TTKS0700 Data Security Testing

Lab 02. Port scan

Jarmo Nevala, 10.09.2019

Mava updated 20.10.2020

jamk.fi

Lab 02. Port scan

Network traffic audit

- GOAL
  - To understand basics of the PORT SCAN
  - To learn basics of NMAP
  - To learn basics of NETCAT
  - To learn basics of NETSTAT
- In this document
  - RED color = TASK
  - BLUE color = TIP
  - Green color = Example

jamk.fi

Lab 02. Port scan

Port scan

- The goal of PORT SCANning is to find open services in network devices
- PORT SCAN is often divided to
  - INTERNAL SCAN (LAN)
  - EXTERNAL SCAN (WAN, INTERNET)
- External scan tells you what services are available outside of the target network (through routers, firewalls and other security devices)
- Internal scan tells you what services are enabled in the target device/system (through host base firewalls and security software)

Lab 02. Port scan

Tasks

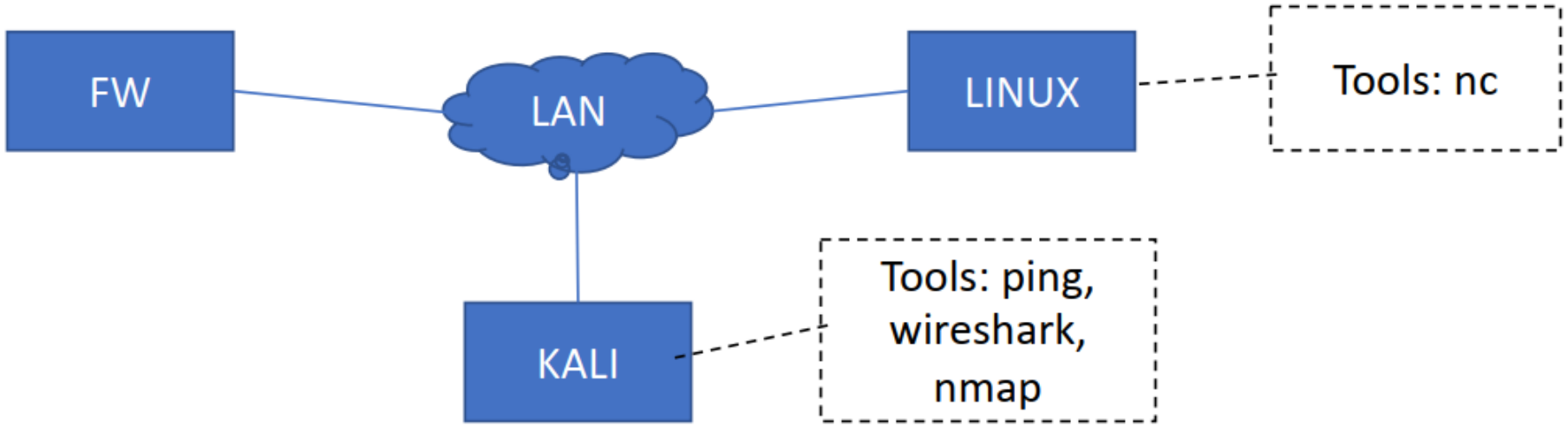
- Understood how NMAP works
- Run Internal scan against windows, linux, and firewall
- Run external scan against windows, linux, and firewall
- Use NMAP to validate Firewall rules
- Other ways to figure out running services??

- Extra: Use NMAP to scan IPv6 addresses

Lab 02. Port scan

NMAP

- How NMAP works ?
- Test setup:
  - Attach KALI workstation to LAN network.
  - Ping LINUX workstation from KALI (test connection)



jamk.fi

Lab 02. Port scan

NMAP

- Reading material:
  - https://nmap.org/
  - https://resources.infosecinstitute.com/nmap/#gref
- Understanding NMAP
  - start netcat on Linux (terminal, nc -lk –p888, starts netcat listener on port 888)
  - start wireshark on KALI
  - run following scans and look from wireshark what happens
    - nmap –sL x.x.x.x/yy (scan whole network)
    - nmap –sn x.x.x.x/yy (scan whole network)
    - nmap –sT –p888 x.x.x.x (scan single target)
    - nmap –sS –p888 x.x.x.x (scan single target)
    - nmap –sU –p888 x.x.x.x (scan single target) – what did you get as a result? Why?
    - nmap –sV –p888 x.x.x.x (scan single target) - what do you see in netcat listener? Why?

