TEST & EVALUATION TASK

OPEN NEEDS INFO

0

#116 Type 3 - Kernel Exploit Simulation Test

This task belongs to #63 Morphisec

Assigned to
jacky lim zhiqi

Created by jacky lim zhiqi
03 Aug 2017 10:04

0 Watchers

WATCH + ADD WATCHERS

+ Add tag

Test Harness = HEVD

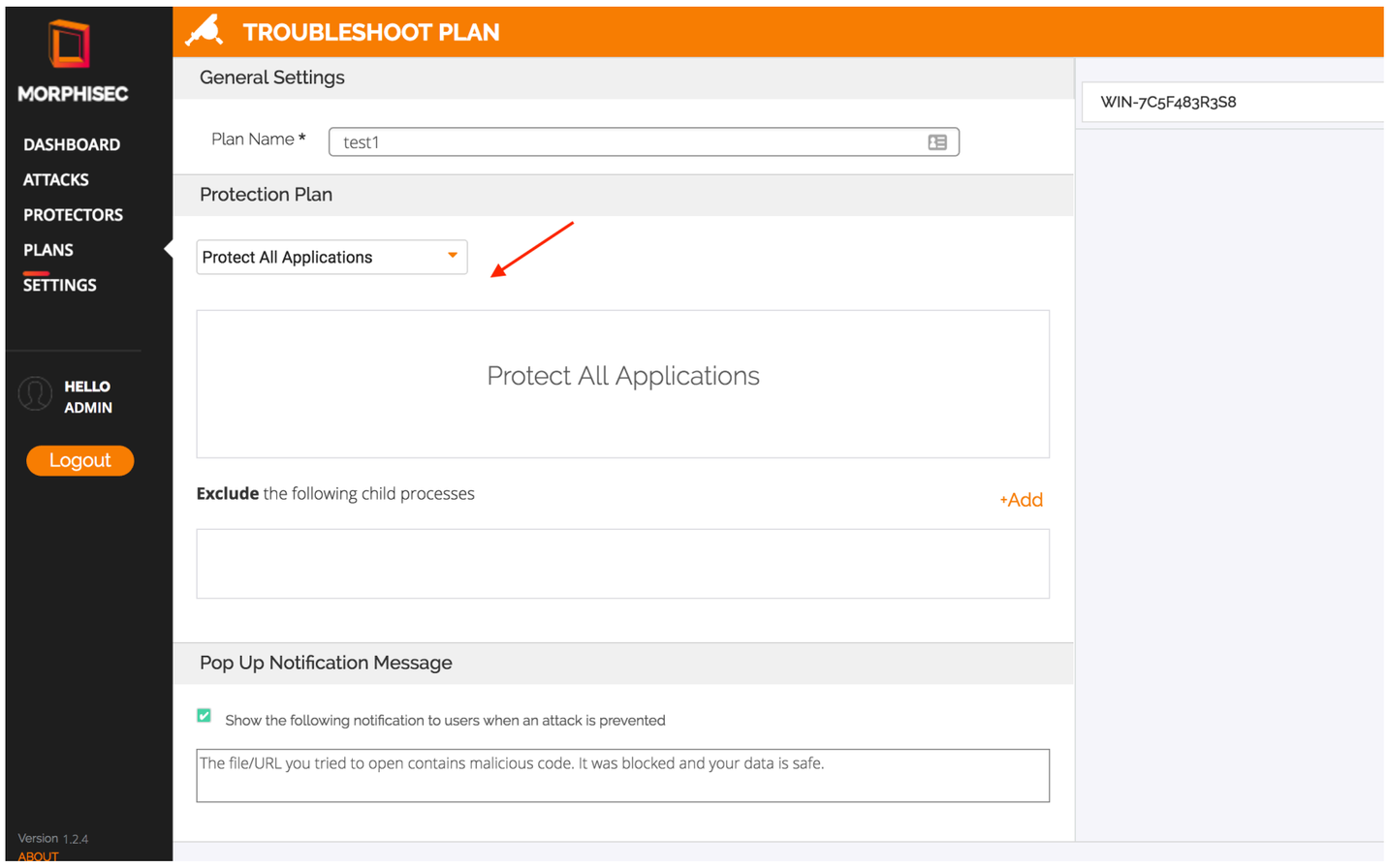
github.com/hacksysteam/HackSysExtremeVulnerableDriver

