Network Security Threats, Vulnerabilities, and Attacks

Module 02

Lab 1

Conducting Vulnerability Research

Vulnerability research plays an important role in current threat environment.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

The vulnerability research findings can serve to better protect information by knowing the flaws that could put sensitive information at risk of exposure. As a network administrator, you should be able to conduct vulnerability research to know possible vulnerabilities on network devices and applications from various vendors.

Lab Objectives

This lab demonstrates how to conduct vulnerability research on network devices and applications.

Lab Environment

To carry out this lab, you need:

- A virtual machine running Windows Server 2012
- A web browser with the Internet Connection
- In this lab we are using Chrome browser
- Screenshots might differ if you are using any other browser

Lab Duration

Time: 10 Minutes

Overview of the Lab

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

Lab Tasks

TASK 1

Conducting Vulnerability Research using NVD

1. Browse National Vulnerability Database (NVD) website https://nvd.nist.gov and click **Vulnerability Search Engine**

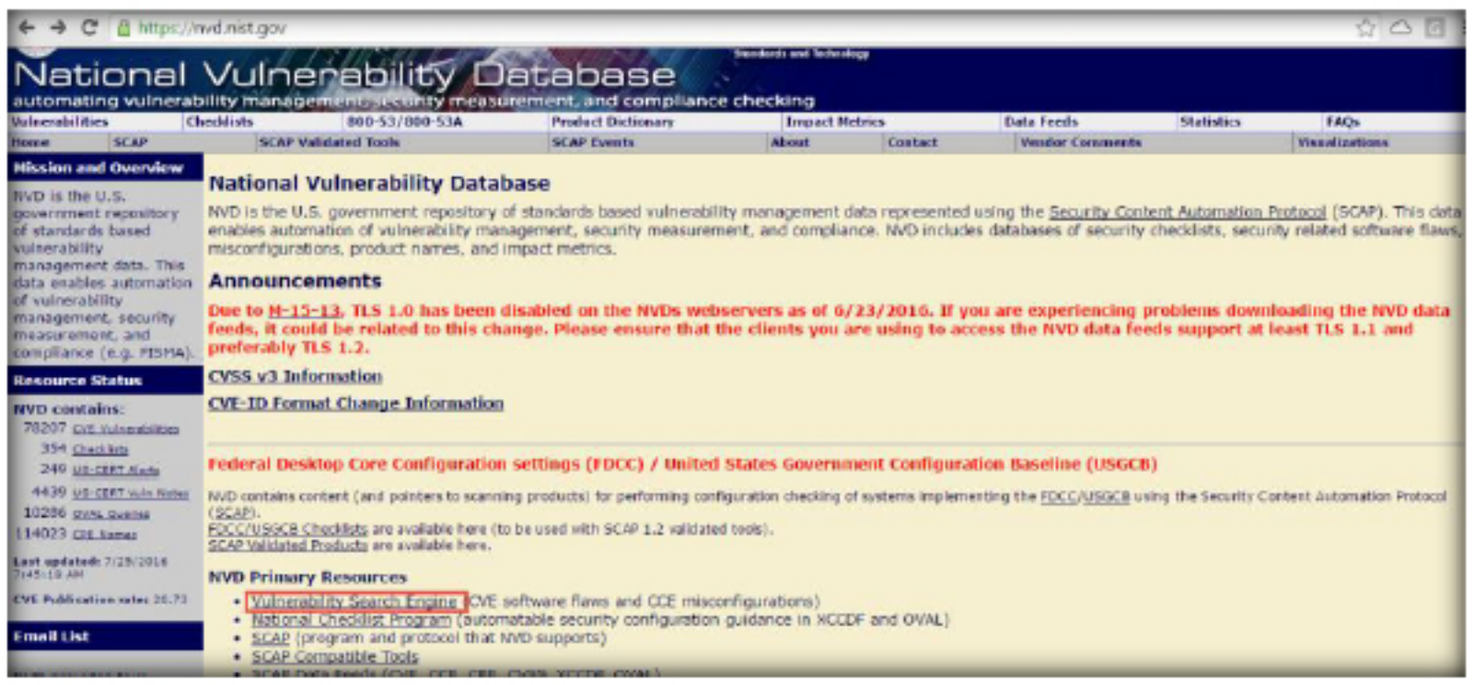


Figure 1.1: Browsing NVD website

NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics. NVD supports the Information Security Automation Program (ISAP).