Lab 02. Port scan

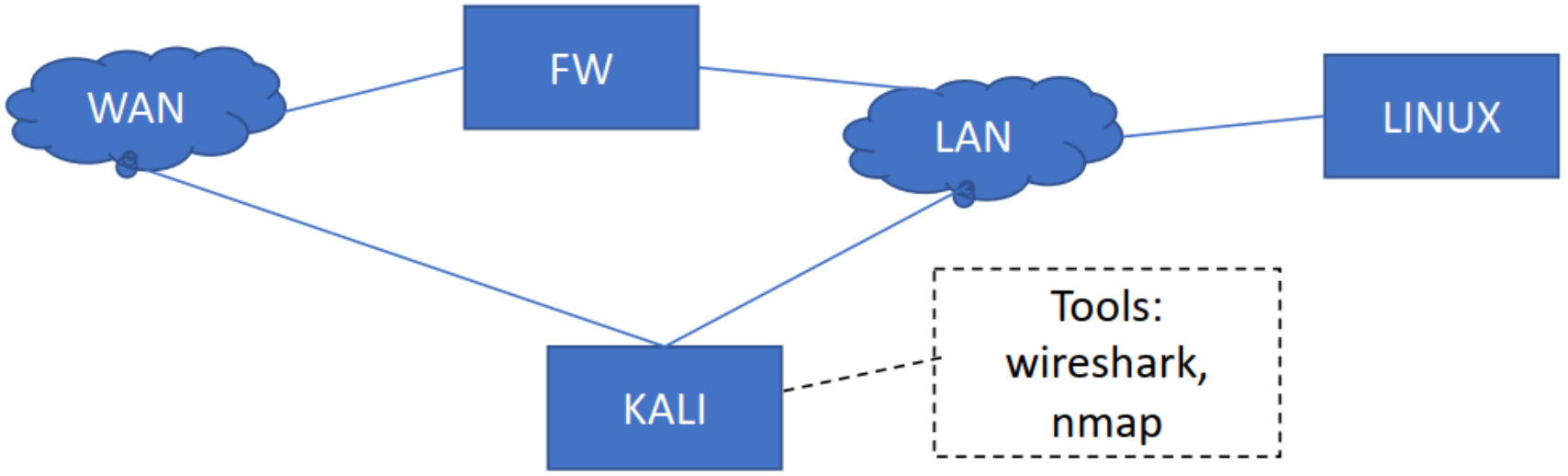
Task

- Run NMAP from KALI terminal
  - Run ICMP –scan against target network
  - Run TCP and UDP scans against target(s)
  - Run Service detection scan against target(s)
- ! Use output parameter to save results to file (-oA filename, -oX filename, etc)
- ! Remember
  - -n (do not resolve names)
  - -Pn (do not ping targets)
  - -p1-1024 (scan first 1024 ports)
  - -p- OR –p1-65535 (scan all 65535 ports)

Lab 02. Port scan

Use NMAP to validate Firewall rules

- TEST SETUP:
  - Connect one interface to WAN and another to LAN
  - Start wireshark on LAN interface



jamk.fi

Lab 02. Port scan

Use NMAP to validate Firewall rules

- FIREWALL is in NAT mode, so you can't scan internal hosts directly from WAN, but you can test if there any port forwarding rules from WAN to LAN
- Generate full scan from WAN to firewall interface
- Look from the Wireshark if you see any traffic from your KALI machine WAN-network ip-address
- Look at the results of port scan – are there any differences in:
  - What are the results of port scan
  - What you saw in wireshark
  - WHY?

Lab 02. Port scan

More scans!

- Run NMAP scans also against the Windows machine, and other Firewall interface
- Document the results

- EXTRA, You can also check the firewall rules with NMAP and WIRESHARK from LAN to WAN – network !

Lab 02. Port scan

Validate results!

- With NMAP you can only find services that are running in targets!
- List all running network services by using netstat –command
  - from windows –machine
  - from linux –machine

  - Are there any differences in listed network services an scanning results?

  - In audit you can use netstat to look running services and limit your NMAP scan to those ports only! (Save time!)
    1. WITH NETSTAT you see the services
    2. WITH NMAP you see what services are available from the network
       - host based firewall software etc. might block something
       - some services might listen only localhost interface
  - if you are not familiar with netstat –command use help, man page, or google ;)

jamk.fi

Lab 02. Port scan

Results – FIXED

- Look at the service descriptions in the NEXT slide
- Are there differences between the service description and NMAP scanning results?
- Is it possible that you missed something?
- Do you have any recommendations?

Service descriptions

Description of system (Use cases)

- Windows workstation is used to manage firewall and web server (linux)
  - Management is done with HTTP, and SSH
- Remote management, RDP connection is allowed to Windows workstation
- Web service is open to internet (public service)

Lab 02. Port scan

Conclusion

- Do you feel you understood methods to do External and Internal SCANS?
- How much time did you spend? Was it enough to get reliable results?

jamk.fi

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi