Cybersecurity (Security+) and P4 Programmable Switches

Lab 5: Social Engineering Attack: Credentials Harvesting and Remote Access through Phishing Emails

Elie Kfoury, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

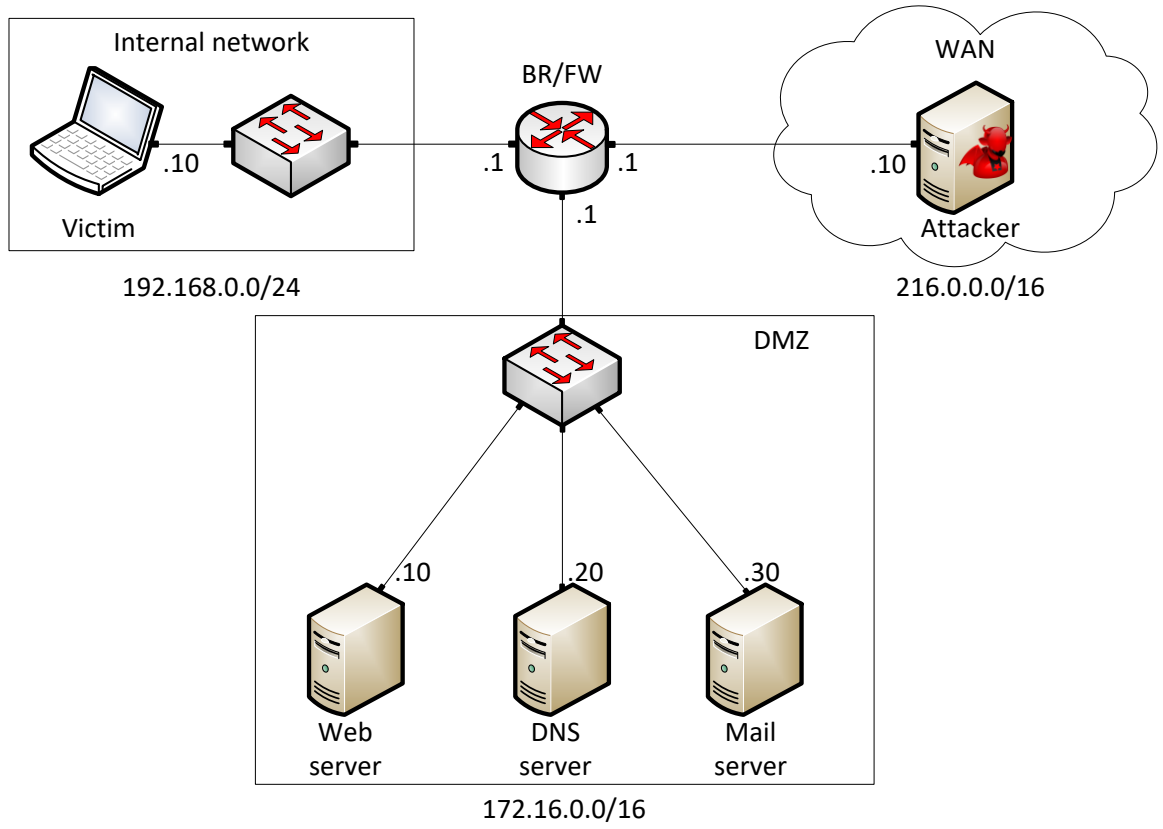
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 20th, 2023

Lab 5: Social Engineering Attack: Credentials Harvesting and Remote Access through Phishing Emails

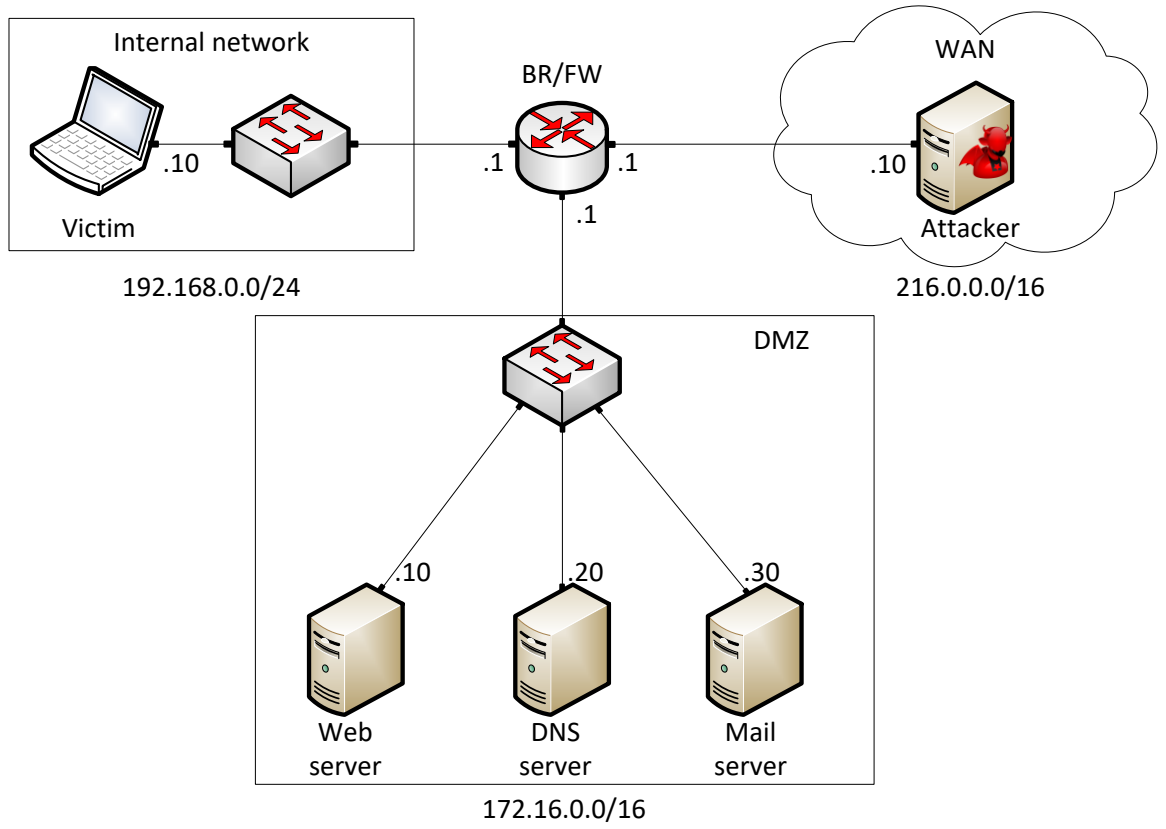
Topology

- The topology consists of:
  - Internal network: victim's machine
  - Wide Area Network (WAN): attacker's machine
  - Demilitarized zone (DMZ): three servers
  - Border router interconnecting the networks
- Internal can reach WAN and DMZ
- WAN can reach DMZ but not Internal
- All devices are Linux-based except the victim's machine (Windows 10)



Lab Objectives

- Part 1: perform credentials harvesting attack
  - The attacker clones Gmail's webpage
  - The attacker creates an email containing the URL of the server hosting the fake webpage
  - The email is sent to the victim
  - The victim logins by providing the credentials
  - The credentials are transmitted to the attacker



Lab Objectives

- Part 2: perform reverse shell attack
  - The attacker generates a malicious payload
  - The attacker creates an email containing the malicious file as attachment
  - The email is sent to the victim
  - The victim downloads and executes the payload
  - A reverse shell is opened allowing the attacker to execute arbitrary commands