



UNIVERSITY
OF TRENTO - Italy



eit Digital
MASTER SCHOOL


Offensive technologies

Fall 2016


Lecture 7

Exploit assignments

26/10/16 Fabio Massacci - Offensive Technologies 1



UNIVERSITY
OF TRENTO - Italy




eit Digital
MASTER SCHOOL


Exploit presentation session

- ***Analysts → 7th of November (Monday)***
- ***Technical → 9th of November (Wednesday)***
- ***Both tracks: Exploit session must convey that you have a clear understanding of how the exploit works***
 1. Input or procedure that triggers the vulnerability
 2. Exploitation of the vuln
 3. Effect of the exploit (return shell, return true/false)
- ***We'll release a template for the presentation by tomorrow***

26/10/16 Fabio Massacci - Offensive Technologies 2




UNIVERSITY OF TRENTO - Italy




Analysts

- **Prepare analysis for 4 exploits among the vulnerabilities you selected**
 - Choose whatever you prefer
 - We'll pick **only two** and ask you to present those
 - This will work as a "probe" for all the rest
 - Vote is a function of
 - Overall difficulty of selected exploits
 - You choose all tomcat/poc exploits? → vote will reflect that
 - Presentation quality
 - You do not understand either exploits we choose from the bunch? → 0/3

26/10/16 Fabio Massacci - Offensive Technologies 3




UNIVERSITY OF TRENTO - Italy




Analysts - presentation

- **The slide deck must have**
 1. First slide with a summary of the four exploits you selected
 - We'll choose the two exploits from this slide
 2. Detailed description of each of the four exploits
 - a. Language they're written in (C/Python/Input only/..)
 - b. Shellcode/binary exploit analysis if present
 - c. Procedure that triggers the vulnerability
 - Array that overflows the buffer, input string that triggers the parsing error, etc.
 - d. Procedure that generates the impact if any
 - Returns the shell, calls home/downloads malware
- **Access the exploits in the MalwareLab**

26/10/16 Fabio Massacci - Offensive Technologies 4




UNIVERSITY OF TRENTO - Italy




Technical track

- **Demo presentation of exploits (Selenium automation not required)**
- **Choose two Tomcat exploits to demo**
 - We'll select one
- **For each exploit, prepare two demos**
 - One for latest vulnerable version of tomcat
 - One for a previous version
- **Goal is to show that you understand the exploit functionality**
 - The demo sessions will be "interactive"
 - Not the equivalent of a video where you have a fixed setting and run that
 - We may ask for deviations or additional details on specific aspects

26/10/16 Fabio Massacci - Offensive Technologies 5



UNIVERSITY OF TRENTO - Italy



Technical track - presentation

- **Presentation must have**
 - First slide with summary of demo steps for the two chosen exploits
 - In this demo we'll first do A) then B) and finally C)
 - Slides of demo content (we'll use these to follow your demo)
 - Walk-through of the target environment
 - e.g., vulnerable software, version, pre-requisites, source code of the web page/app
 - Describe the success criterion of the exploitation
 - Attacker scenario
 - detailed steps that an attacker has to do to exploit the vulnerability;
 - Victim scenario/user interaction (if any)
 - detailed steps that a victim has to do to trigger the vulnerability;
 - Demo should be set up on a VM
 - Prepare starting snapshot to cut booting times etc.
 - Bring your own laptop + VGA adapter
 - If you don't have one please let us know now

26/10/16 Fabio Massacci - Offensive Technologies 6



Feedback sessions and material

- ***We'll have a free-to-join feedback session on the 2nd of November***
 - Remember the class on the 31st is cancelled
- ***All material should be uploaded to Google classroom by (will post announcement)***
 - 7th of November (Monday) at 8.00 am