Vulnerabilities Implemented

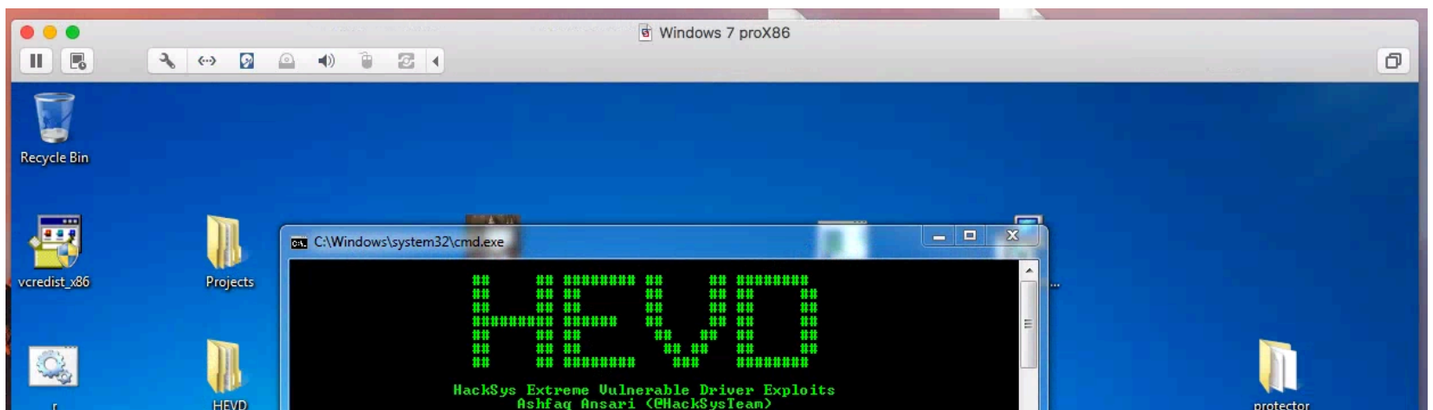
- Double Fetch
- Pool Overflow
- Use After Free
- Type Confusion
- Stack Overflow
- Integer Overflow
- Stack Overflow GS
- Arbitrary Overwrite
- Null Pointer Dereference
- Uninitialized Heap Variable
- Uninitialized Stack Variable

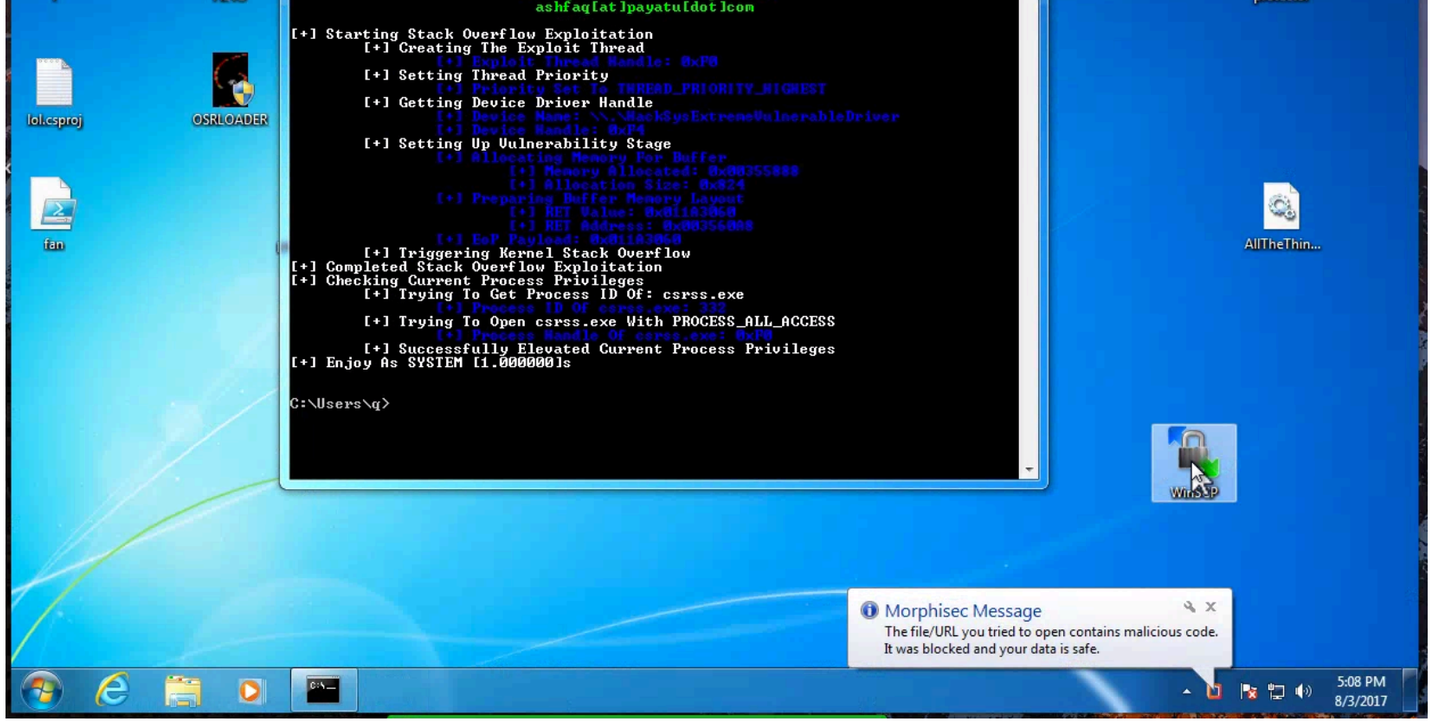
Excluded: Doube Fetch, Pool Overflow & Stack Overflow GS didn't work on the target VM.

