Nmap

- A classic reconnaissance tool for host and services discovery.
- The majority of the pentesters use it for the very first steps of the process

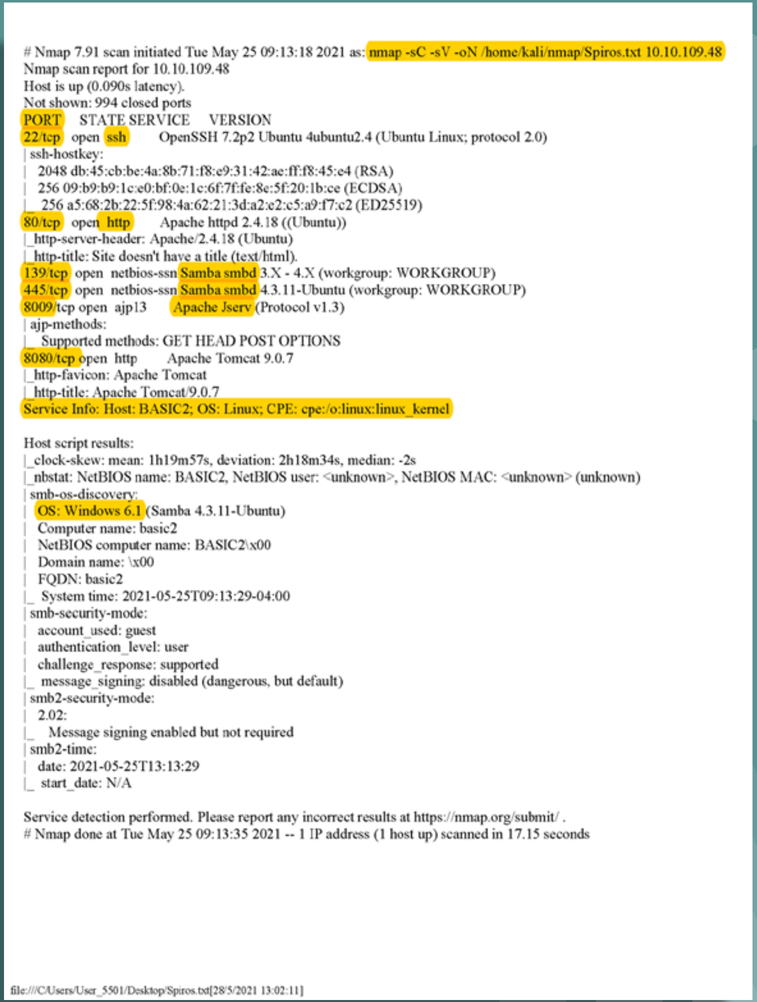
Example's commands explained :

- nmap -sC --> Performs a script scan using the default set of scripts
- nmap -sV --> Probe open ports to determine services
- nmap -oN --> extracts the terminal's result to a grepable form (xml, txt or html)

More about nmap > https://nmap.org/book/man.html

Group 2

Raquel Martinez Diez / Lukasz Kosmaczewski / Vaibhav Chawla
Anagnostopoulos Spiros



```
# Nmap 7.91 scan initiated Tue May 25 09:13:18 2021 as: nmap -sC -sV -oN /home/kali/nmap/Spiros.txt 10.10.109.48
Nmap scan report for 10.10.109.48
Host is up (0.090s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m57s, deviation: 2h18m34s, median: -2s
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2021-05-25T09:13:29-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-25T13:13:29
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 25 09:13:35 2021 -- 1 IP address (1 host up) scanned in 17.15 seconds
```

file:///C/Users/User_5501/Desktop/Spiros.txt[28/5/2021 13:02:11]