2. Type the name of device against which you want to check the vulnerabilities and click **Search**. In this lab we are searching vulnerability for **cisco asa firewall**.

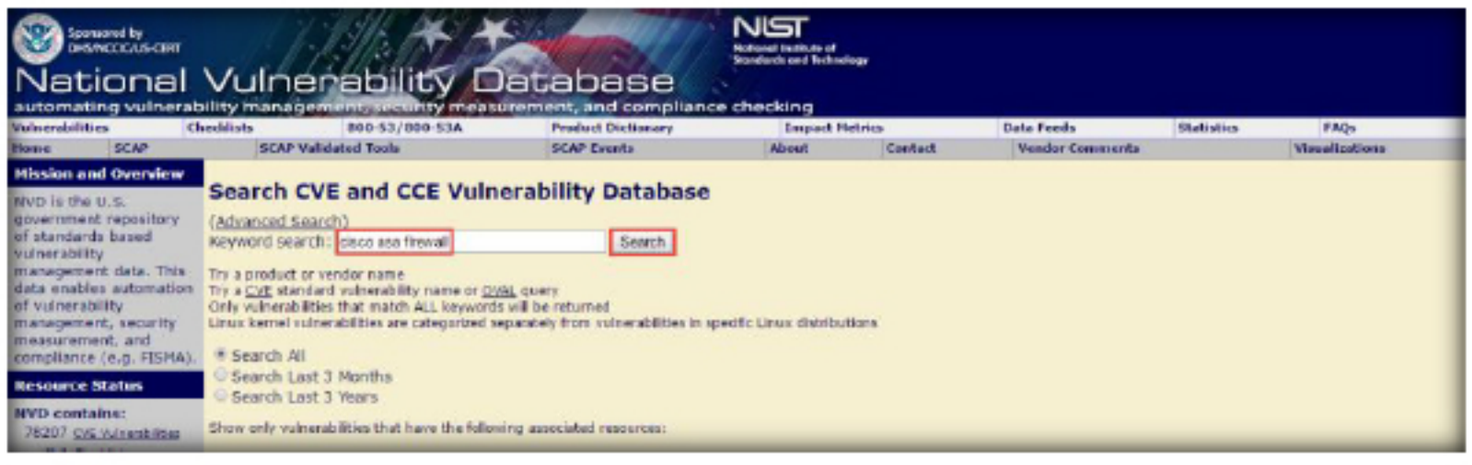


Figure 1.2: Checking for vulnerabilities

3. You will find that vulnerabilities exist across different variants of devices.

The National Vulnerability Database is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP).