Ensure Plan Covers ALL Applications & Updated for the target Protector

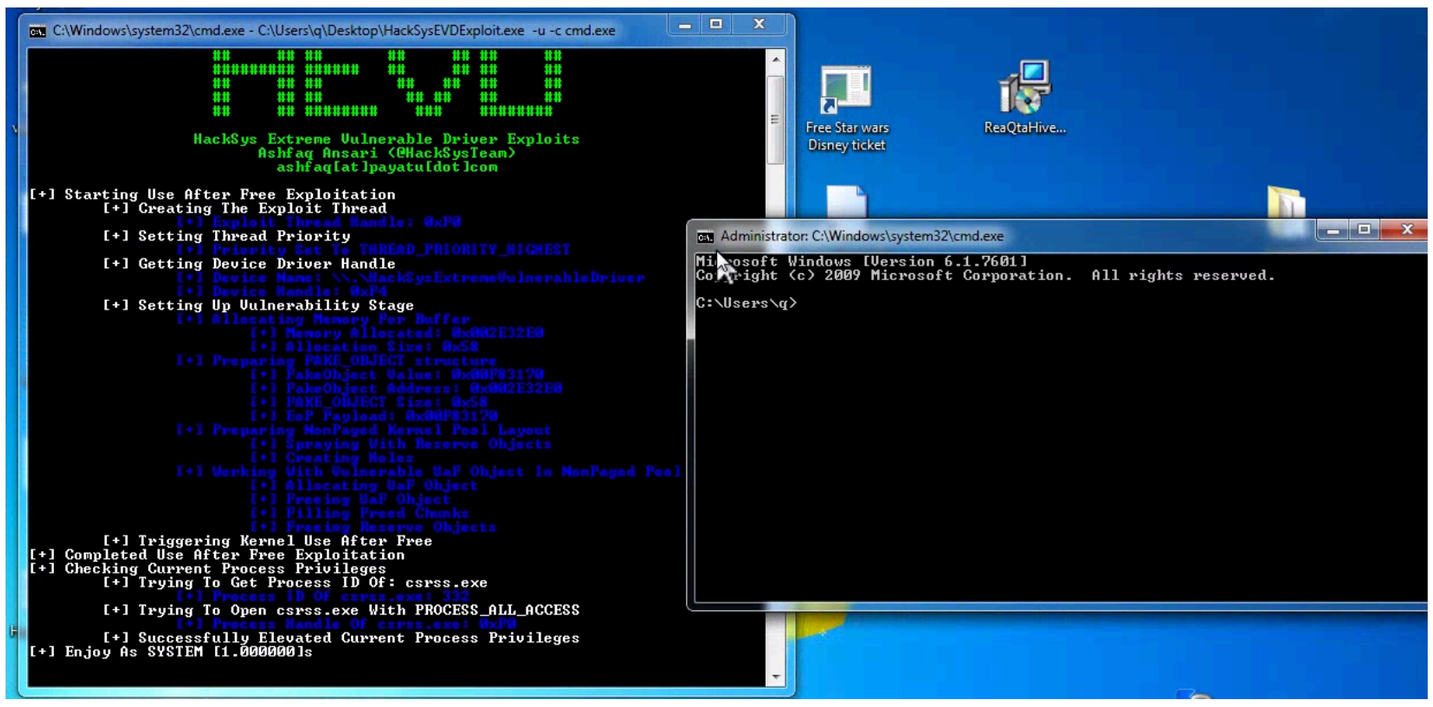


Run Shellter-tainted Winscp to ensure