OpenVAS

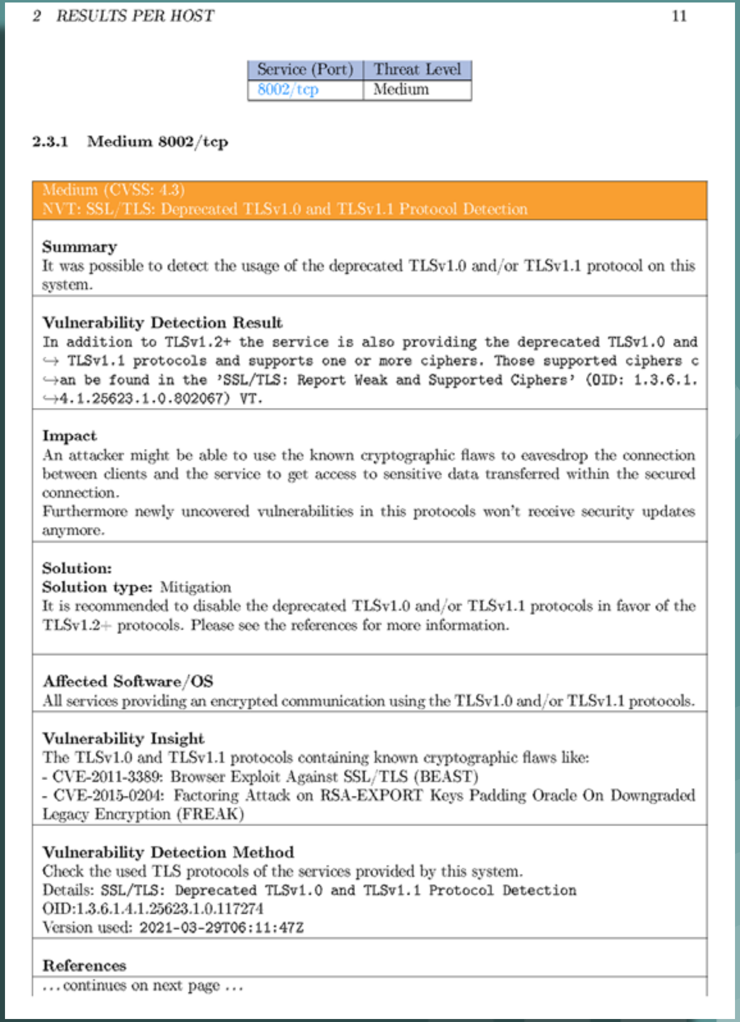
Greenbone
Sustainable Resilience

Is an open source Vulnerability Assessment Scanner

- It is not considered an intrusive way of scanning because it doesn't send malicious payloads that could cause a disruption
- Summary and Impact Description
- Produces an extended report per host and matches CVE ID for every vulnerability, providing suggestions to mitigate the vulnerability
- Further manual testing could focus on points already highlighted by OpenVAS

Group 2

Raquel Martinez Diez / Lukasz Kosmaczewski / Vaibhav Chawla
Anagnostopoulos Spiros



2 RESULTS PER HOST 11

Service (Port)	Threat Level
8002/tcp	Medium

2.3.1 Medium 8002/tcp

Medium (CVSS: 4.3)
NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.
↪4.1.25623.1.0.802067) VT.
```

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols containing known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2021-03-29T06:11:47Z`

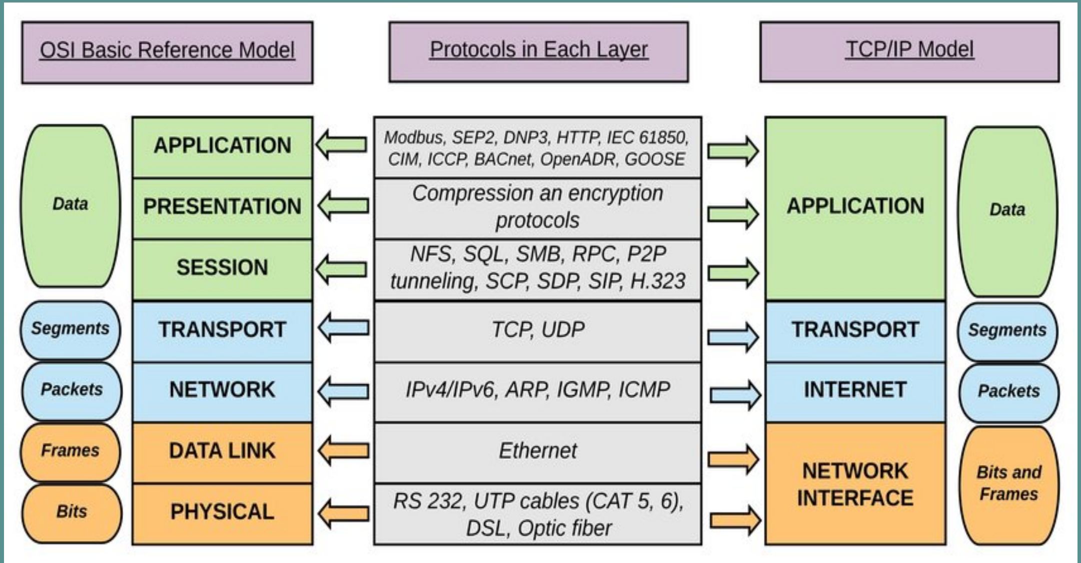
References

. . . continues on next page . . .

Additional tools we have also take under consideration:

- Dirbuster / Gobuster
- sqlmap
- Command Injection / XML External Entity

DISCLAIMER:
Not sure if this type is allowed because it may be against aws policy



	OSI Basic Reference Model	Protocols in Each Layer	TCP/IP Model	
Data	APPLICATION	Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE	APPLICATION	Data
	PRESENTATION	Compression an encryption protocols		
	SESSION	NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323		
Segments	TRANSPORT	TCP, UDP	TRANSPORT	Segments
Packets	NETWORK	IPv4/IPv6, ARP, IGMP, ICMP	INTERNET	Packets
Frames	DATA LINK	Ethernet	NETWORK INTERFACE	Bits and Frames
Bits	PHYSICAL	RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber		

Why does the Internet use TCP/IP and not the OSI stack ?

OSI Model was developed as a theoretical model in an attempt to streamline and define various data networking functions. On the other hand, TCP/IP stack was used by the DoD to implement protocols practically, by adhering the simplicity principle. This required merging/coupling of layers with higher interdependencies, thus decreasing avoidable complexities.

> *“Increased layering can quickly lead to violation of the Simplicity Principle. Industry experience has taught us that increased layering frequently increases complexity and hence leads to increases in OPEX, as is predicted by the Simplicity Principle” (RFC 3439).*

References:
https://datatracker.ietf.org/doc/html/rfc3439#section-3