**Nwachukwu Edumanichukwu**

**CYBR 445 - Advanced Incident Detection and Response  
Module 2 Lab – Active Defense and Cyber Deception**

In this second lab, we will explore some free active defense and cyber deception tools that can help us improve our defenses and transition from a passive to active mindset. The tools we will be using are provided by Thinkst and Active Countermeasures/Black Hills Information Security. The tools we will explore are used to detect, attribute, and annoy/frustrate attackers. Unbelievably, these countermeasures can significantly slow or dissuade those who would attack your network. This includes red teams and penetration testers as well as real attackers.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

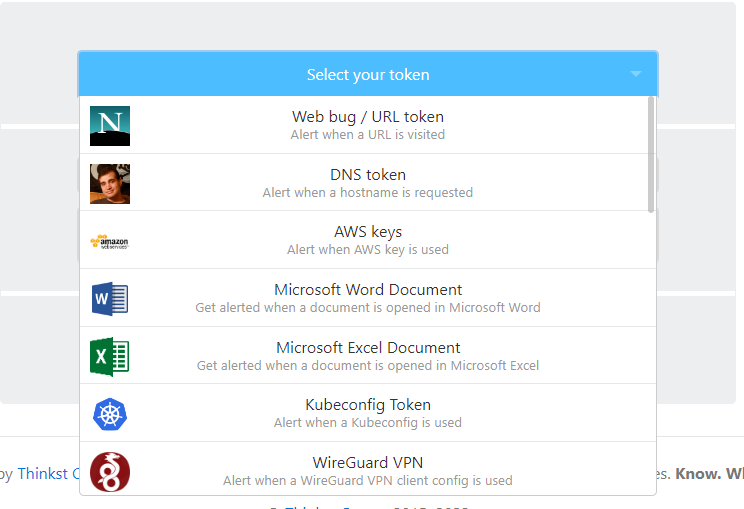
Accessing the Lab

This lab is hosted in the university's IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. You should use the native Horizon client when possible as it provides better performance. The web client can be accessed at <https://workspace.bellevue.edu>. Make sure you log into this interface with your Bellevue student ID and password.

Part 1 - Canary Tokens

Canary tokens are a type of honeypot that helps defenders detect an attacker by having the attacker announce their presence when performing actions that are typically considered benign or uninteresting. Think about it as setting up tripwires that normal users and admins should normally not trip in their normal day-to-day activities. For example, the canary tokens we will be exploring will alert the defender when a document is opened and give a geolocation and IP address of where the canary token was opened. This is an efficient way to detect breaches or intelligence gathering by attackers who have otherwise managed to evade your defenses or by malicious insiders.

1. Start by browsing to <https://canarytokens.org/generate>. Click on the drop-down name Select your token and read the several types of canary tokens available. Answer the following questions.

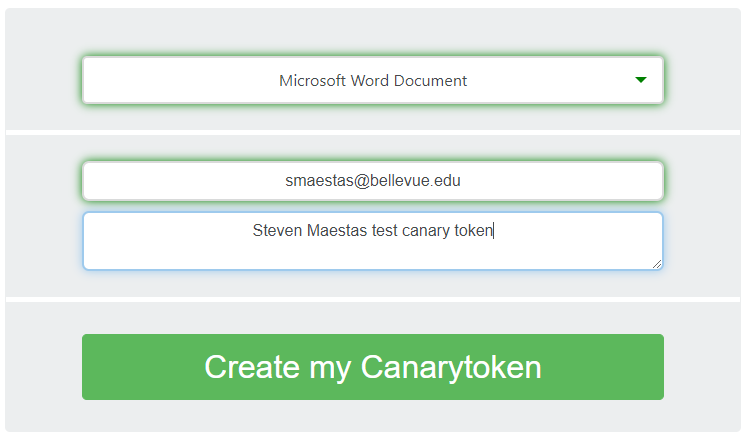


**How many different types of canary tokens are currently available?**

23

**Pick two different canary tokens (not Microsoft Word Document or Microsoft Excel Document). Explain how they could be used to set traps for attackers on an enterprise network.**