it is working. As shown it is blocked

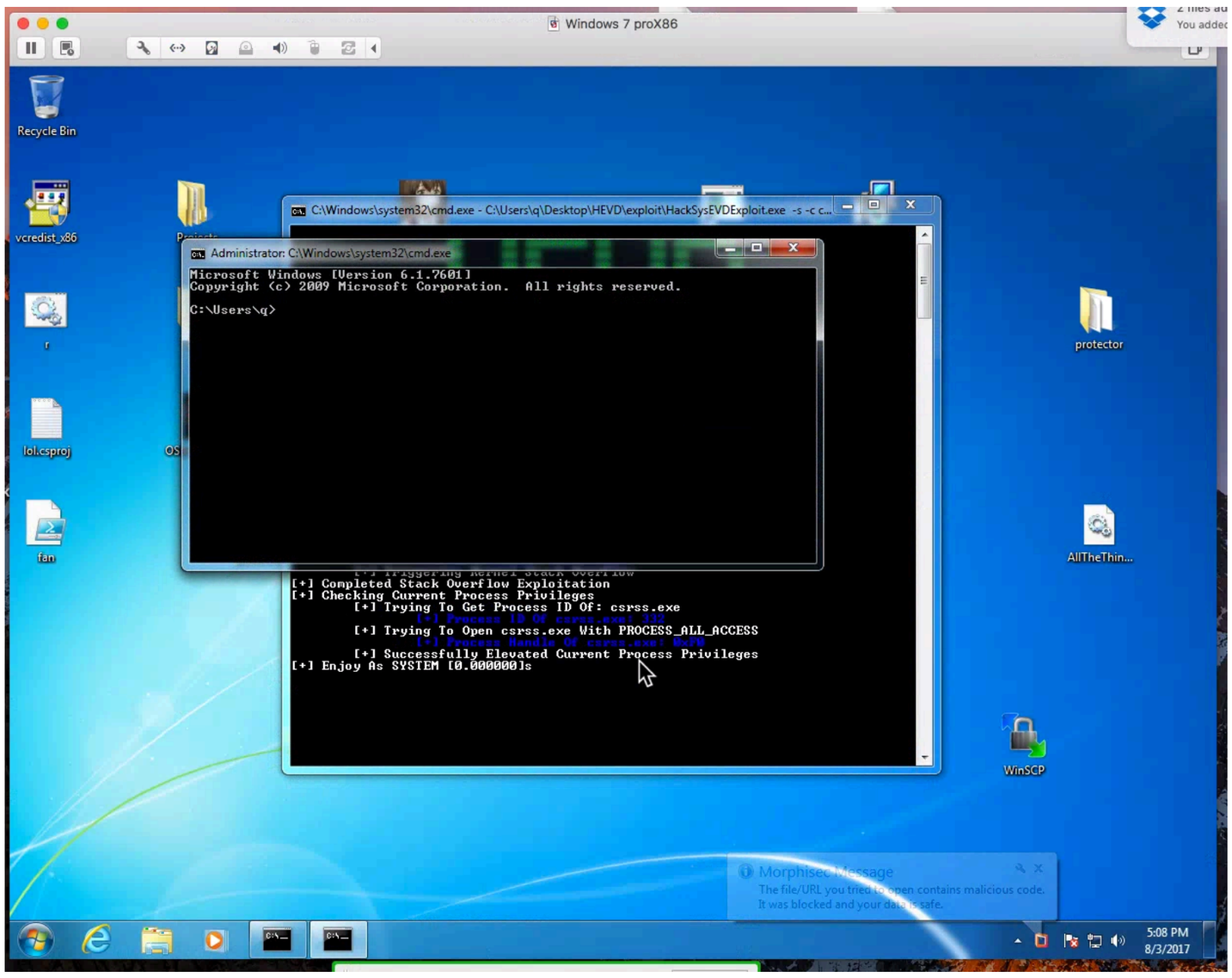




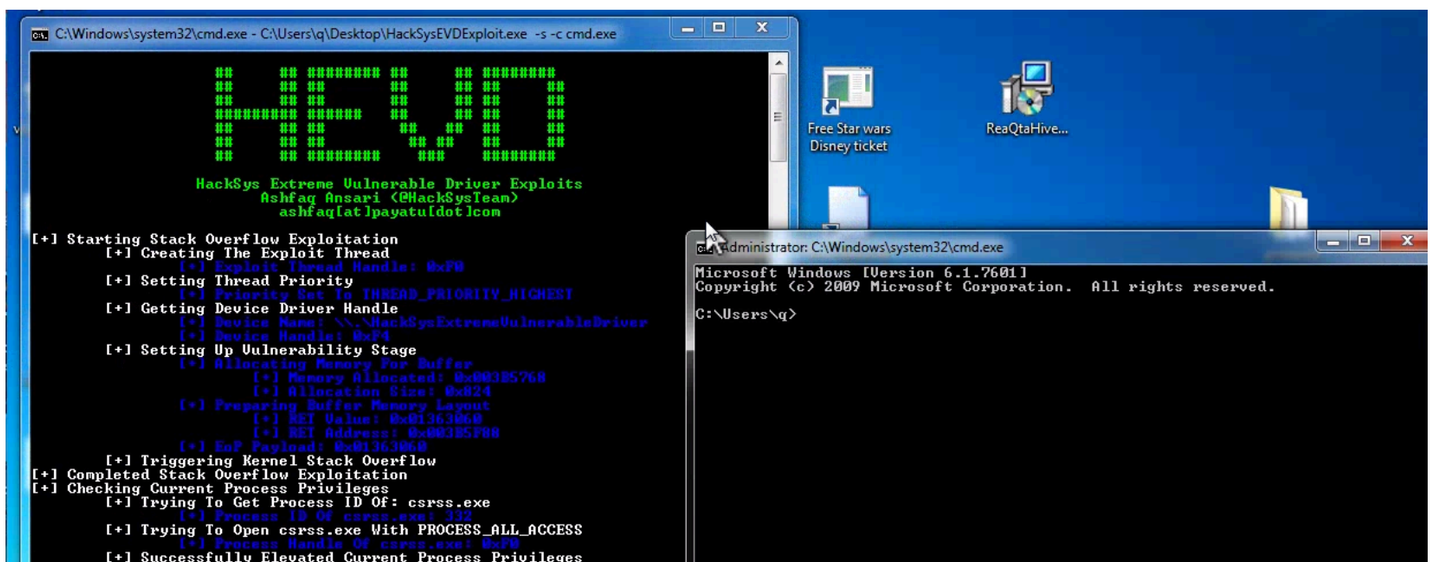
UAF - MISSED



