

TEST & EVALUATION TASK

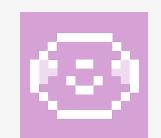
#116 Type 3 - Kernel Exploit Simulation Test <>

This task belongs to #63 Morphisec

 Created by jacky lim zhiqi
03 Aug 2017 10:04

+ Add tag

OPEN NEEDS INFO ▾

 Assigned to
jacky lim zhiqi

0 Watchers

 WATCH

+ ADD WATCHERS



Test Harness = HEVD

github.com/hacksystem/HackSysExtremeVulnerableDriver

Vulnerabilities Implemented

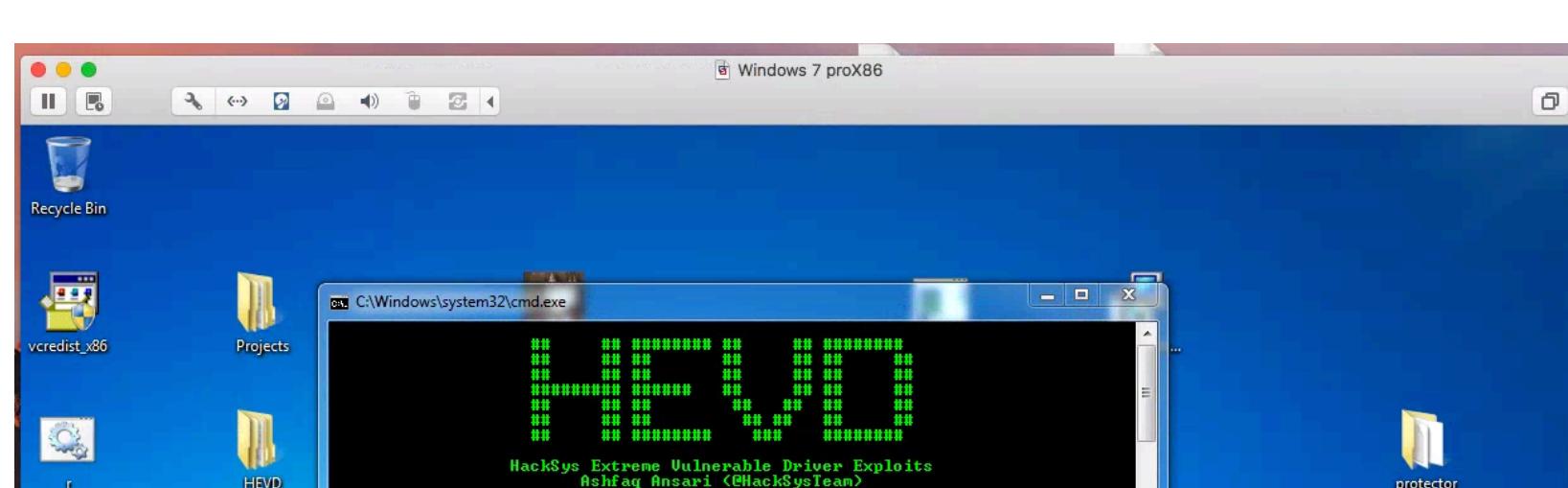
- Double Fetch
- Pool Overflow
- Use After Free
- Type Confusion
- Stack Overflow
- Integer Overflow
- Stack Overflow GS
- Arbitrary Overwrite
- Null Pointer Dereference
- Uninitialized Heap Variable
- Uninitialized Stack Variable

