Hands-on session 1: Collecting Information with Spyware: Screen Captures and Keyloggers

Elie Kfoury
University of South Carolina (USC)
https://research.cec.sc.edu/cyberinfra

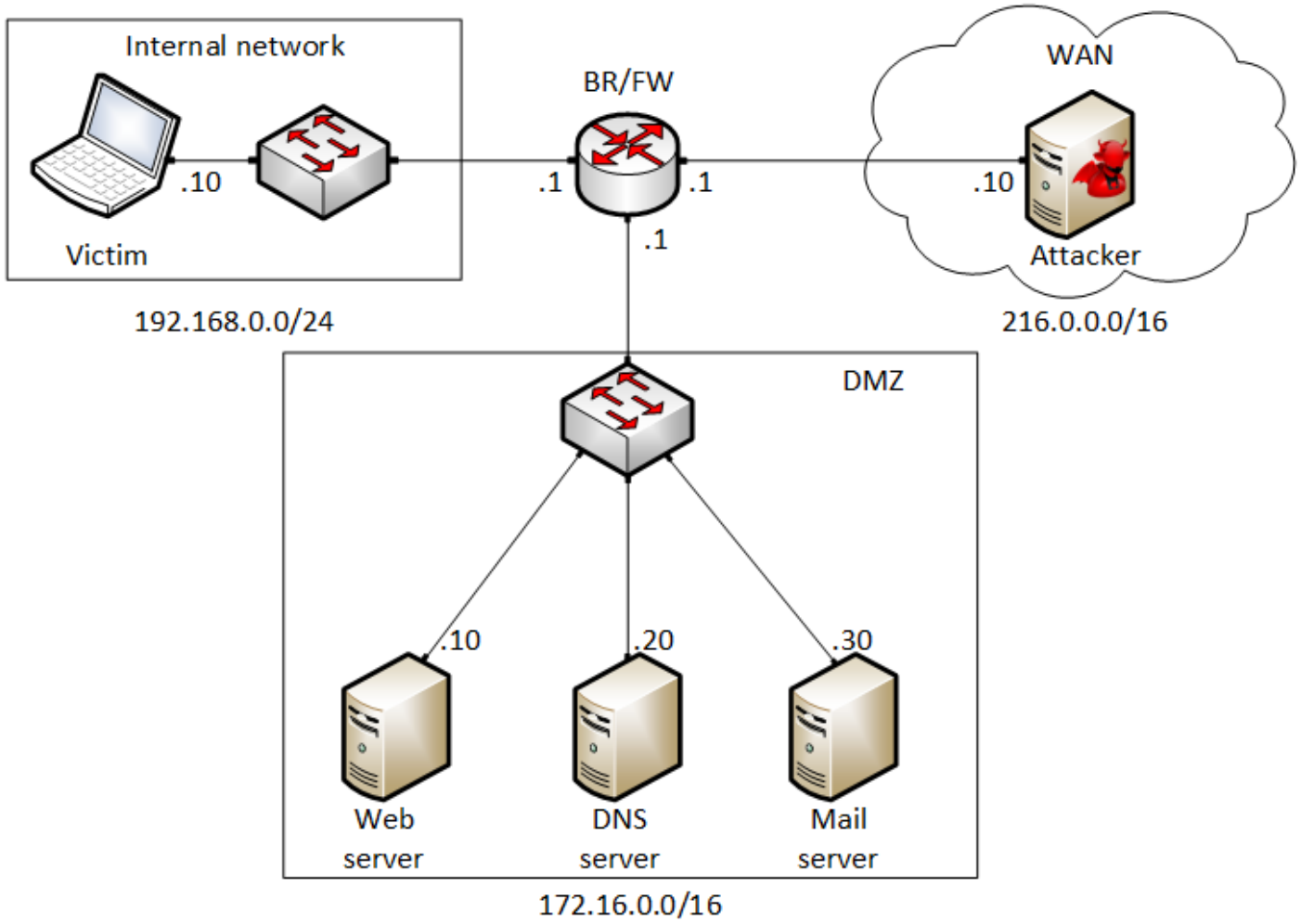
University of South Carolina (USC)
Minority Serving - Cyberinfrastructure Consortium (MS-CC)

Hands-On P4-DPDK Workshop
Friday, May 30, 2025.