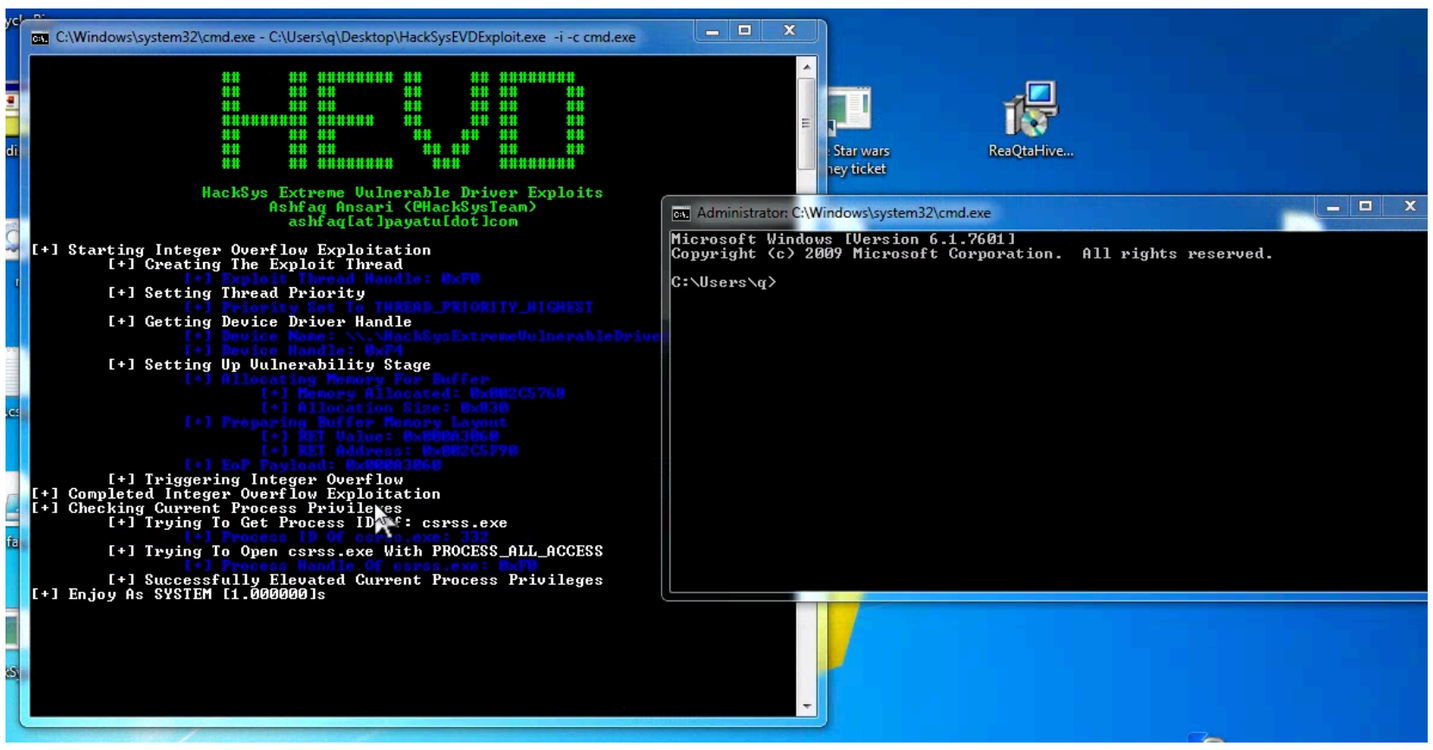
Type Confusion - MISSED



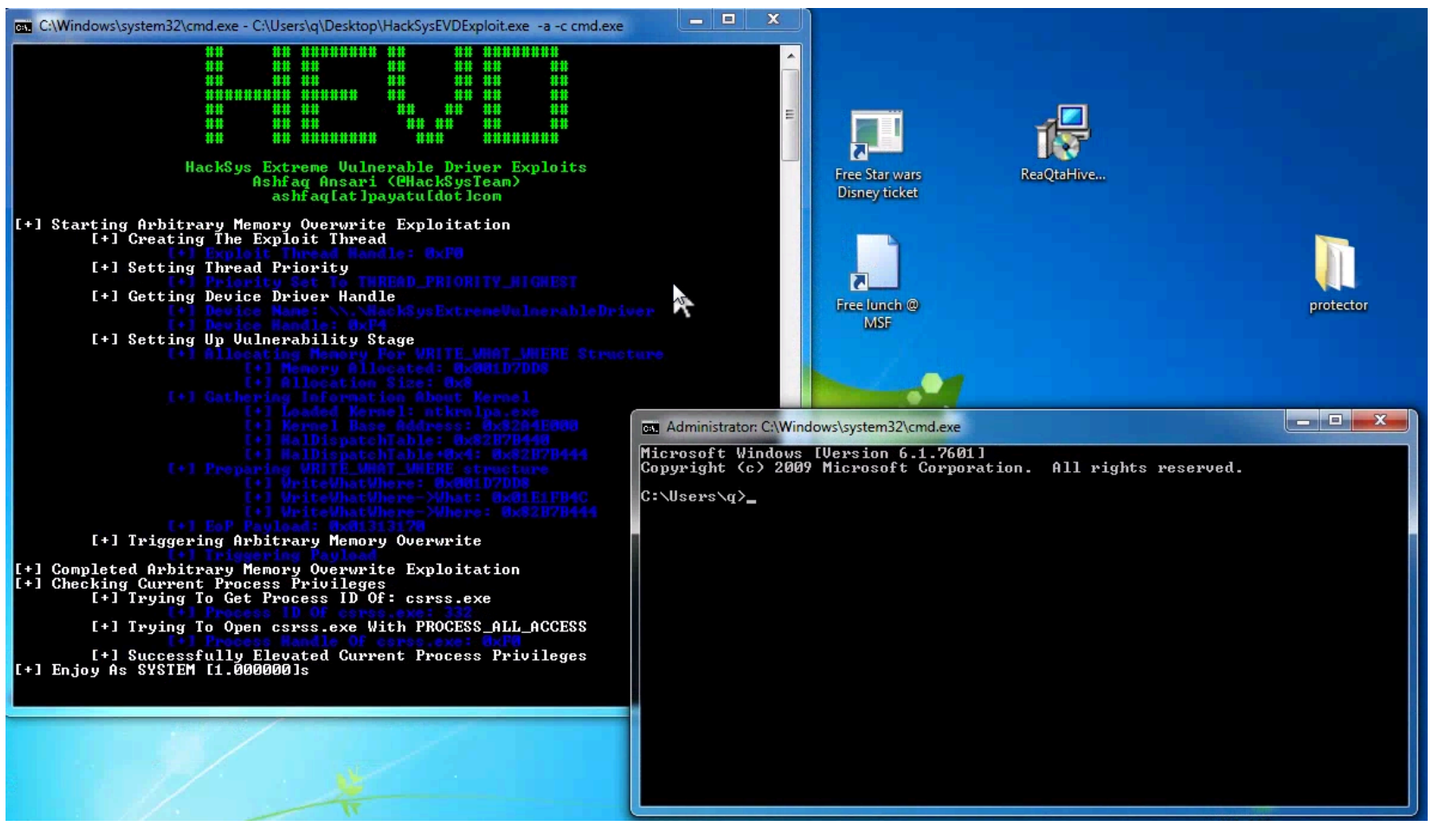
Stack Overflow - MISSED



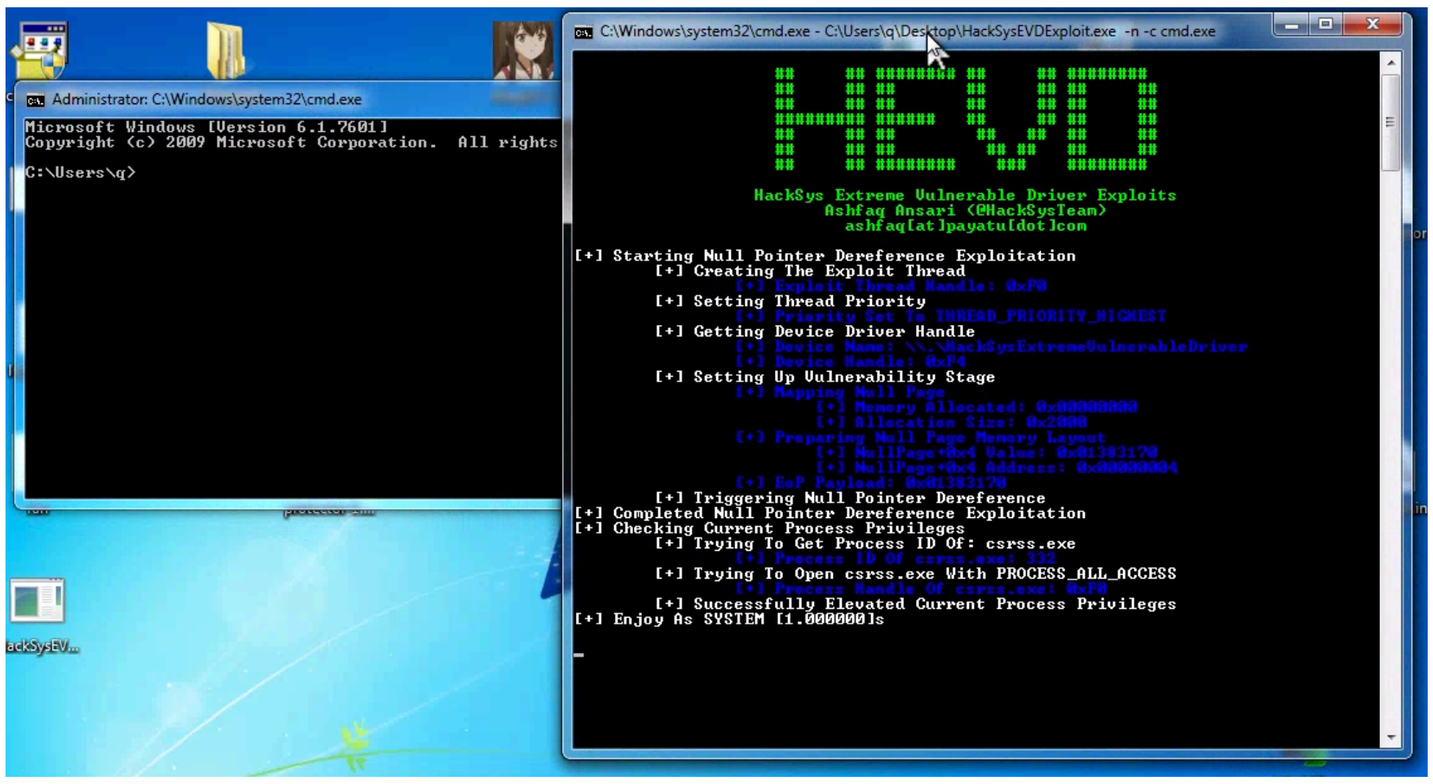