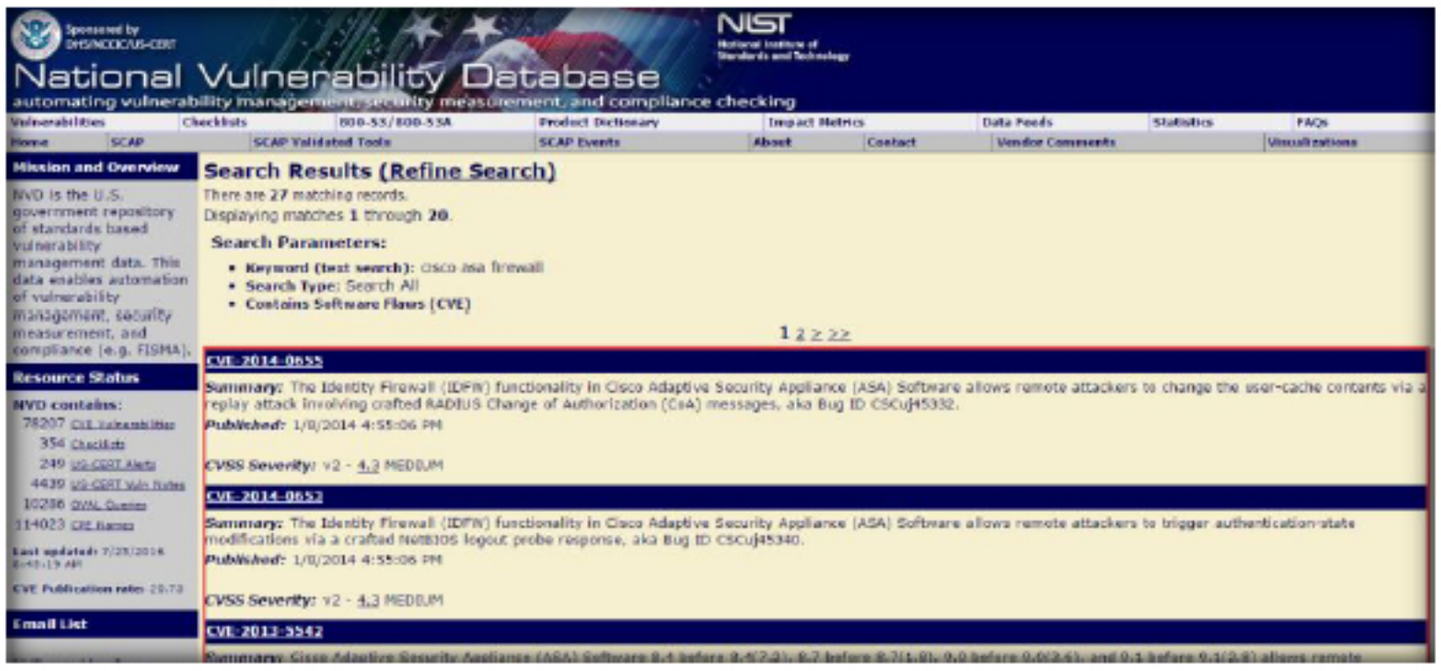


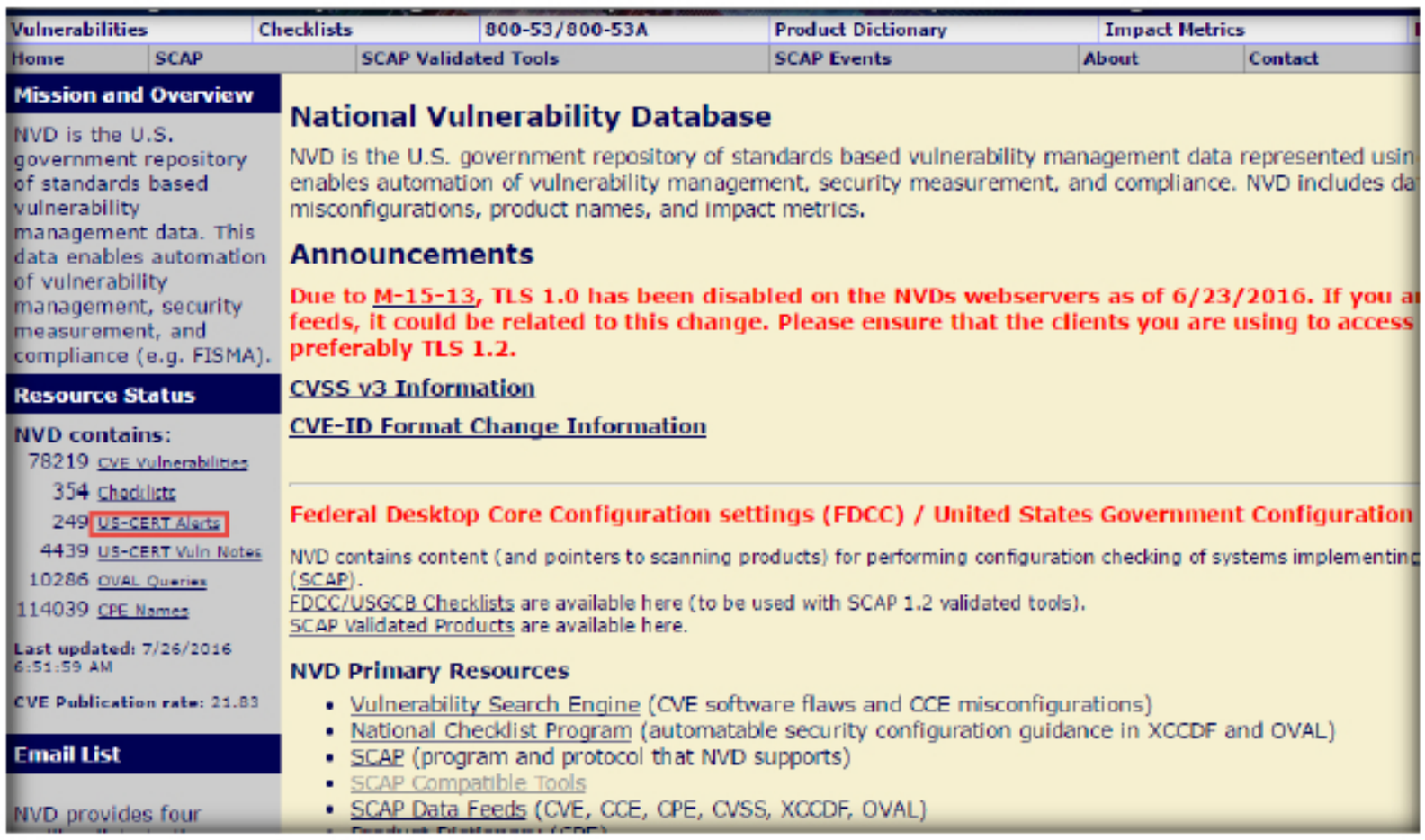
Figure 1.3: Vulnerabilities Explored

4. Click on **CVE Vulnerabilities** to know common vulnerabilities

Figure 1.4: Checking CVE Vulnerabilities

In addition to providing a list of Common Vulnerabilities and Exposures (CVEs), the NVD scores CVEs to quantify the risk of vulnerabilities, calculated from a set of equations based on metrics such as access complexity and availability of a remedy

5. Click on **US-CERT Alerts** to know current security issues, vulnerabilities, and exploits



The data enables automation of vulnerability management, security measurement, and compliance

