Computer Science 6907-10
Computer Network Defense

Capture The Flag #2

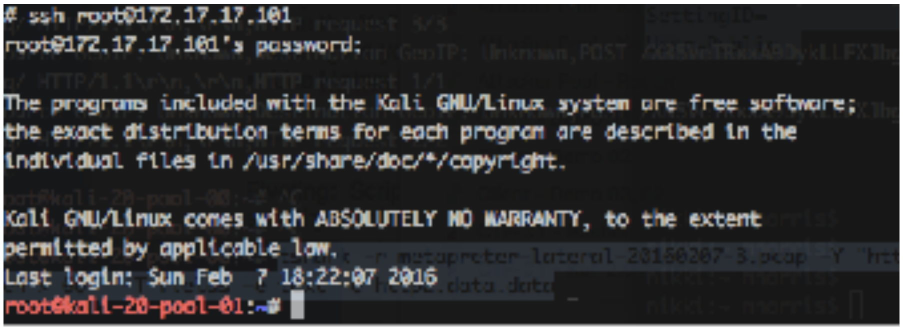
Kevin Yasuda
Matthew Norris

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 as you did in the first capture the flag exercise.

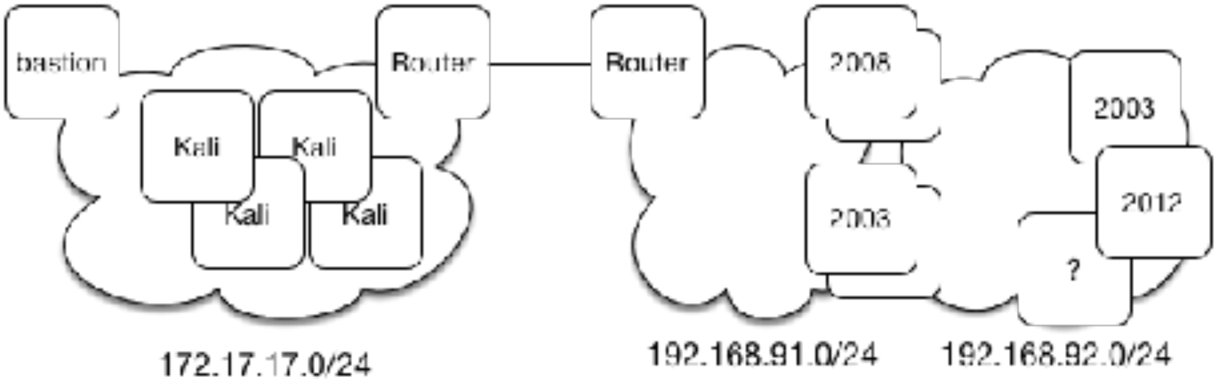


```
# ssh root@172.17.17.101
root@172.17.17.101's password:

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb  7 18:22:07 2016
root@kali-20-pool-01:~#
```

- Once connected to your Kali attacker box, you can connect to the victim/target network. The general network architecture is as follows:



- In this exercise, the targets are available on the 192.168.91.0/24 and 192.168.92.0/24 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:
  - Proof of remote compromise through the use of a Windows remote exploit (e.g. the netapi one demonstrated in class)
  - Proof of hash retrieval
  - Proof of pass the hash to connect into a host on the 192.168.92.0/24 network (through metasploit using a meterpreter payload)
- You may also create and provide a pcap of your traffic. Hint command: pcap -w ….
  - If you choose a plaintext protocol in Metasploit, it will provide a much more interesting pcap for later review.

Stretch Goal

If you are creative, you can also connect into the Windows Domain Controller. Once there, you should try to generate a Golden Ticket. This will allow you to connect to any other Windows domain member on the network. This technique will prove very helpful for the next exercise and will earn you extra credit on this one. To prove that you have done it:

- Screenshots that show the critical steps that you followed
- The network/compromise path that you used to get to that host
- A dump of the krbtgt hashes