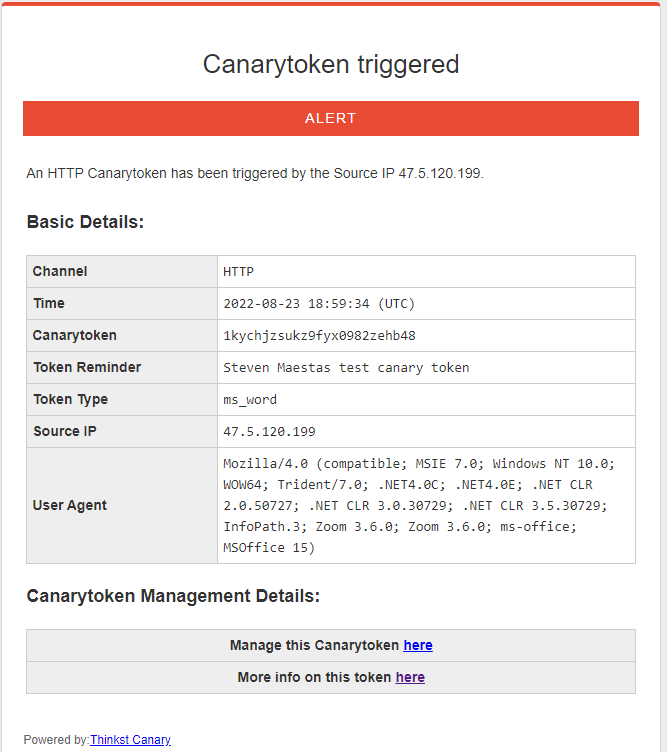
1. Microsoft SQL Server: This can be configured to look like valuable targets like financial or government databases. An attacker will be immediately detected, and their activities monitored once they tried to access the honeypot.
2. Cloned Website: A replica website created to look like the real website can be used to set traps for attackers on an enterprise network. This can be used to monitor suspicious activities such as multiple attempts to login in with incorrect credentials. This alerts the cybersecurity team to take actions to prevent the attacker from gaining access to the enterprise network.
3. Create a Microsoft Word canary by entering the following:
   1. Select your token: Microsoft Word Document
   2. Email Address: Your personal or Bellevue email address
   3. Reminder Note: Your Name test canary token



1. Click Create my Canarytoken and then Download your MS Word file.



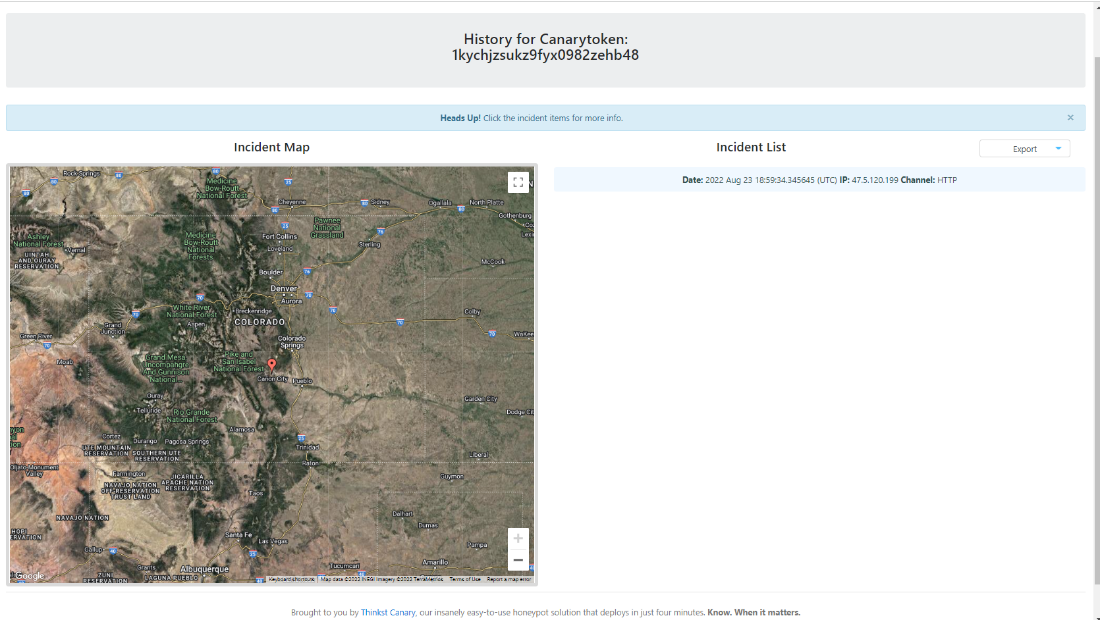
1. Open the MS Word file and click Enable Editing in MS Word. After a few minutes you should get an email from canary tokens showing an alert triggered. Below is an example. Make sure you check your junk mail if you don’t see the canary tokens email in your inbox. Paste a screenshot of the email you received below.



