**Lab Report**

**Lab Completed: Poison Ivy - Remote Access Trojan**

**Objective:** Complete the lab presented. Using your textbook, the written lab, and the hands-on activity, use the lab report to demonstrate understanding of the concept presented.

**Part 1: Lab Activity**

Directions: Complete the lab assigned in Netlab. Take 2 screenshots (or more) that demonstrate completion of the lab. Answer the following:

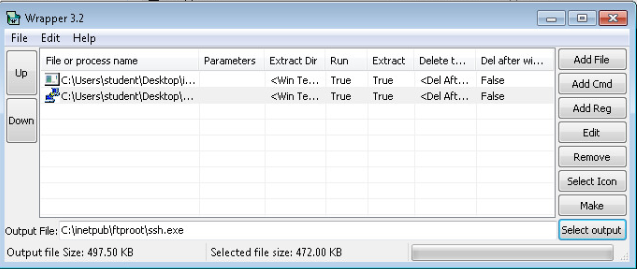
**Q1:** Provide a synthesis of the activity you completed in your own words.

In this lab we used the Poison Ivy RAT client to generate a server payload. We named this server payload in an inconspicuous way (iexplorer.exe) and then wrapped it with a common remote access client (putty) to give it legitimacy as a program.

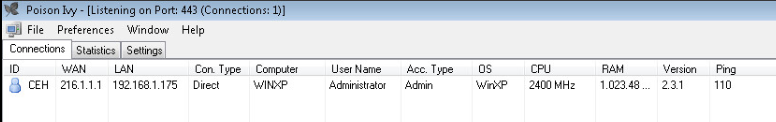
After the payload was generated and wrapped, we sent an email to an employee at XYZ Company under the guise that the program might be useful in their studies.

Upon executing the wrapped payload file their machine, which was on a LAN with a natted internal IP, established communication with our machine, giving us direct access to use and abuse their machine as we please.

**Q2:** Provide 2 screenshots that demonstrate lab completion. For each screenshot, include 1-2 sentences explaining what the screenshot is demonstrating.



In this step I had generated the Poison Ivy server payload and chose to wrap it in a single executable file that masqueraded as putty.



This is a screenshot of the Poison Ivy Client after I had sent an email to an employee at XYZ Company. They subsequently opened it which gave me a reverse shell on their machine.

**Part 2: Critical Thinking**

**Directions**: Complete the following questions. Provide an explanation of your reasoning for each answer.

The answers should address the lab you just completed.

Suggested length for Part 2: 1-2 pages

**Q1**: What vulnerability(s) are demonstrated or found in this lab? Vulnerabilities may occur during the lab as part of the lab activity.

Well, to start, there is a very obvious human vulnerability. The fact that an employee chose to download and execute a program hosted on an unknown remote ftp server is a pretty glaring vulnerability.

The security policy on their device allowed them to download and execute this program that was not signed by a trusted publisher.

Whatever virus scanning software is installed on the XP machine did not pick up the wrapped malicious server payload.

**Q2:** How might this (these) attack(s) be utilized during a penetration test?

There are so many ways that one might utilize Poison Ivy during a pentest, so I am only going to list a few below:

- Scrape password hashes and run any number of tools against them to (hopefully) decrypt them

- Scrape stored wireless passwords and hopefully score some information that will allow you to put a foot in the door of the network you are targeting

- Run active and passive reconnaissance from a machine on the LAN, possibly even a machine that has access to sensitive parts of the domain.

**Q3:** Explain your reasoning as to what phase of the attacker methodology this lab falls under.

I would say this falls both in the “infiltration and escalation” and “exfiltration” categories. We are exploiting an identified vulnerability to gain access to a resource, and then we are accessing protected resources and data (e.g. hashed passwords).

**Q4:** Research how the attack(s) in this lab can be mitigated or prevented. Cite any sources used. (APA)

First, you could conduct employee security training. This employee obviously should not have downloaded and run this program, and a solid security education program for employees would help prevent things like this from happening in the future.

The company could also deploy an intrusion detection and prevention system such as OSSEC or Snort that could be configured to notice and shutdown anomalies like outbound traffic on port 80/port 443 that is not http/https traffic.

The company should probably implement some sort of security policy in Windows that does not allow download and/or installation of unsigned executables.

**Q5:** What ethical or potentially problematic issues should a penetration tester consider if they plan on implementing this (these) attack(s) by exploiting a vulnerability?

Is this employee part of the scope of this pentest? Could this reverse shell create outbound traffic that might be of interest to someone targeting the company with malicious intent? Which processes and services can I safely kill to accomplish my end goal without causing actual harm to this companies assets?