Integer Overflow - MISSED



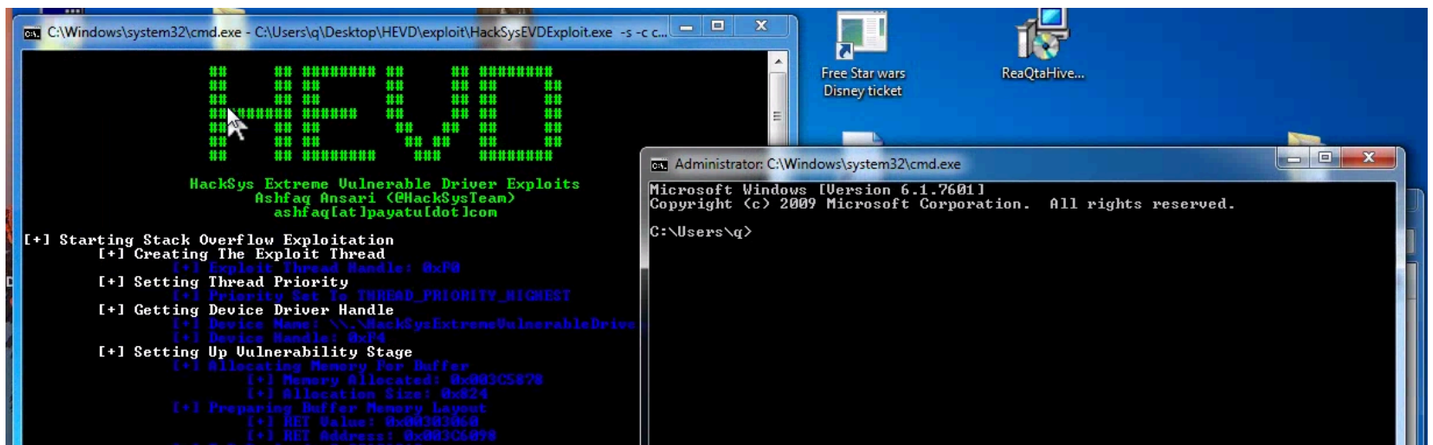
Arbitrary Overwrite - MISSED

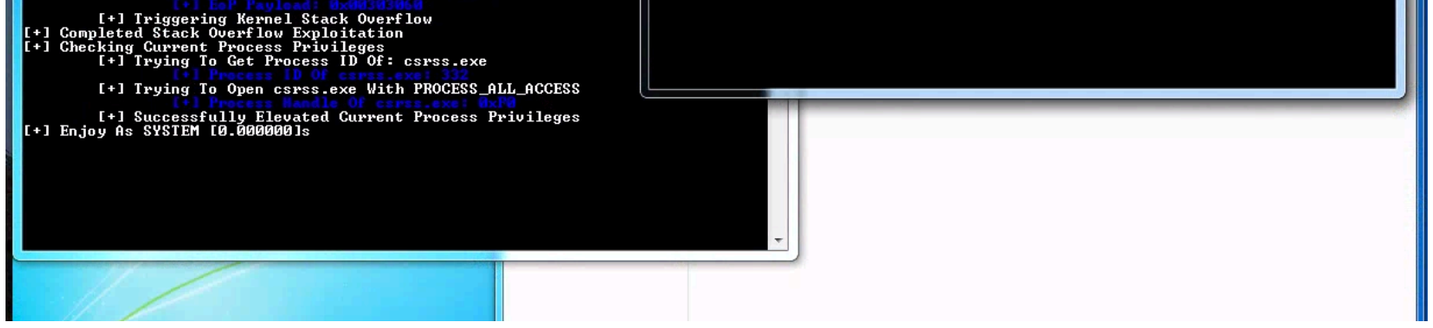


Null Pointer Deref - MISSED

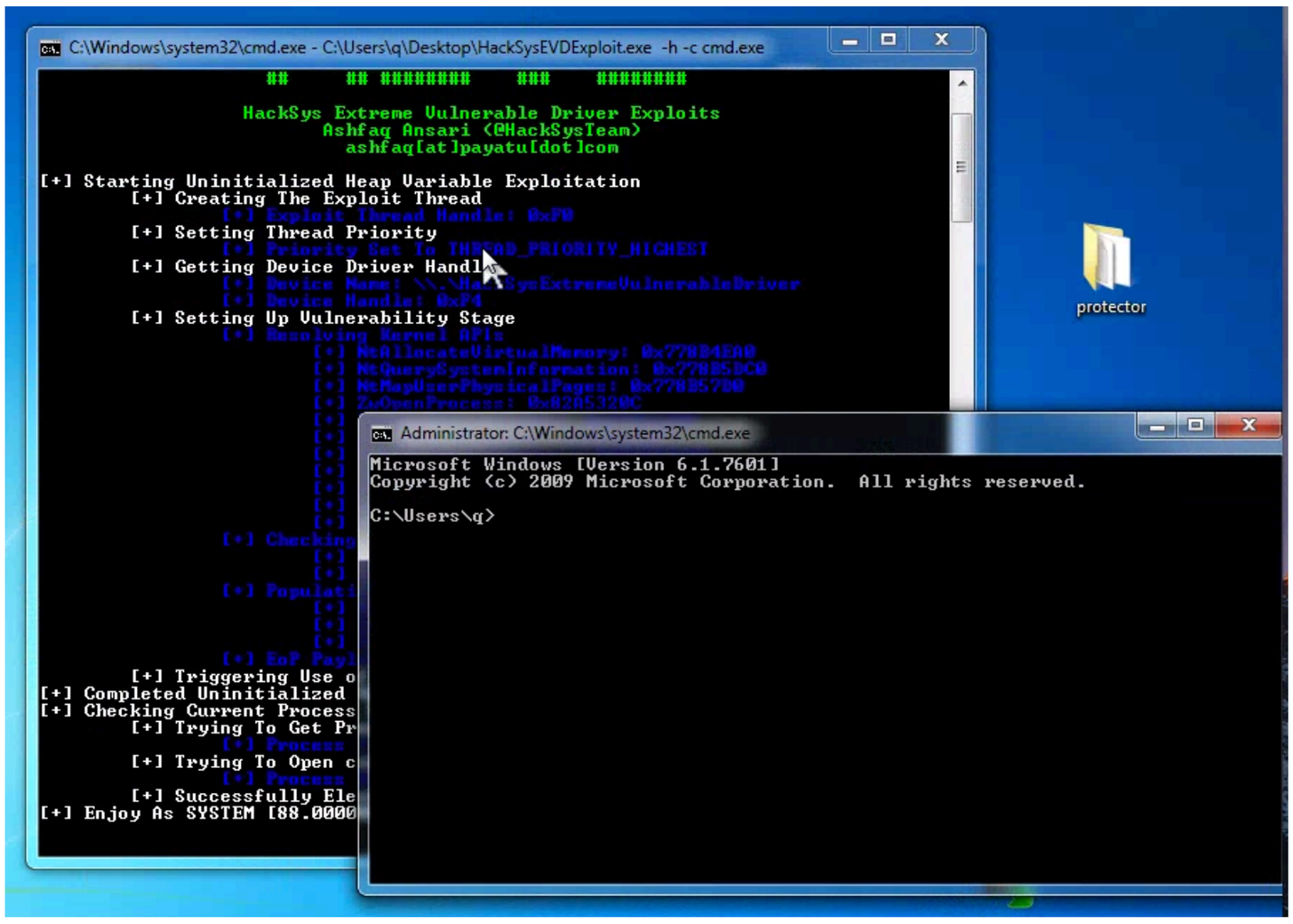


Stack Overflow - MISSED

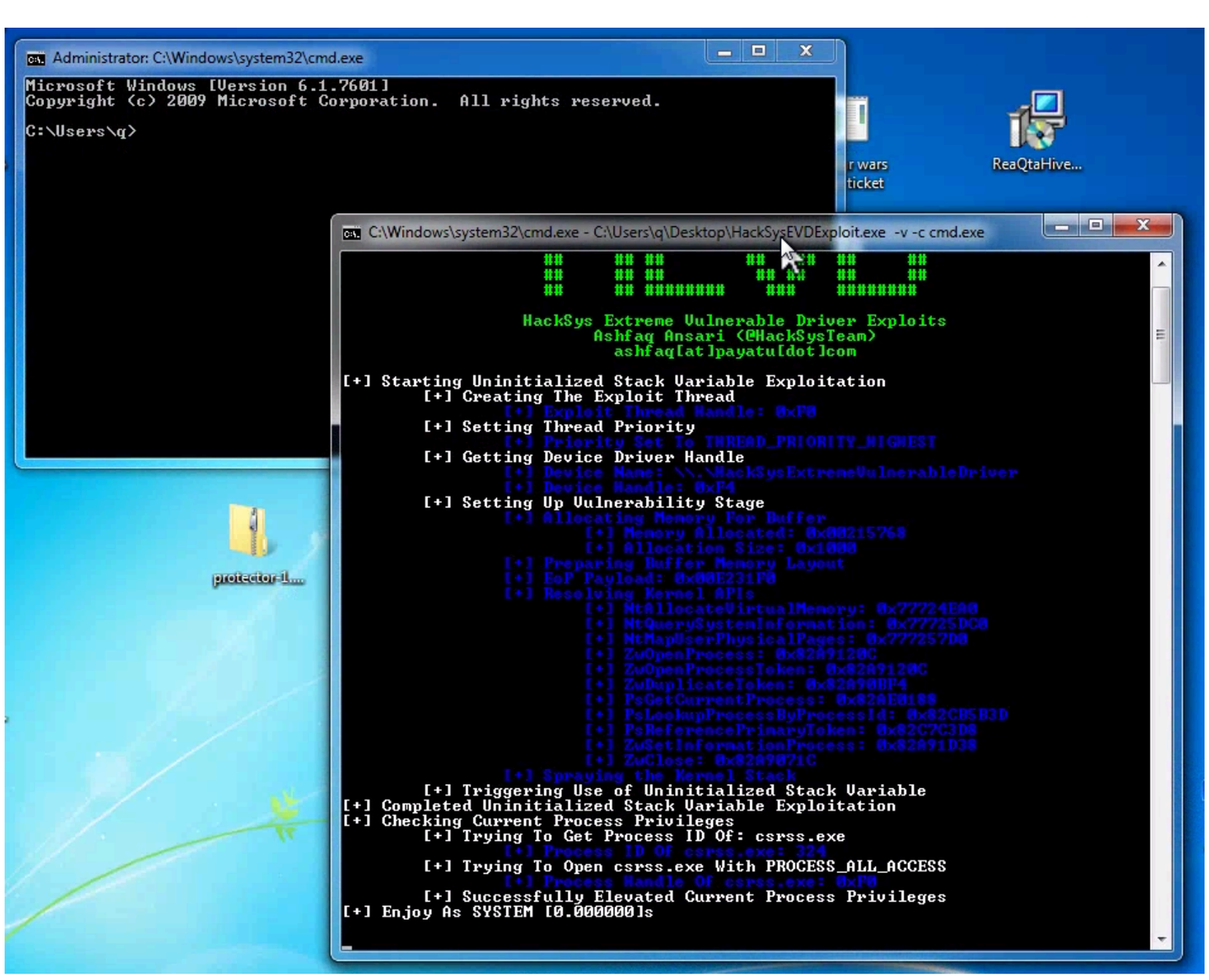




Heap Variable Exploitation - MISSED



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.

13 attachments

Screenshot 2017-08-03 17.08.47(2).png 751.1 KB