Cybersecurity (Security+) and P4 Programmable Switches

Lab 1: Reconnaissance: Scanning with NMAP, Vulnerability Assessment with OpenVAS

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 19th, 2023

Reconnaissance

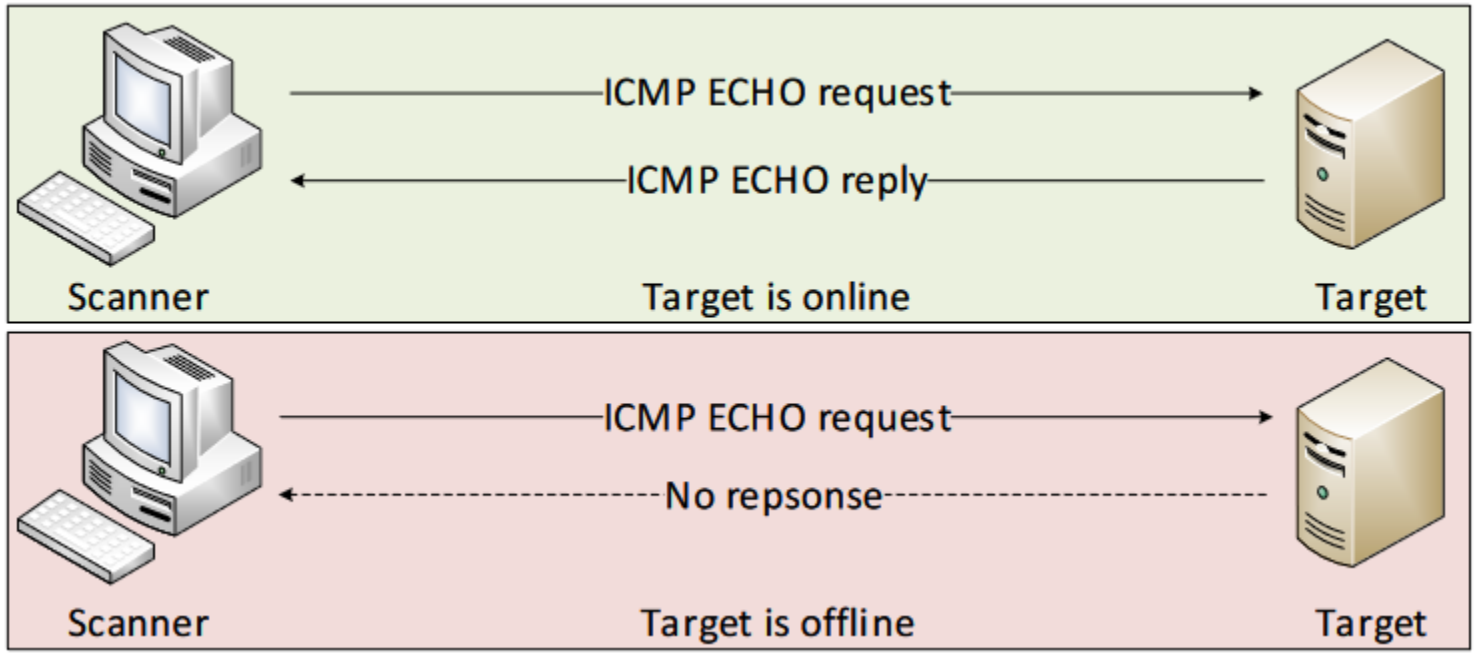
- Reconnaissance is the first step in a cyber attack
- It allows gathering information about targets
- Two methods by which reconnaissance can be performed:
  - Active reconnaissance: sending probes to the target
  - Passive reconnaissance: no interaction with the target
- Reconnaissance can be used by white hat hackers or black hat hackers

Active Reconnaissance

- By sending probes, information about a target server can be gathered:
  - **Host discovery**: determine the IP addresses of targets
  - **Port scanning**: determine the services running on targets
  - **Service version detection**: determine the version of the services running on targets
  - **OS fingerprinting**: determine the operating system used by the target