Lab 4: Collecting Information with Spyware: Screen Captures and Keyloggers

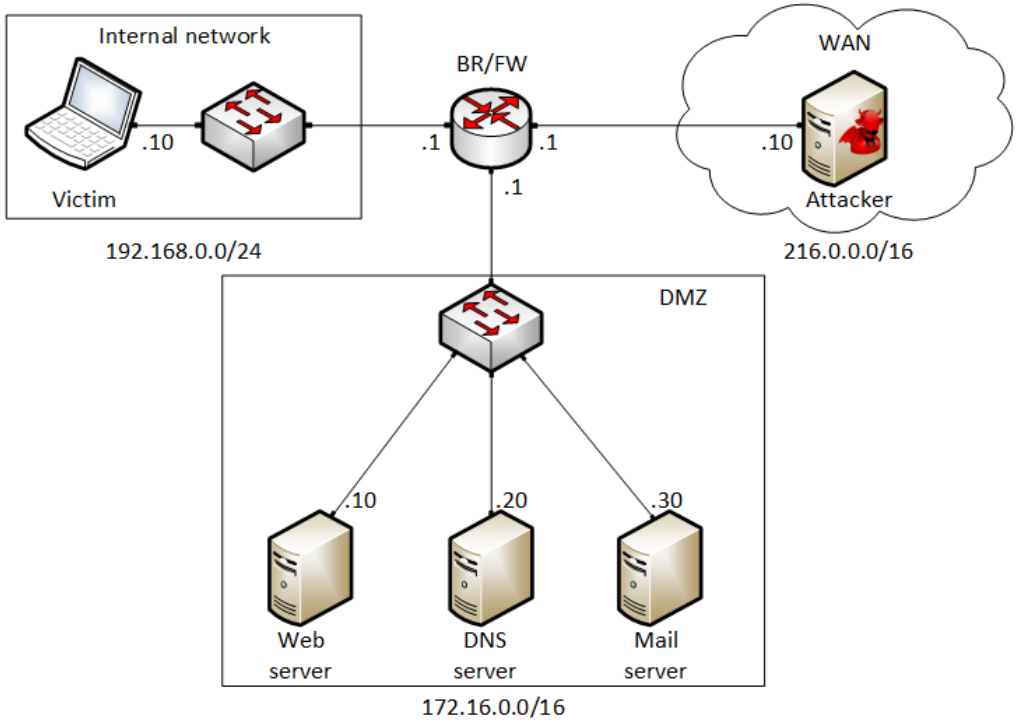
Lab Topology

- Attacker in the WAN running Kali
- Victim in the internal network running Windows 10
- Web, DNS, and Mail servers in the DMZ zone
- Border router interconnect the networks
- Border router implements basic security policy:
  - Attacker cannot initiate connections to devices in the internal network



Spyware Scenario

1. The attacker creates a “payload” and attaches it to a valid program (for example, “putty.exe”)
2. The attacker uploads the program to his website
3. The attacker starts the “command and control server,” listening to incoming connection
4. The victim downloads the program
5. The victim executes the program
   a) The program starts
   b) At the same time, the malware connects to the attacker
6. The attacker starts the spyware
   a) Takes screen captures of the victim’s computer
   b) Transmits the view of the victim’s computer in real time
   c) Controls the victim’s computer
   d) Monitors the victim’s camera
   e) Monitors the victim’s microphone
   f) Records the keystrokes…



Platform Information

We will use the NETLAB virtual platform:

- **URL:** https://netlab.cec.sc.edu/
- **Username:** your_email_address
- **Temporary Password:** nsf-2025