**Screenshot of canary tokens alert email.A screenshot of a computer

Description automatically generated with medium confidence**

1. In the email you received, click the More info on this token here link. You will be brought to another page that has a little more information on the IP addresses associated with the opening of the document, including a map with the geo location of the IP address. Examine the Incident Map and Incident List for that canary token. An example is shown below.



**Screenshot of canary tokens incident history page.A screenshot of a map

Description automatically generated with medium confidence**

1. Answer the following questions:

**Are you surprised at the amount of information available by the Word canary token? Why or why not?**

I’m surprised that it could detect my Ip address and was able to pinpoint a location as well.

**Where could the Word canary token be used to detect attackers?**

This could be used to detect attackers who are trying to gain access to a sensitive document.

**How could we change the default name and content of the canary token to make it more enticing for an attacker to open?**

The default name can be changed to upcoming stock exchange annual report to shareholders. It can contain a random annual report meant to appear like a tip which will serve as a factor whether to buy or sell the company’s stock.

Part 2 - Active Defense Harbinger Distribution

Active Defense Harbinger Distribution (ADHD) is a Linux security distribution that is like security-oriented Linux distributions. For example: Kali, Parrot, or Security Onion. The difference is that ADHD contains tools focused on providing active defense and cyber deception tools. We will be using this distribution for the second part of this lab.

1. From the IS Lab virtual machine desktop, open two Firefox windows and place them side to side. In each window, navigate to <https://10.98.100.11:4200>. Login in use the username analyst# and password An@lyst#!! where # is your student/analyst number.

Graphical user interface, application, Word

Description automatically generated

1. The first tool we will use is called portspoof. The directions for setting up portspoof can be found here: <https://adhdproject.github.io/#!Tools/Annoyance/Portspoof.md>. It is a tool that can slow down reconnaissance port scanning. In the right-hand terminal run the command ssh analyst#@172.28.37.91 and enter the password.

Graphical user interface, text, application, email

Description automatically generated

1. Run the command nmap –p 1-30 172.28.37.27 to scan ports 1-30 on your ADHD system. It should look similar to the picture below. If there are more results, run the command: sudo iptables –t nat –F then sudo pkill -9 portspooof to perform a clean in the left terminal window and repeat the nmap scan. This can happen if another student leaves portspoof running.

Graphical user interface, text, application, email

Description automatically generated

1. Now in the left-hand terminal run the following commands in order:
   1. sudo iptables –t nat –A PREROUTING –p tcp –m tcp –dport 1:30–j REDIRECT –to-ports 4444
   2. sudo portspoof –s /usr/local/etc/portspoof\_signatures

Graphical user interface, text, application, email

Description automatically generated

1. In the right-hand screen (in the Kali ssh terminal) type nmap –p 1-30 –sV 172.28.37.27 to run a nmap scan, this time showing the versions of services running on the spoofed ports, the results should be confusing and give back bad information.

Graphical user interface, application

Description automatically generated

1. Press CTRL+C in the left-hand terminal and then run the command: sudo iptables –t nat –F to clean up portspoof firewall rules. Then type clear to clean up the terminal window.

