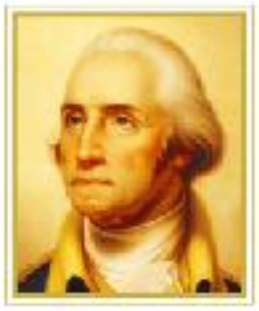


THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

Computer Science 6907-13
Computer Network Defense

CTF #3

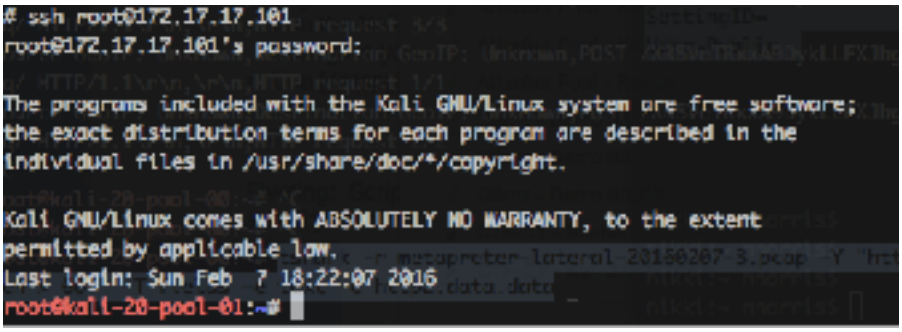
Kevin Yasuda
Matthew Norris

Attacking a network

Setup

To connect to the Kali attacker pool, you will need to follow the instructions below:

- First connect to the GW network via the Cisco VPN client
  - Further instructions can be viewed here: http://it.gwu.edu/vpn
- Once you have connected to the GW network, you can connect to the bastion host located on class network. You will need to open an SSH session to port 52525 on class.tiwaz.net. Credentials are provided on blackboard.
- Once connected to the bastion host, you can connect to a Kali attacker box. Work with your classmates to choose a unique Kali host (or select the host number that you used last week). The Kali hosts are all located in the range 172.17.17.201-210.



- Once connected to your Kali attacker box, you can connect to the victim/target network. The general network architecture is the same as the previous CTF, except with new hosts and a new network - hidden behind some pre-existing hosts.

- In this exercise, the targets are available on the 192.168.91.0/24, 192.168.92.0/24, and 192.168.93.0/24 networks. There are multiple different targets on this network running various Windows operating systems. You may use one remote service exploit to connect through the network, all of the rest of your compromises must use credential/lateral style attacks.

Requirements

You must submit the following:

- Screenshots that show the critical steps that you followed

    - You do not need to show every step - just the steps that are required to tell the story of your compromise
- A description of:
    - Why you chose the steps you did
    - The methodology that you followed to identify and spread across the network
    - Lessons learned during the process
- You must demonstrate the following access:
        - Using pass the hash to connect to the domain controller
        - Obtaining the krbtgt hash and using it to generate a golden ticket
        - Discovery of 192.168.93.0/24 network and using pass the hash to connect to a host within it
        - Obtaining ‘sensitive corporate documents’ from two of the new hosts - a file server and the Widgeteer workstation
            - These files are actually image files, but are named as though they were corporate documents
- You may also create and provide a pcap of your traffic. Hint command: pcap -w ….