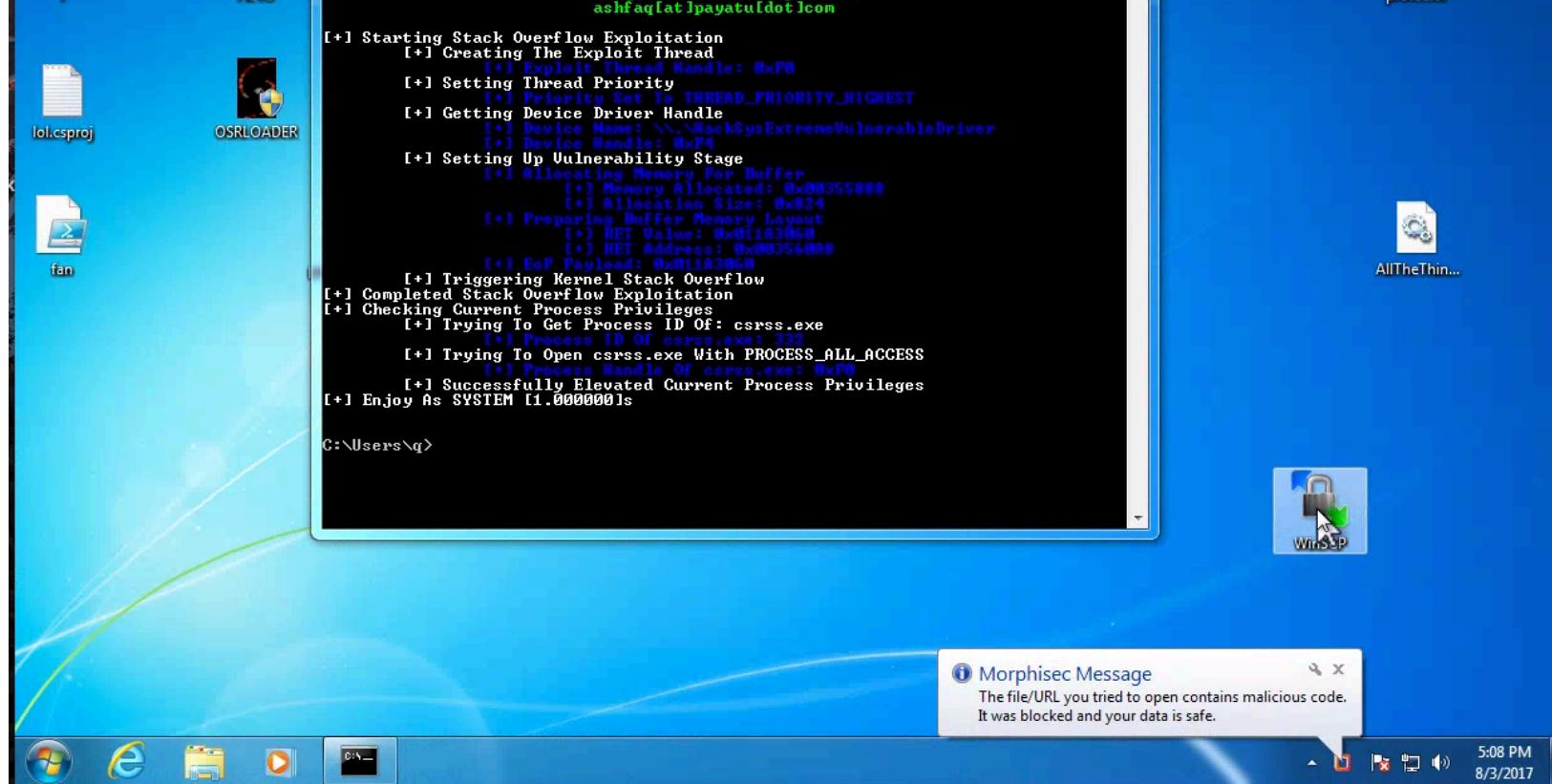
Excluded: Double Fetch, Pool Overflow & Stack Overflow GS didn't work on the target VM.

Ensure Plan Covers ALL Applications & Updated for the target Protector

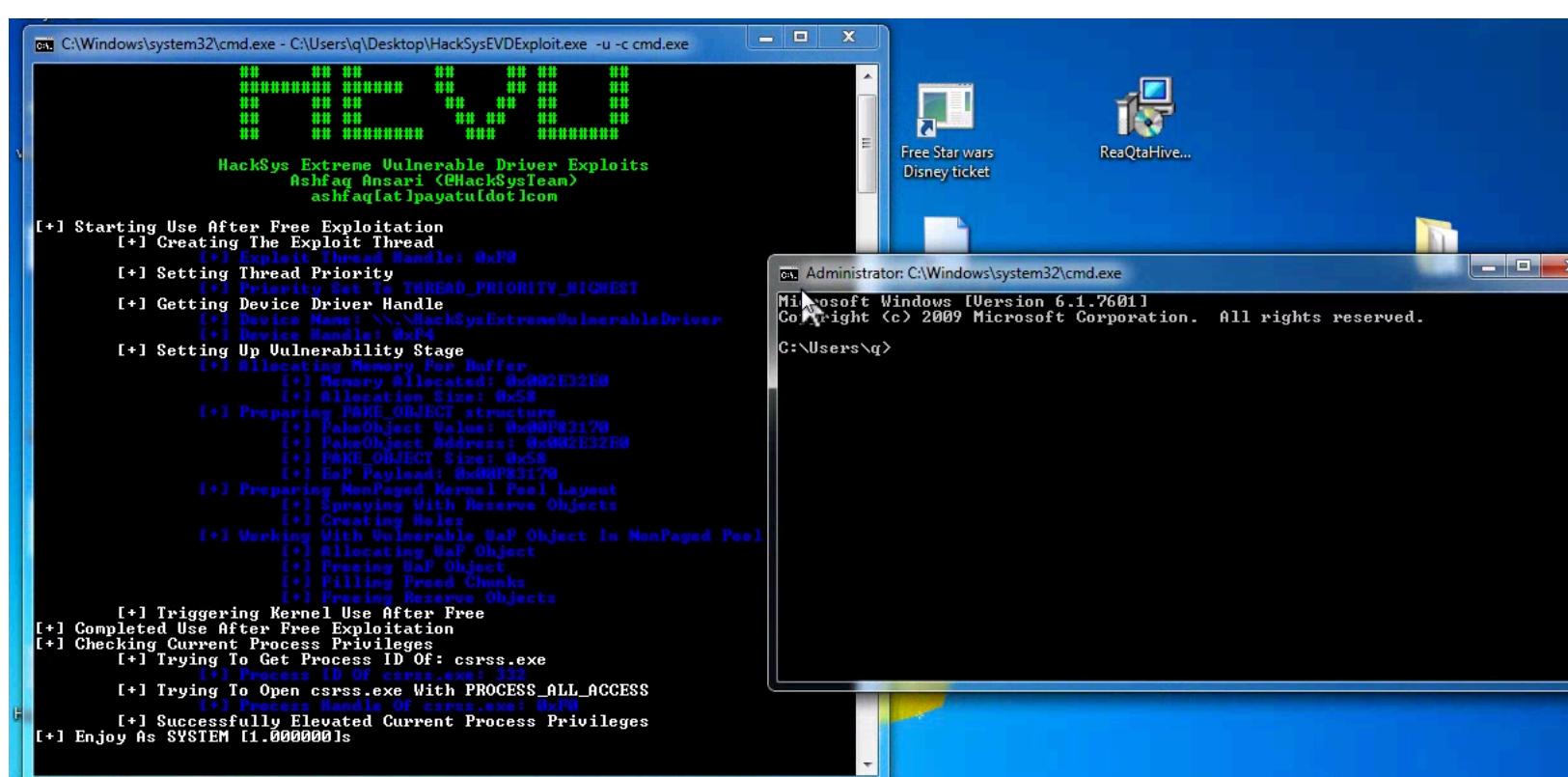
The screenshot shows the Morphisec interface for creating a troubleshoot plan. The left sidebar has 'MORPHISEC' and 'PLANS' selected. The main area is titled 'TROUBLESHOOT PLAN'. It includes sections for 'General Settings' (Plan Name: test1), 'Protection Plan' (dropdown set to 'Protect All Applications' with a red arrow pointing to it), 'Exclude the following child processes' (empty field), and 'Pop Up Notification Message' (checkbox checked, message: 'The file/URL you tried to open contains malicious code. It was blocked and your data is safe.'). A sidebar on the right shows a host entry: 'WIN-7C5F483R3S8'.