**Paste a screenshot of your nmap results with portspoof turned on below.A screenshot of a computer

Description automatically generated**

1. In the right hand screen exit your ssh session by typing exit, and then clear.
2. The next tool we will use is an SSH honeypot called Cowrie. Instructions similar to this lab can be found here: <https://adhdproject.github.io/#!Tools/Annoyance/Cowrie.md>. In the left window type the following commands.
   1. cd /opt/cowrie
   2. ./bin/cowrie start

Note: If you get an error regarding accessing the cowrie.pid file, it means another student has already started cowrie. Proceed to the next step ignoring the errors. Come back to this step if Cowrie stops working (is turned off by another student). You can also kill cowrie by typing sudo /opt/cowrie/bin/cowrie stop.

Graphical user interface, text, application, email

Description automatically generated

1. In the right terminal window, ssh into Cowrie using the following command:
   1. ssh –o HostKeyAlgorithms=+ssh-rsa root@localhost –p 2222
   2. Type in any password. The prompt should change to root@svr04
   3. Type in ls, then pwd, then exit. Notice that the prompt changes to root@localhost:~#. You are trapped in the ssh honeypot and any command typed will be captured in the cowire logs.

Graphical user interface, text, application

Description automatically generated

1. In the left window, run the command: more /opt/cowrie/var/log/cowrie/cowrie.log. Scroll to the bottom and find the logs with the CMD flag to review the commands you typed into the ssh honeypot.

Text

Description automatically generated

**Paste a screenshot of your Cowrie log below:A screenshot of a computer code

Description automatically generated with low confidence**

1. In the left window stop cowrie by typing the commands:
   1. cd /opt/cowrie
   2. sudo ./bin/cowrie stop

Graphical user interface, text, application, email

Description automatically generated

1. In the final step, we will examine a http tarpit. This is meant to confuse web spiders and vulnerability scanners. Instructions for using spidertrap can be found here: <https://adhdproject.github.io/#!Tools/Annoyance/Spidertrap.md>. In the left terminal window. Type the following commands:
   1. cd /opt/spidertrap
   2. python3 spidertrap.py

Graphical user interface, text, application, email

Description automatically generated

1. In the right window type the following command to spider the spidertrap.py webserver:
   1. nitko -host http://127.0.0.1:8000

Graphical user interface, text, application, email

Description automatically generated

1. Notice in the left window that all scanned paths are being returned as being valid URLs. You can see this by every path on the web server requested being returned with a 200 HTTP code.

Text

Description automatically generated

**Paste a screenshot of the spidertrap.py log file in the terminal similar to the screenshot shown above.**A picture containing text, screenshot, document, pattern

Description automatically generated

1. Perform the following steps to cleanup.
   1. Press CTRL+C in the left window to stop spidertrap.py
   2. Press CTRL+C in the right window to stop Nikto
   3. Close both windows
2. Answer the following questions:

**There are three types of active defense and cyber deception techniques, annoyance, attribution, and attack. For each of the four tools used in this lab, which tool matches up with which technique?**

**Canary Tokens: Attribution**

**Portspoof: Annoyance**

**Cowrie: Attack**

**Spidertrap: Annoyance**

**Give a brief description of how each of the tools examined in this lab could be used to slow down, detect, or identify attackers that evade other defenses.**

1. **Canary Tokens: This** is used as a tripwire to identify and possibly locate cybercriminals trying to gain access to sensitive information or an unauthorized attempt to access a system. It can be embedded in a file, URL, or used to monitor changes in a system behavior.

They can be used to identify the source of an attack which can be used to track down and hold attackers accountable for their actions. They can be used to improve security defenses such as early detection of an attack with gives the defense team an ample time to respond to the attacks and avoid significant damage.

1. **Portspoof:** This can be used to slow down a suspicious attacker by redirecting all traffic coming from the attacker’s Ip address to a honeypot. This method makes it more tedious for the attackers to mount any successful attack.
2. **Cowrie:** This tool can be used to identify, detect, and slow down attackers. It can be configured to make it difficult for attackers to establish connections. It can be configured to log all the activities of the attacker including all the commands they run, files accessed, and website visited.
3. **Spidertrap:** This tool helps to provide visibility into the network traffic and activities which helps to identify and reveal suspicious patterns in the network. Such suspicious patterns include botnet activities, DDoS attacks and SQL injection attacks.