

The effectiveness of shellcode might be hindered by:

a. The size of the buffer where the shellcode is placed.
b. Network difficulties.
c. Randomized address spaces.
d. The compilers decision to reorder variables.

Quiz

The effectiveness of shellcode might be hindered by:

a. The size of the buffer where the shellcode is placed.
b. Network difficulties.
c. Randomized address spaces.
d. The compilers decision to reorder variables.

Quiz

Why is implementing your own stack protection mechanisms usually not a good idea:

a. An attacker can reverse engineer it easily.
b. The compiler could optimize them away.
c. Storing a secret-key securely is only possible if you're the OS.
d. Because it's possible that you implement the measurement wrong.

Quiz

Why is implementing your own stack protection mechanisms usually not a good idea:

a. An attacker can reverse engineer it easily.
b. The compiler could optimize them away.
c. Storing a secret-key securely is only possible if you're the OS.
d. Because it's possible that you implement the measurement wrong.

Quiz

What is a commonly used countermeasure against ROP attacks:

a. Removing all ROP-gadgets.
b. CFI.
c. ASLR.
d. NX stack.

Quiz

What is a commonly used countermeasure against ROP attacks:

a. Removing all ROP-gadgets.
b. CFI.
c. ASLR.
d. NX stack.

Quiz

What happens on an integer overflow:

a. An integer container on the stack is used to overflow into the return pointer.
b. The size limit of an integer is exceeded.
c. A program crashes because it was given too much integers as parameters.
d. An integer pointer gets incremented.

Quiz

What happens on an integer overflow:

a. An integer container on the stack is used to overflow into the return pointer.
b. The size limit of an integer is exceeded.
c. A program crashes because it was given too much integers as parameters.
d. An integer pointer gets incremented.

Canary and Format Strings

- Have a look at demo1.c

- Two executables:
  - gcc demo1.c -Wall -o demo1
  - gcc demo1.c -fstack-protector-all -Wall -o demo1_sp

Canary and Format Strings

- Prologue/Epilogue
- Stack frame
- Same canary is used, one leaked all leaked
- If buffer overflow present:
  - Can overwrite return address
  - Normally canary would prevent this
  - But we also know canary value, so we can pass check

ROP Chains

- Try to spawn a shell via ***/bin/sh***

- Recap:
  - Last week we saw how to use systemcalls
  - In order to spawn a shell we need *execve(/bin/sh, 0, 0)*
  - Plenty of gadgets available in binary
  - Buffer Overflow present [Show how to detect]

ROP Chains

- In order to use *execve*, we need to prepare registers
  - Link
  - rax => syscall number = 59
  - rdi => *filename = /bin/sh
  - rsi => *argv = 0
  - rdx => *envp = 0

- How to find gadgets:
  - Can use ***ropper:*** pip3 install ropper
  - Usage: ropper --file rop_n_roll --search "pop rdx"

Time for Clarifications/Mistakes in Marking

- Any gripes?

Feedback Form

- Would like to see anything different?
- Liked it, hated it, something can be improved?

- Link: https://forms.gle/JqMrDToQgf1Utyp16