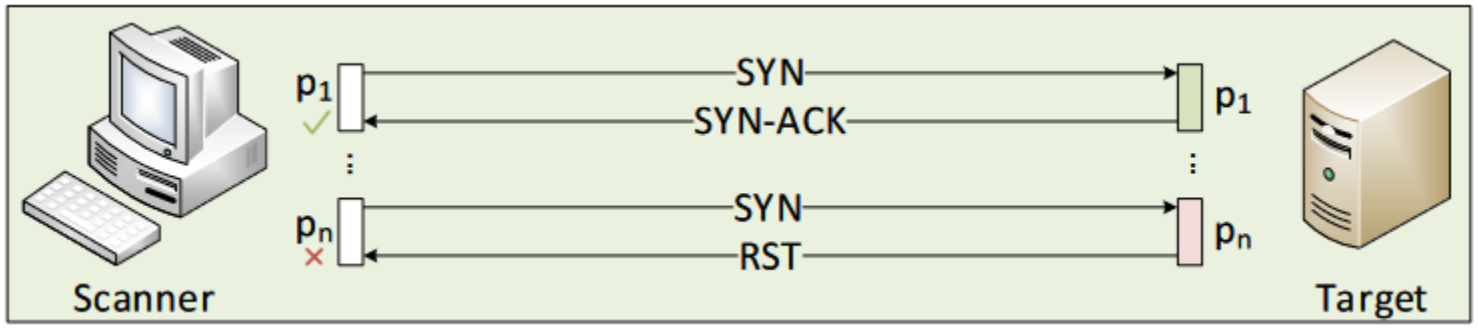
Host Discovery

- Ping sweep (most common):
  - ICMP *echo request* messages are sent to IPs in a certain network
  - Hosts that are online will reply with an ICMP *echo reply*
- Other techniques include TCP sweep, UDP sweep



Port Scanning

- The Internet Assigned Numbers Authority (IANA) assigns TCP/UDP port numbers to well-known protocols
- Knowing the port would allow determining the service running on that port
- Techniques include TCP SYN scan, TCP Connect scan, UDP scan, etc.



Service Version Detection

- Knowing the port number does not guarantee the type of service running on a server (services can be started on different ports)
- Version detection involves sending probes and parsing the responses
- The parsed response is matched against a list of expressions in the database
- Detect the protocol (e.g., HTTP), the application name (e.g., Apache HTTP server), the version number, the device type (e.g., router)

```
match telnet m|^\xff\xfb\x01\xff\xfb\x03\xff\xfc\"\r\n\r\n\n\rauthentication failed!\n\rpassword: | p/Effekta MH 6000 UPS telnetd/ d/power-device/
match telnet m|^\xff\xfc\"\xff\xfb\x01\r\nPassword: \r\nbad password\r\n| p|Campbell Scientific NL-100/105 Ethernet-to-serial bridge telnetd| d/bridge/
match telnet m|^\xff\xfb\x03\xff\xfd\x03\xff\xfb\x01\r\nUsername: \r\nPassword: \r\nAccess Denied\r\n| p/InterSystems CTELNETD/
```

nmap-service-probes database[1]

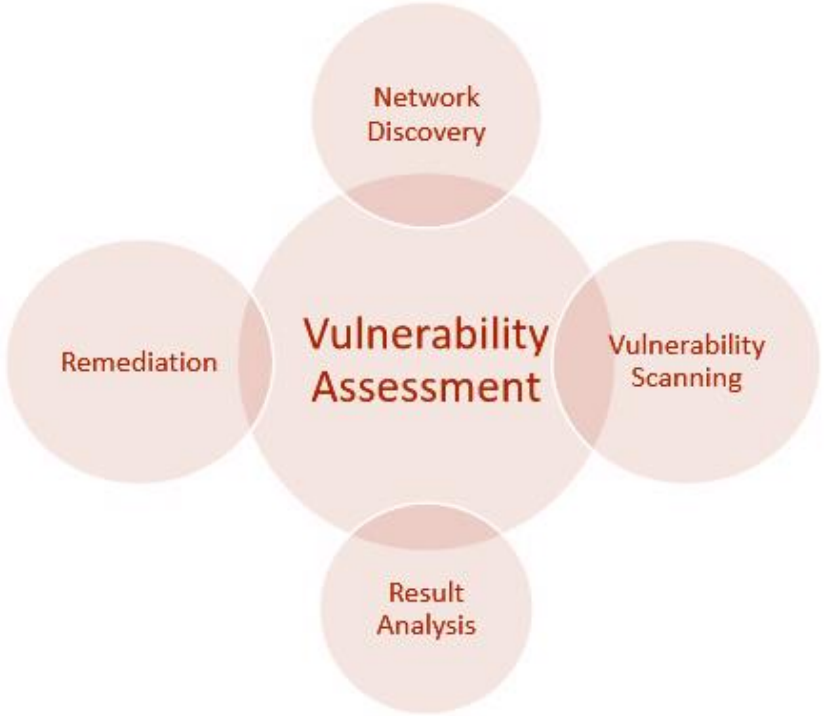
[1] https://svn.nmap.org/nmap/nmap-service-probes

OS Fingerprinting

- Scanners can identify the OS running on a target host by fingerprinting the TCP/IP stack
- The scanner performs tests on the responses and compares these values against a database containing the OS fingerprints
- E.g., examining the TCP options, the initial window size, etc.