Run Shellter-tainted Winscp to ensure it is working. As shown it is blocked

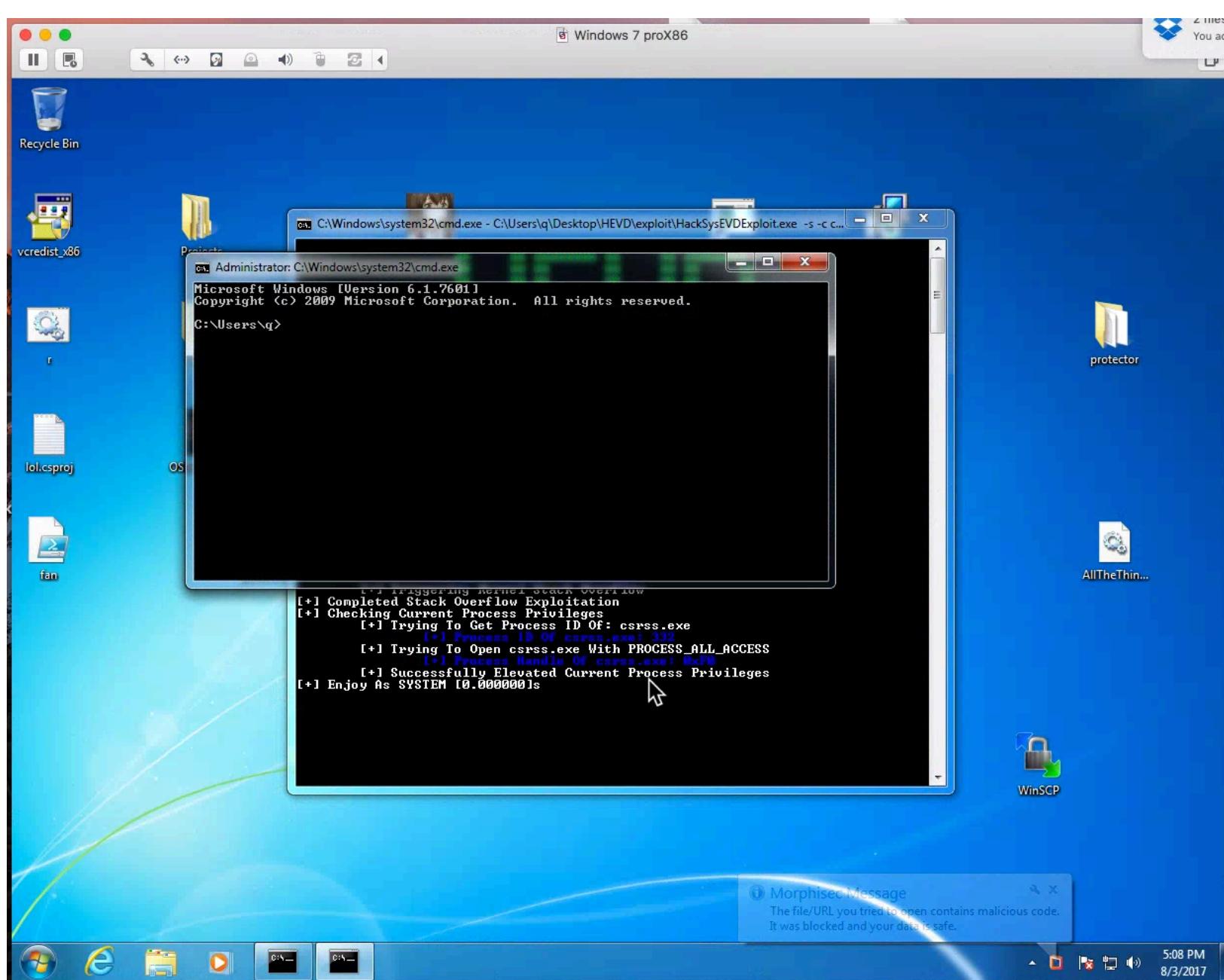




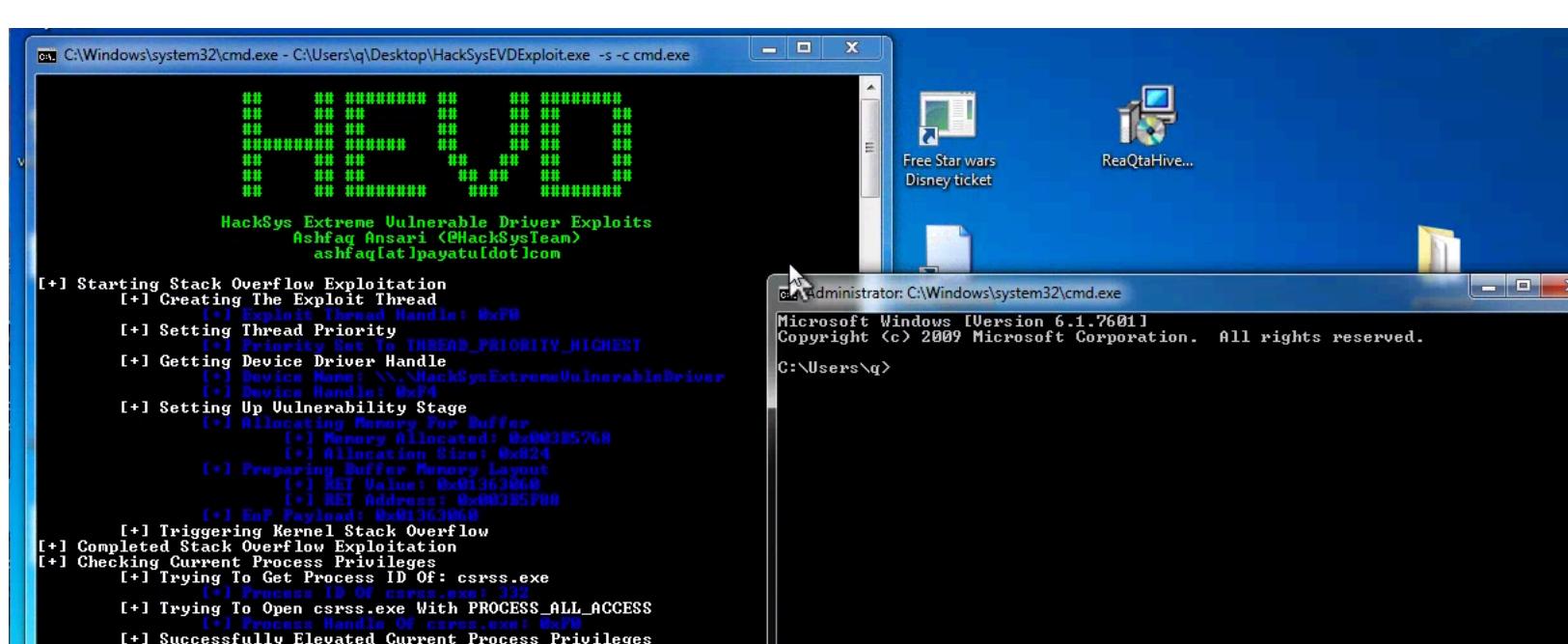
UAF - MISSED



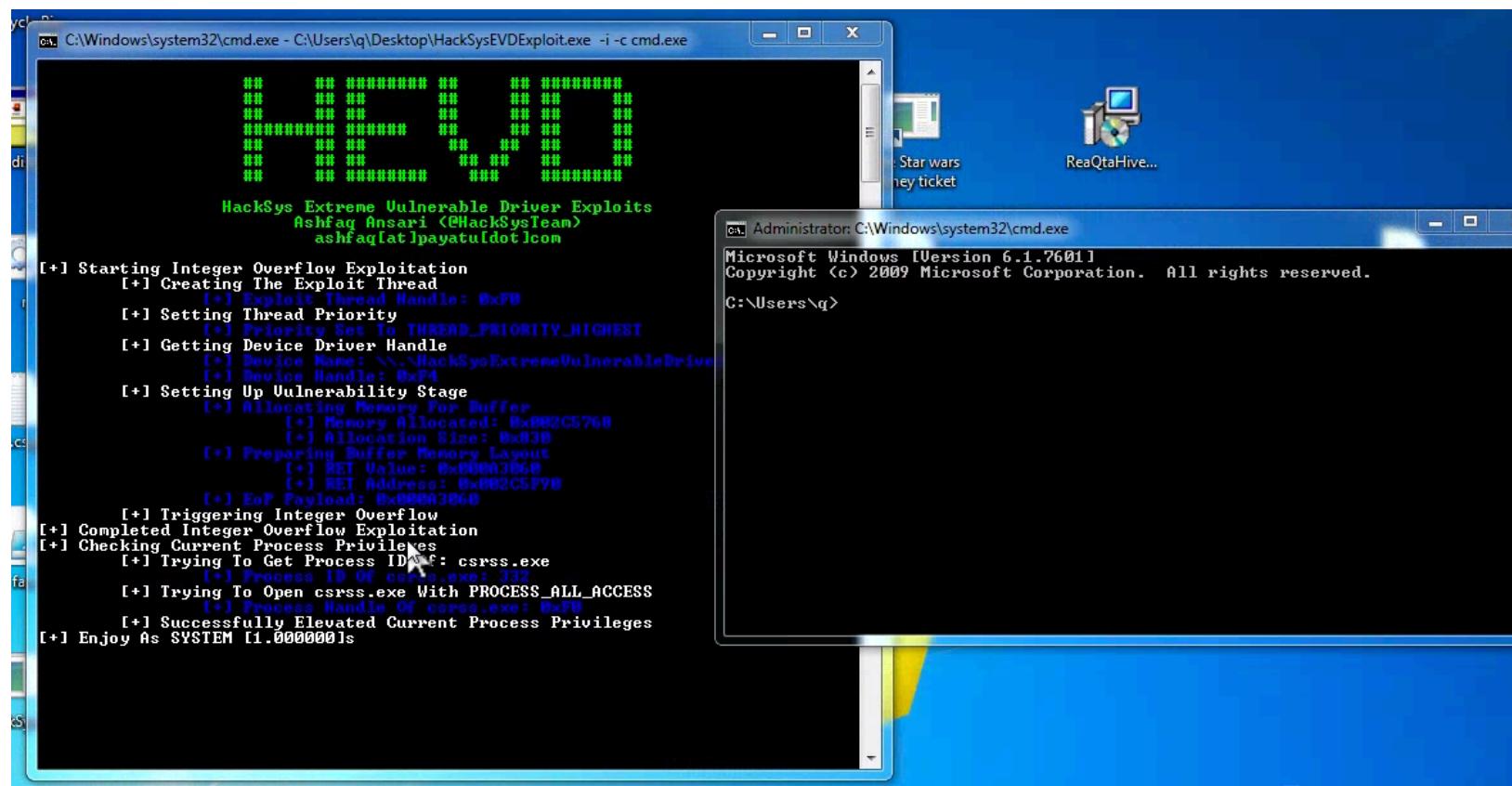
Type Confusion - MISSED



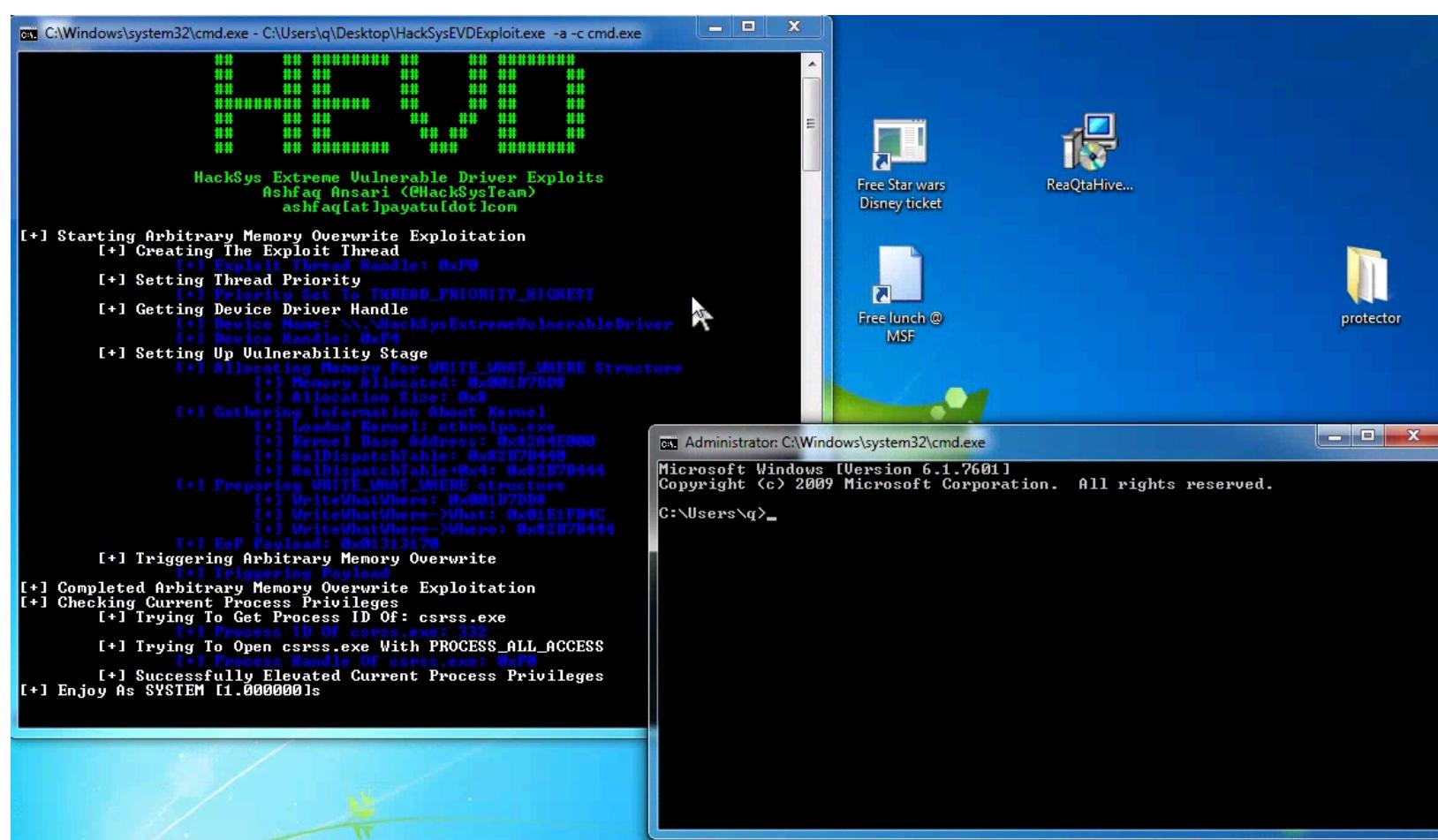
Stack Overflow - MISSED



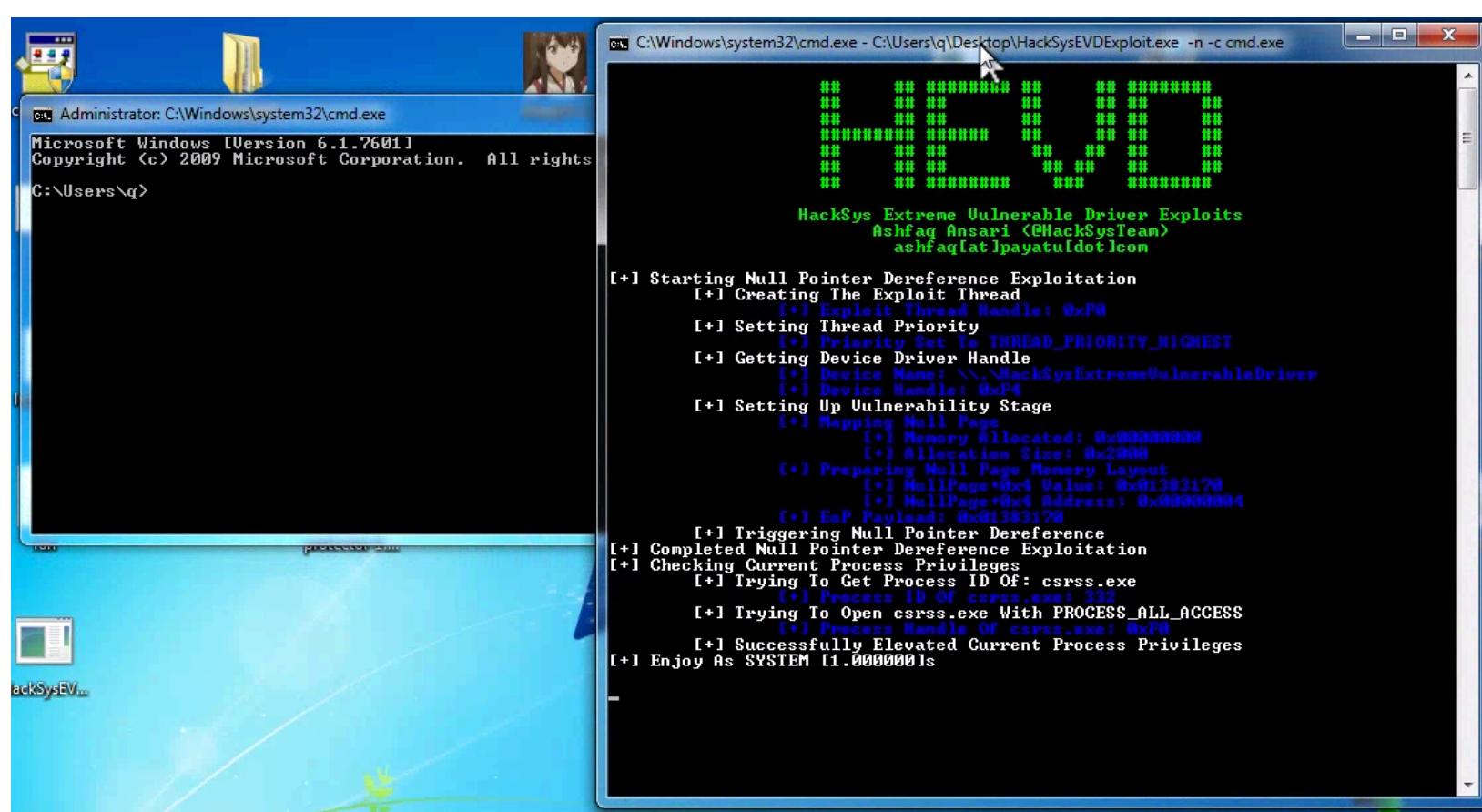
Integer Overflow - MISSED



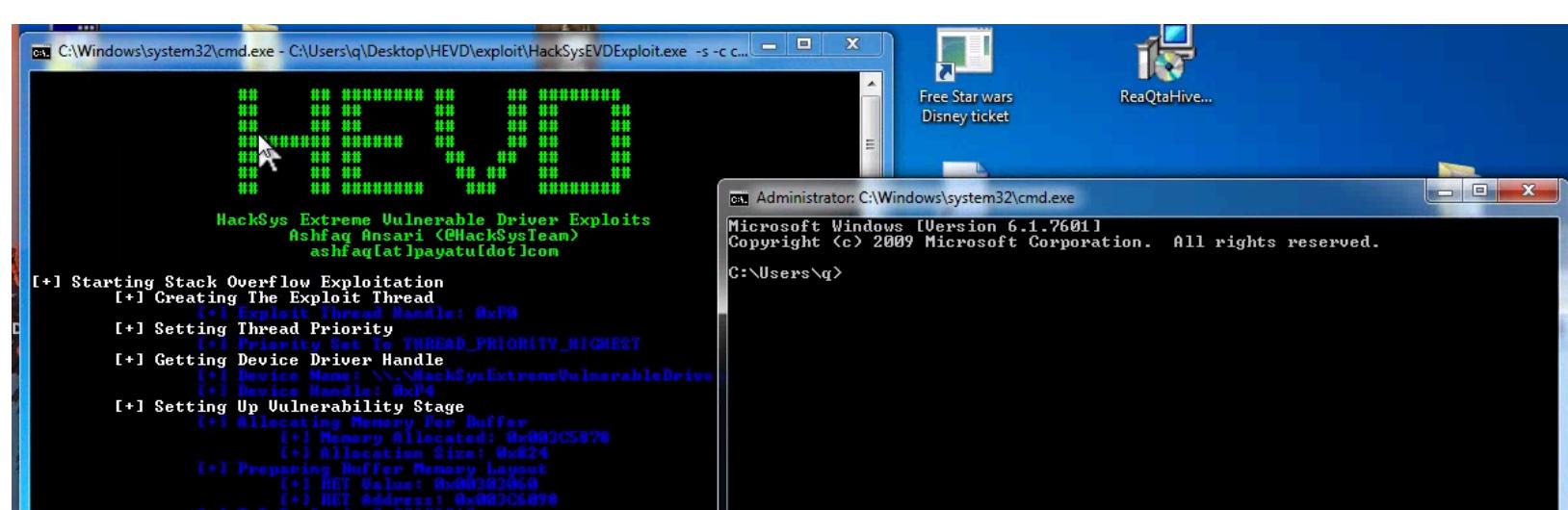
Arbitrary Overwrite - MISSED



Null Pointer Deref - MISSED

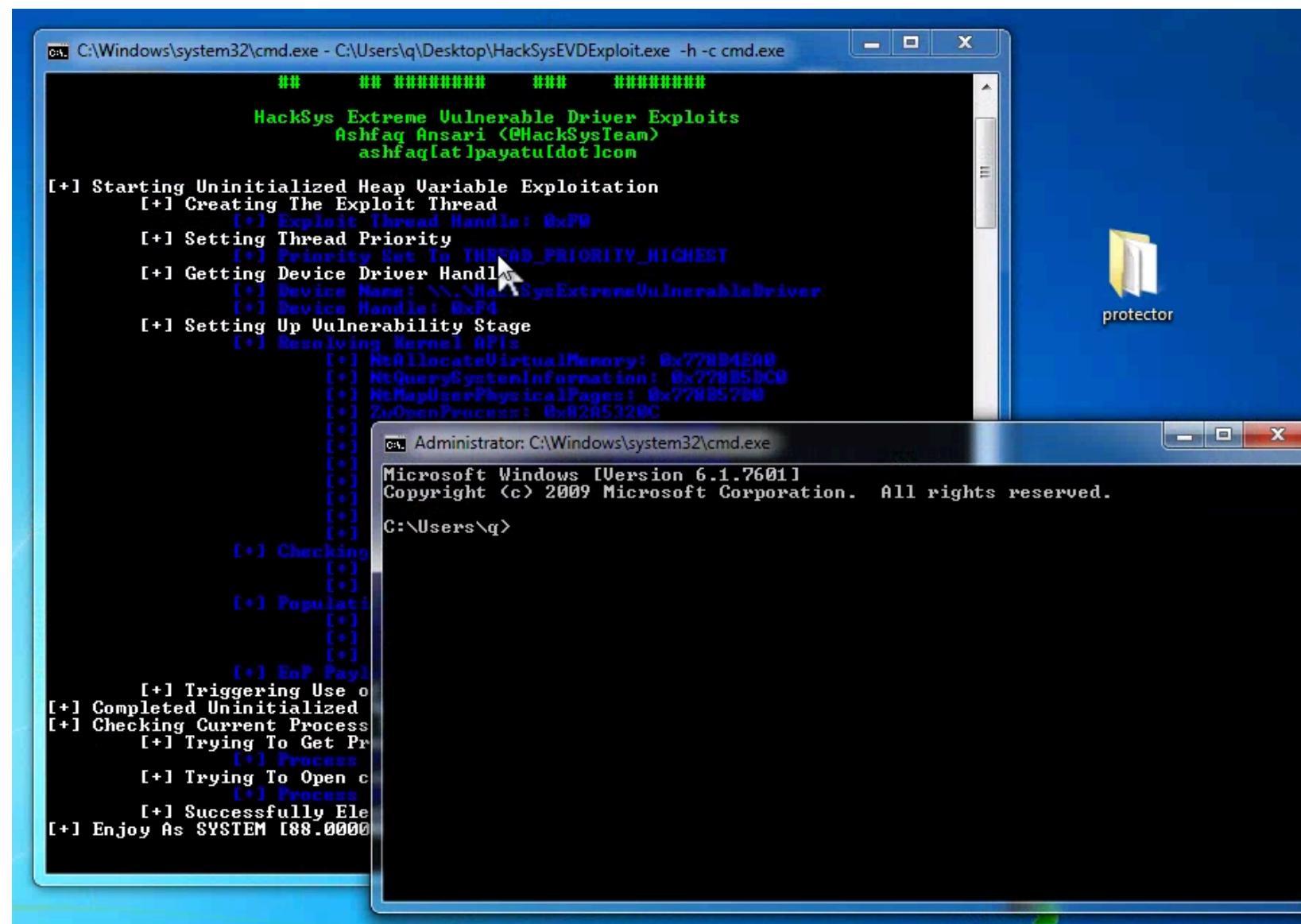


Stack Overflow - MISSED

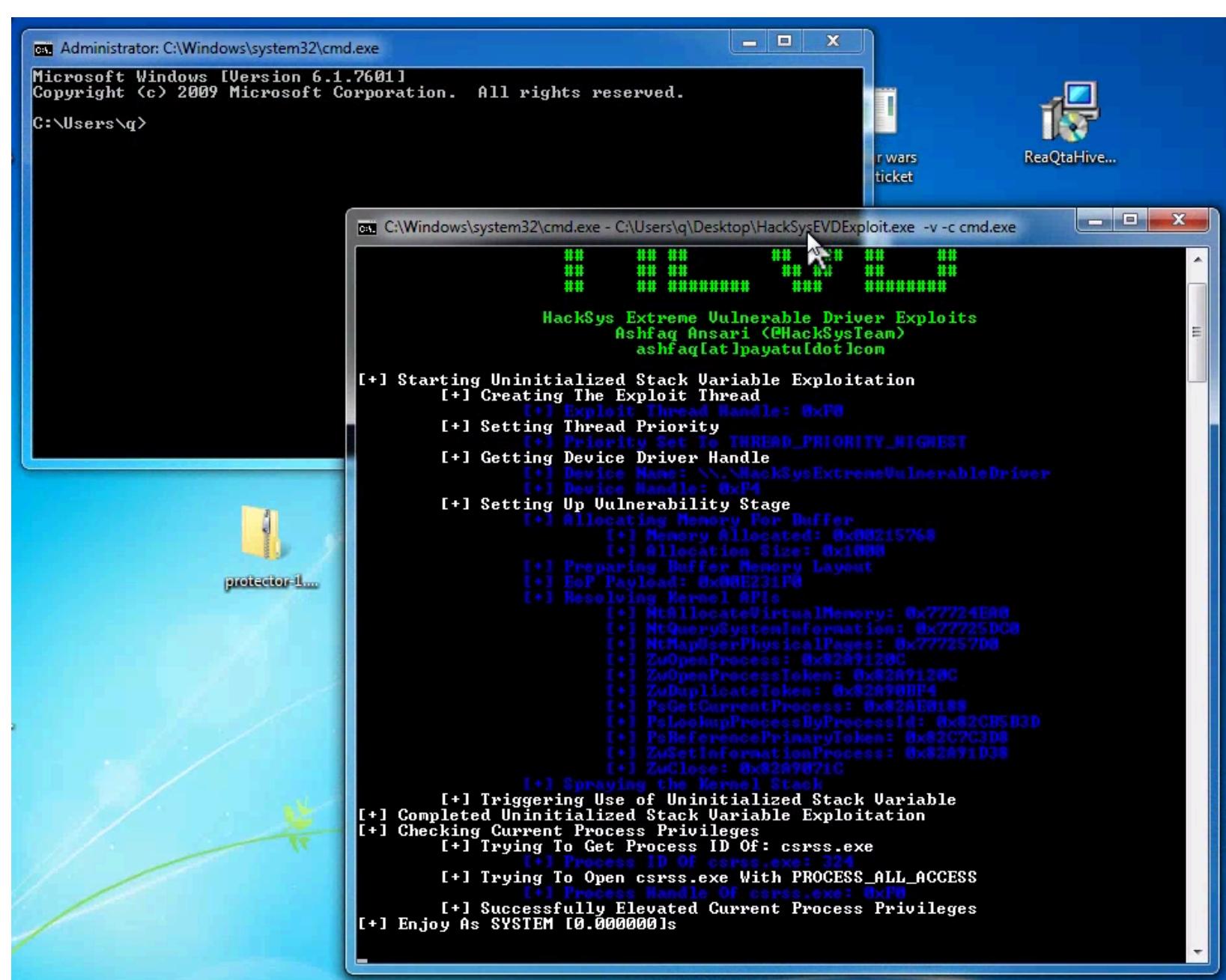


```
[+] EsP Payload: 0x00303060
[+] Triggering Kernel Stack Overflow
[+] Completed Stack Overflow Exploitation
[+] Checking Current Process Privileges
[+] Trying To Get Process ID Of: csrss.exe
    [*] Process ID Of csrss.exe: 332
[+] Trying To Open csrss.exe With PROCESS_ALL_ACCESS
    [*] Process Handle Of csrss.exe: 0x1F0
[+] Successfully Elevated Current Process Privileges
[+] Enjoy As SYSTEM [0.000000]
```

Heap Variable Exploitation - MISSED



Stack Variable Exploitation - MISSED



HEVD Setup

To prepare for HEVD Test Access the link below to download driver

github.com/hacksysteam/HackSysExtremeVulnerableDriver

Extract the download zip file into c:\User\public\ Copy the attached script into test VM.