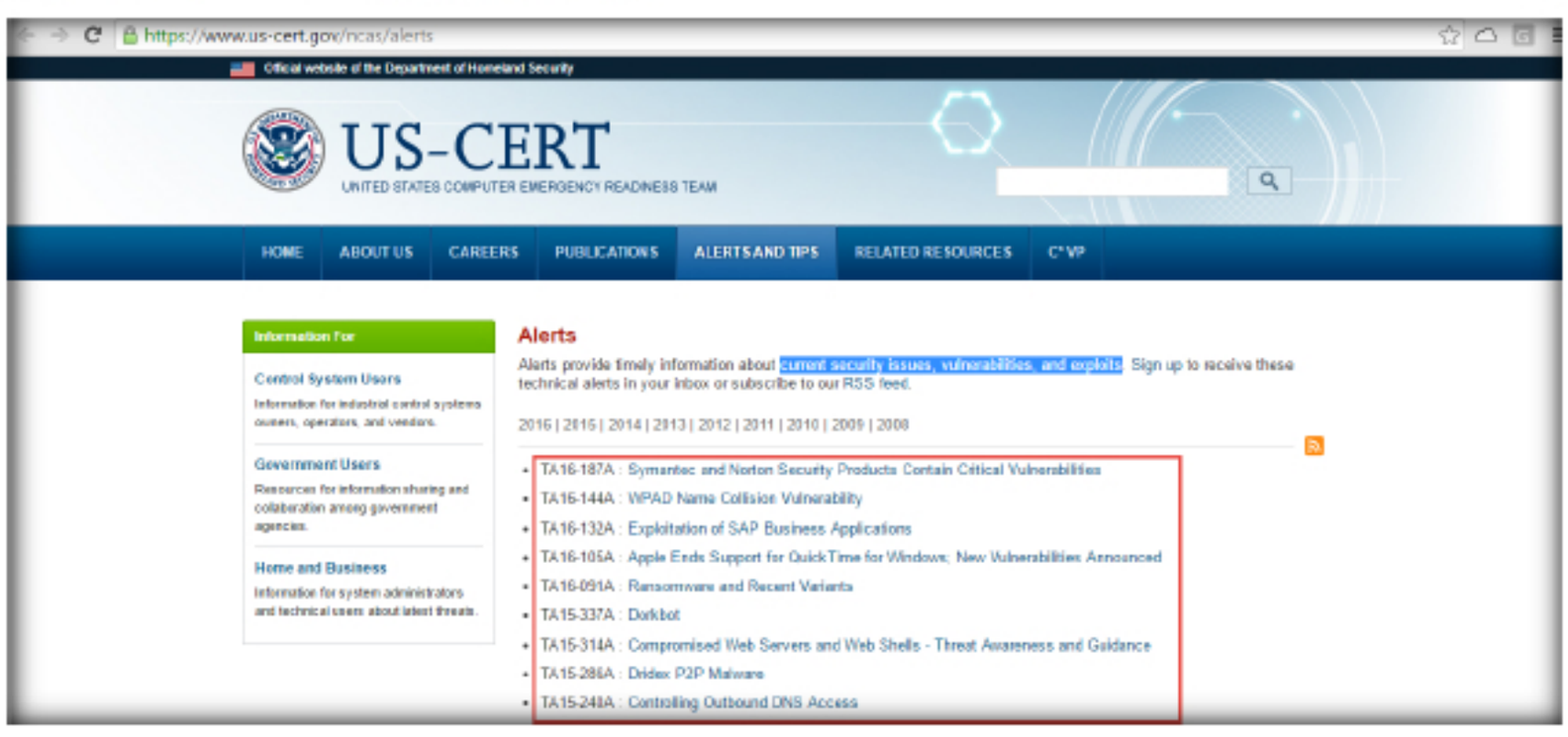


Figure 1.5: Checking US-CERT Alerts

TASK 2

Conducting Vulnerability Research using Securityfocus

6. Browse http://www.securityfocus.com . Research current security vulnerabilities of various technologies.

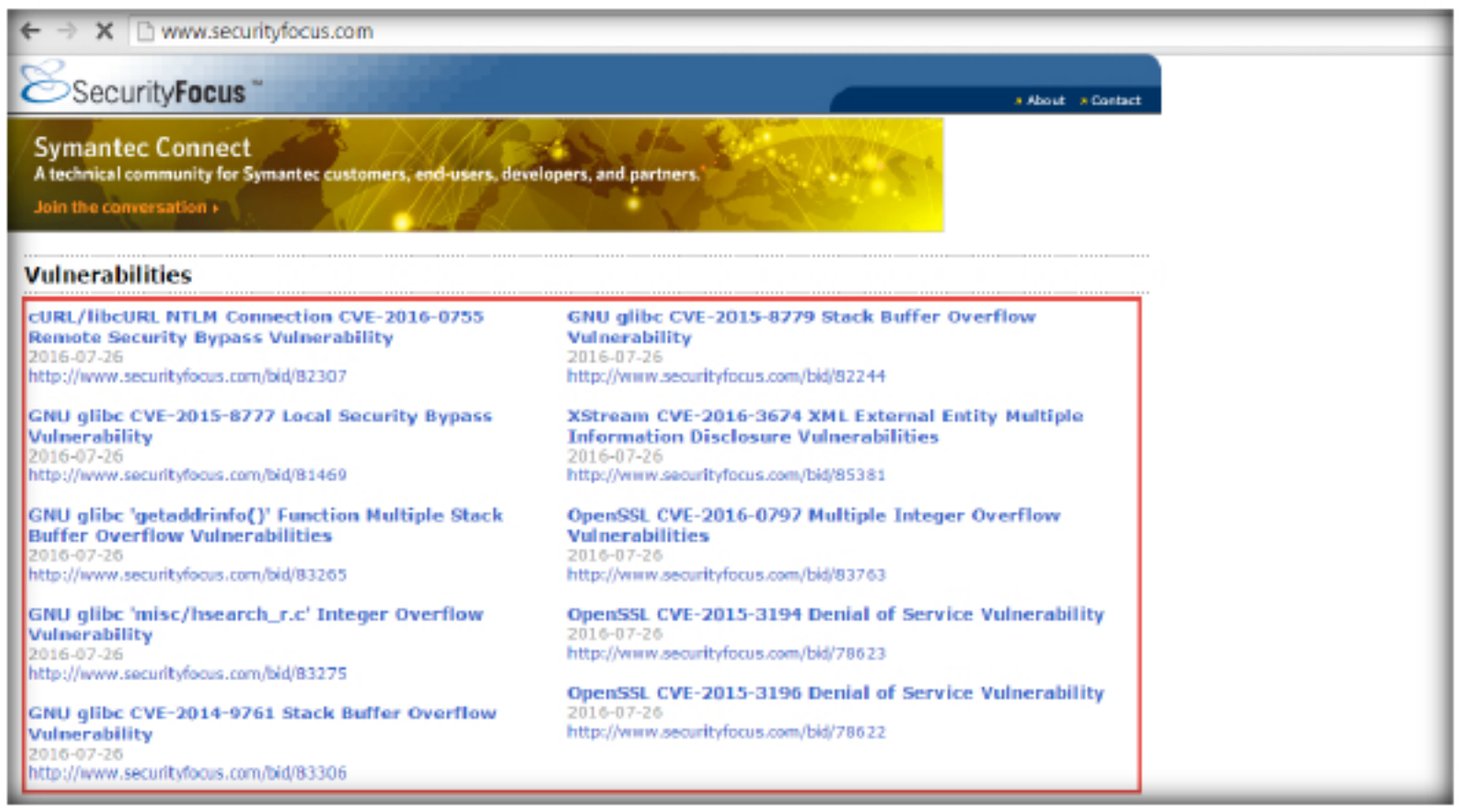


Figure 1.6: Browsing Securityfocus website for vulnerability research

TASK 3