Vulnerability Assessment

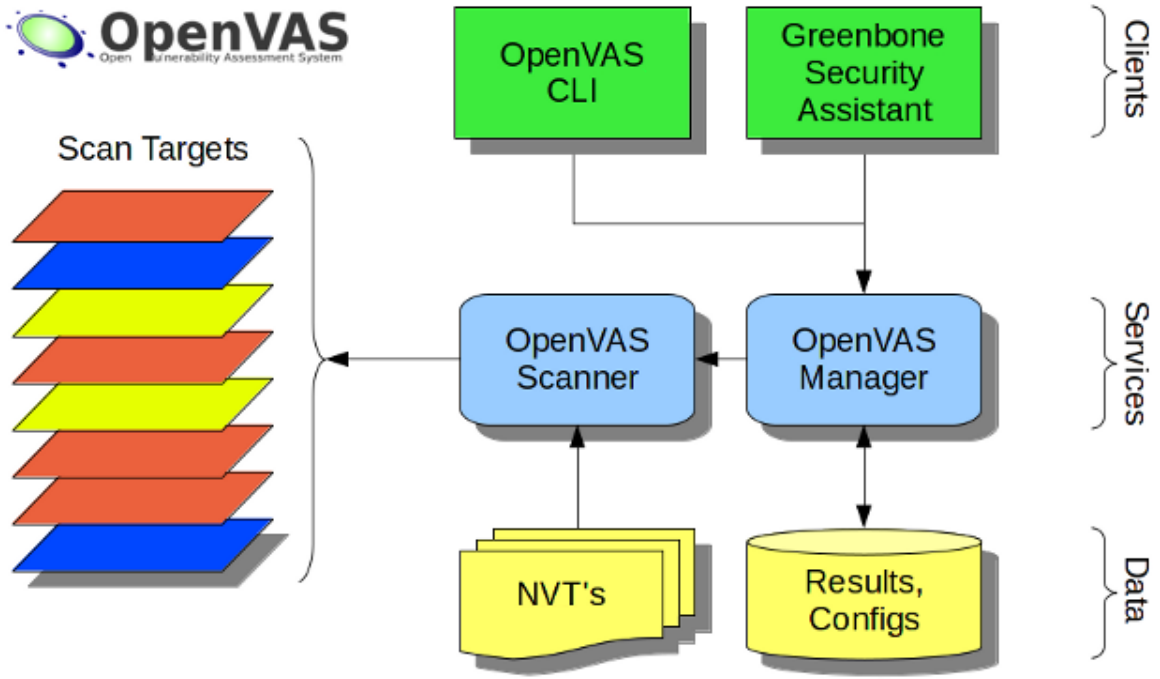
- Vulnerability assessment uses automated software to search for weaknesses (vulnerabilities) in a system
- It produces a report that can be used to remediate the vulnerability
- It identifies the vulnerabilities by consulting a database such as the Common Vulnerabilities and Exposures (CVE)[1]



[1] https://cve.mitre.org/

OpenVAS

- OpenVAS is an open-source vulnerability assessment software[1]
- The scanner obtains the tests for detecting vulnerabilities from a feed with daily updates
- The tests are known as Network Vulnerability Tests (NVTs)

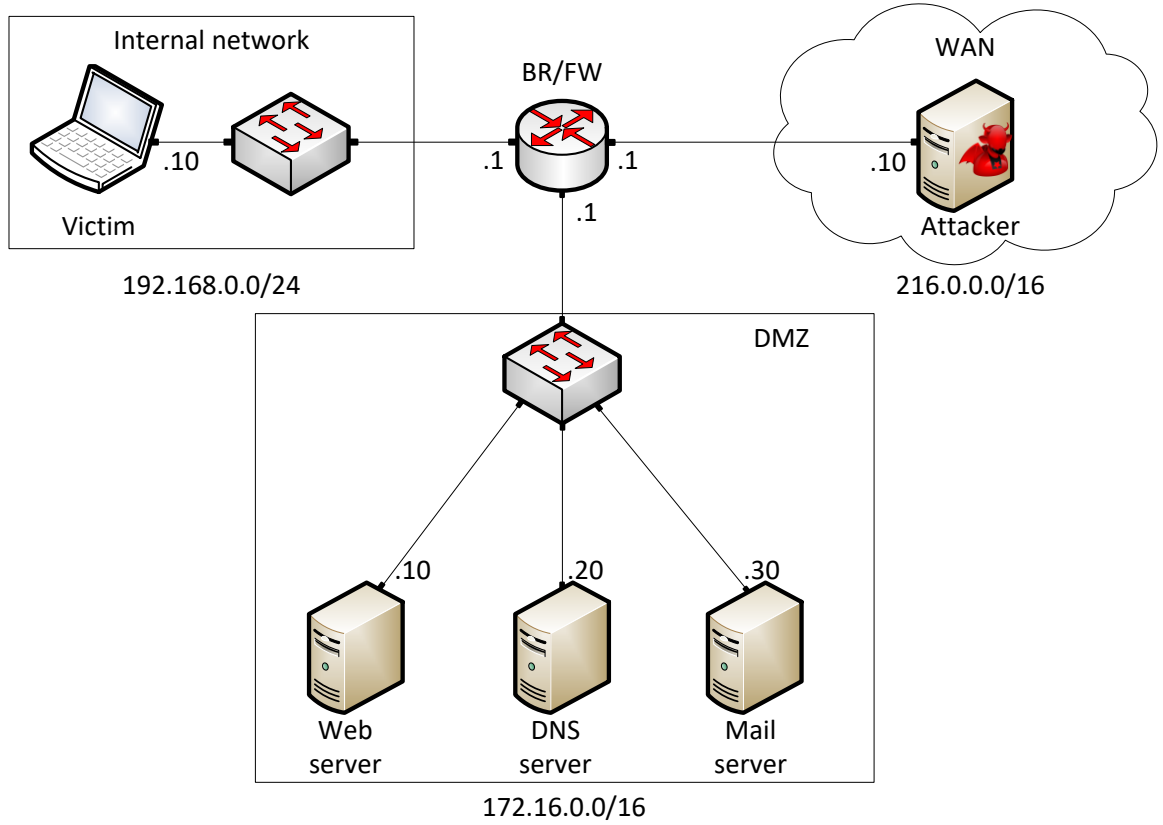


[1] https://openvas.org/

Lab 1: Reconnaissance: Scanning with NMAP, Vulnerability Assessment with OpenVAS

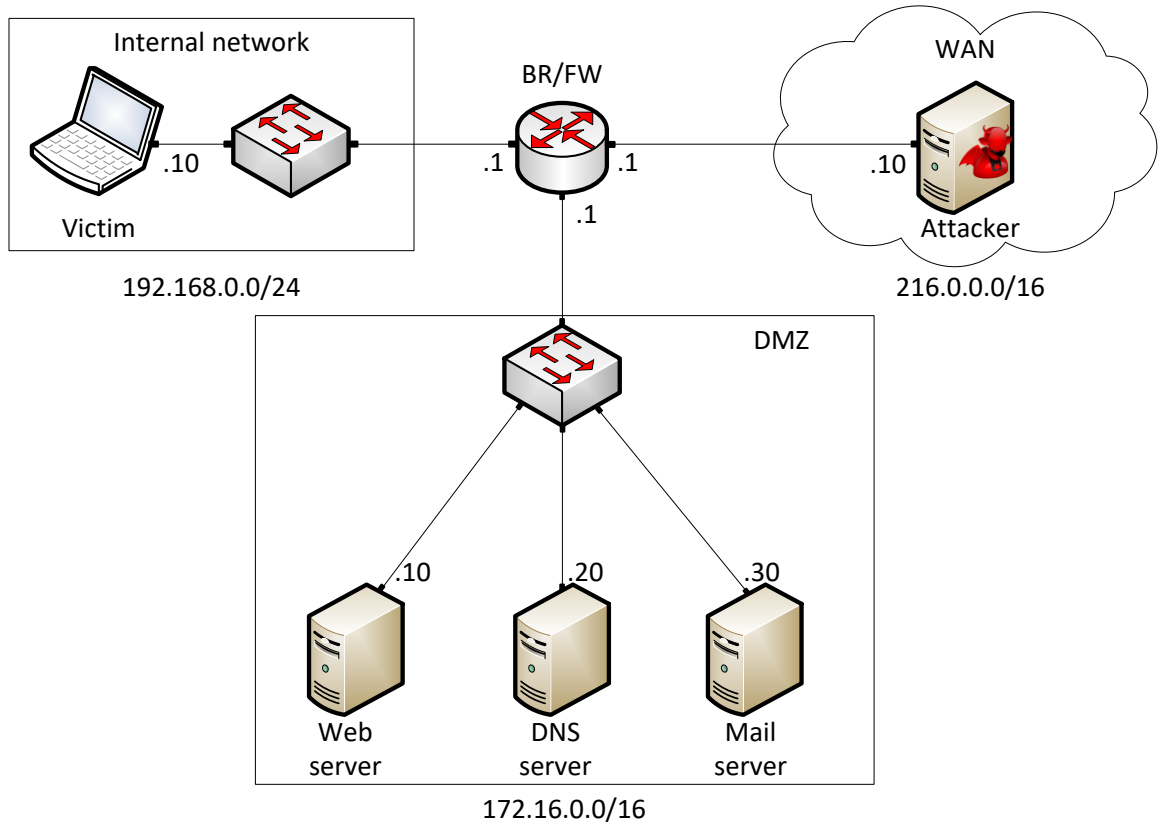
Topology

- 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)



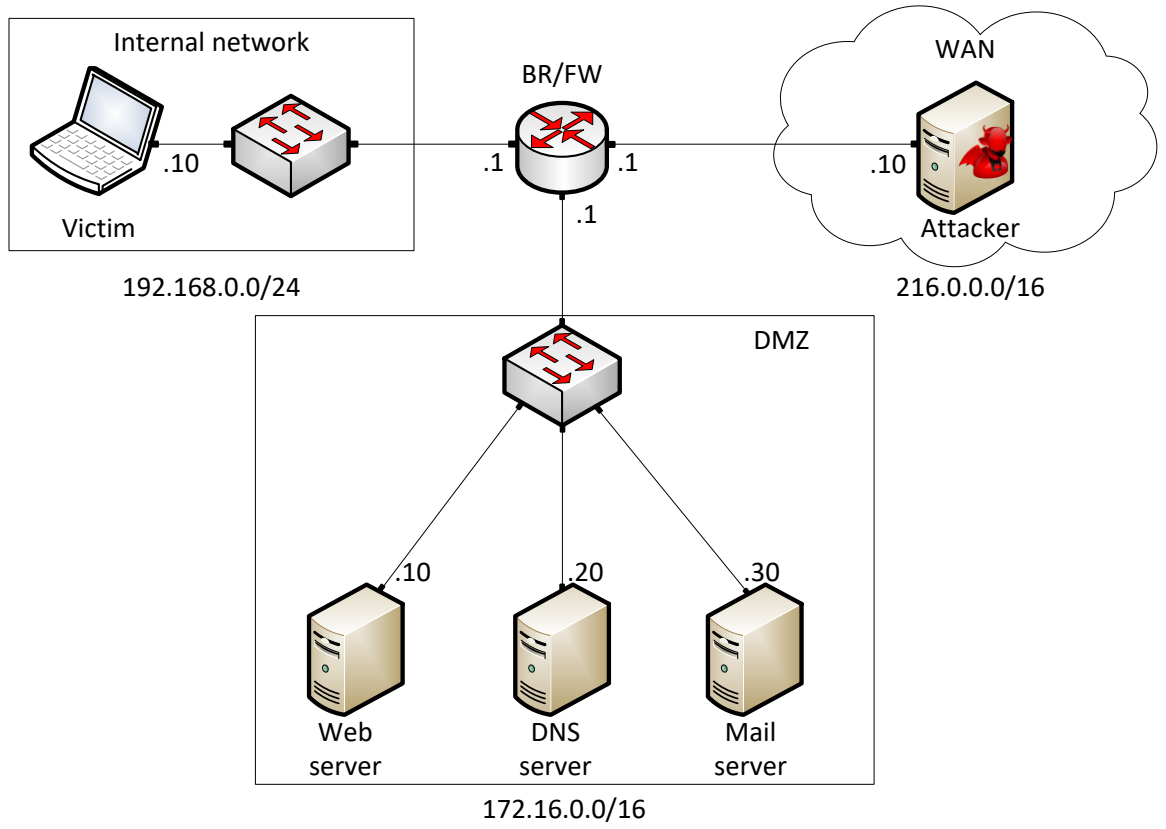
Lab Objectives

- Part 1: perform scanning using NMAP
  - The scan will be executed on the Attacker
  - The scan targets the DMZ network
  - Host discovery
  - TCP port scanning
  - OS and services version identification



Lab Objectives

- Part 2: vulnerability assessment using OpenVAS
  - Attacker machine will be used to perform a vulnerability assessment against the DMZ
  - The assessment uses Network Vulnerability Tests (NVTs) and CVE database
  - A report of the scan is produced



Platform Information

We will use the NETLAB virtual platform:

- **URL:** https://netlab.cec.sc.edu/
- **Username:** your_email_address
- **Temporary Password:** wastc2023