Conducting Vulnerability Research using Zero Day

7. Browse Zero Day website http://www.zdnet.com to know the latest in software/hardware security research, vulnerabilities, threats and computer attacks.

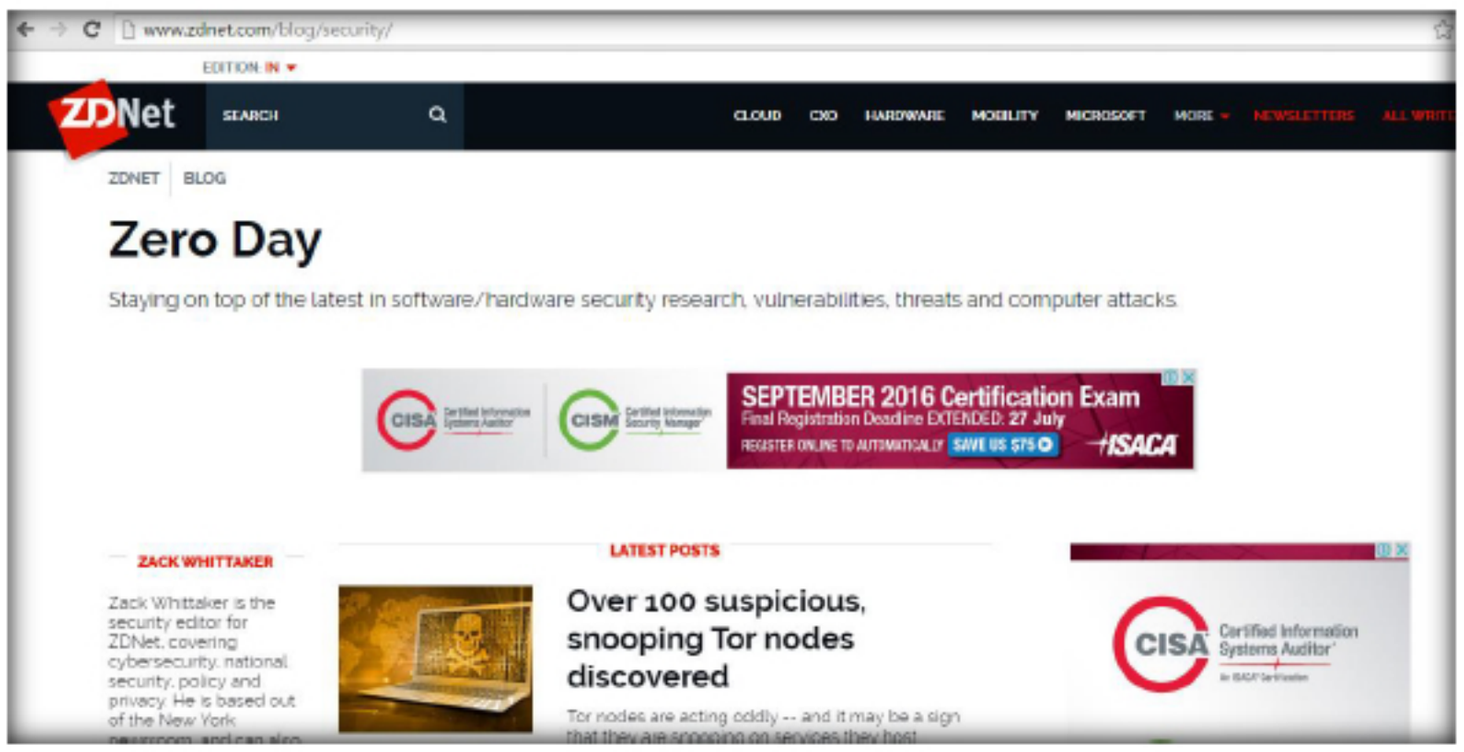


Figure 1.7: Browsing Zero day website for vulnerability research

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs