Vulnerability Management (and Patching)

By: Gary Bevans

Key Takeaways from Today's Lecture

What is Vulnerability Management?

Tools Used?

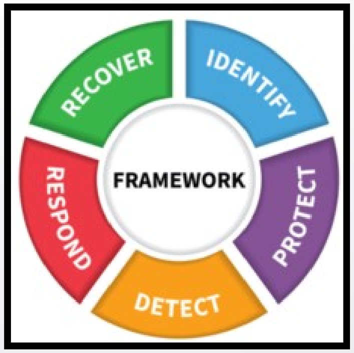
How it relates to Patching?

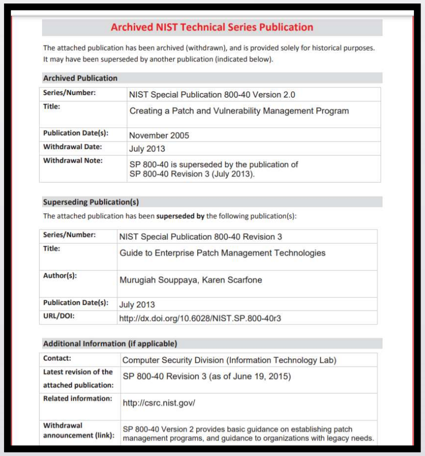
Current Guidance on it?

Guidance

- National Institute of Standards and Technology

- NIST 5 Function Relation:
  - **Identify**
  - "**Identifying asset vulnerabilities**, threats to internal and external organizational resources, and risk response activities as a basis for the organizations Risk Assessment".
  - **NIST SP 800-40**





Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NIST Special Publication 800-40 Version 2.0
Title:	Creating a Patch and Vulnerability Management Program
Publication Date(s):	November 2005
Withdrawal Date:	July 2013
Withdrawal Note:	SP 800-40 is superseded by the publication of SP 800-40 Revision 3 (July 2013).

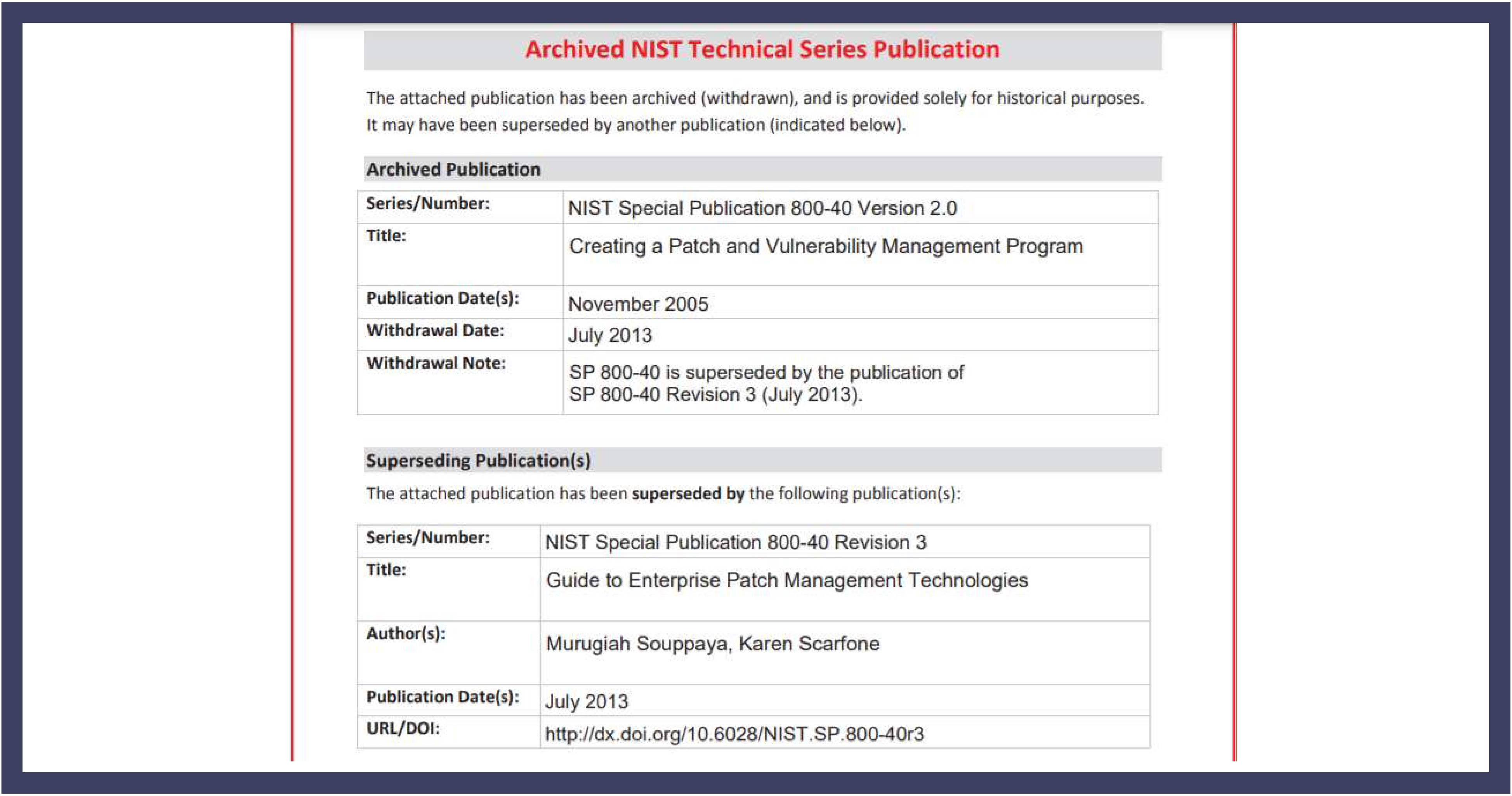
Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	NIST Special Publication 800-40 Revision 3
Title:	Guide to Enterprise Patch Management Technologies
Author(s):	Murugiah Souppaya, Karen Scarfone
Publication Date(s):	July 2013
URL/DOI:	http://dx.doi.org/10.6028/NIST.SP.800-40r3

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Lab)
Latest revision of the attached publication:	SP 800-40 Revision 3 (as of June 19, 2015)
Related information:	http://csrc.nist.gov/
Withdrawal announcement (link):	SP 800-40 Version 2 provides basic guidance on establishing patch management programs, and guidance to organizations with legacy needs.



Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

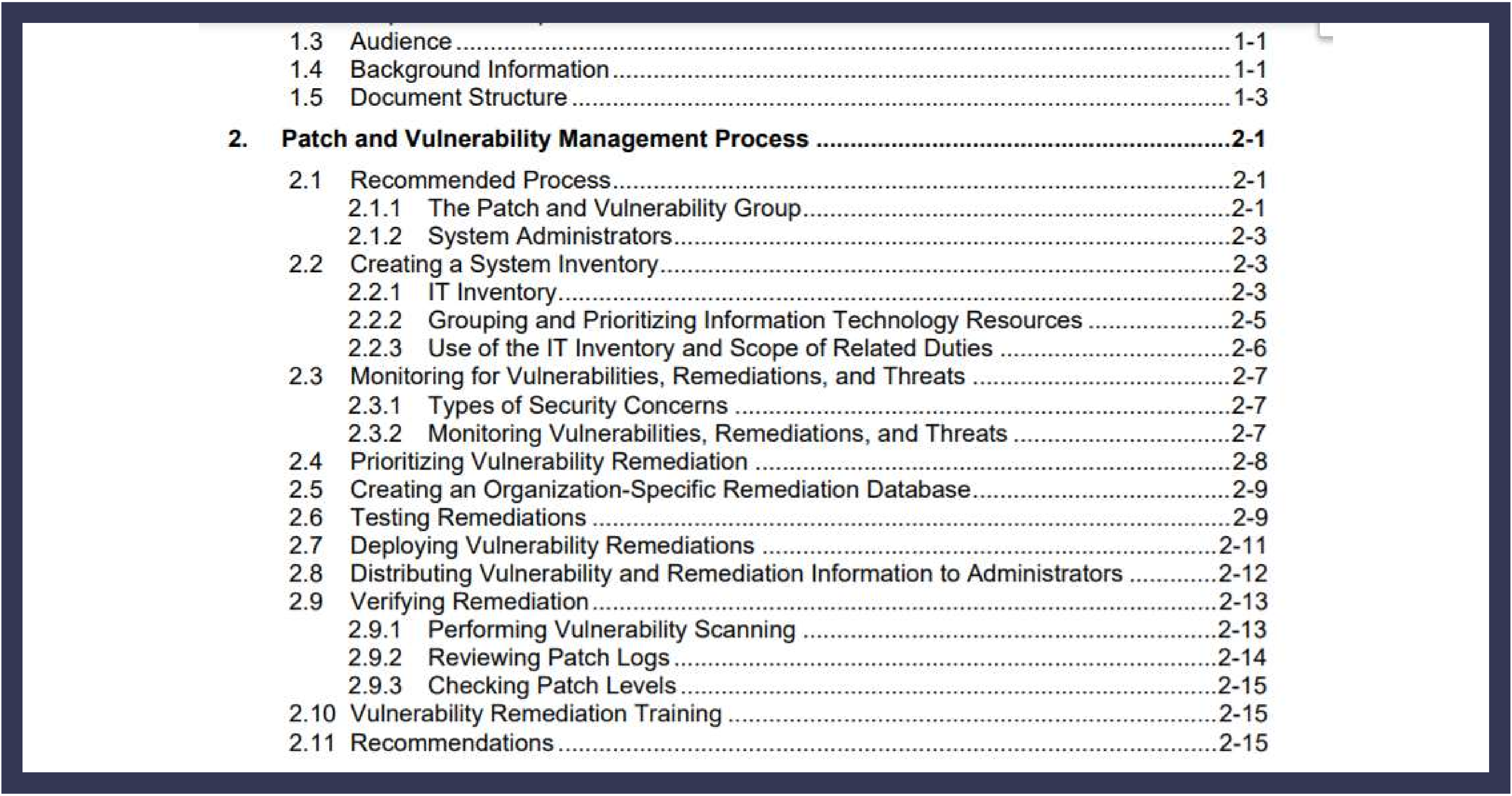
Archived Publication

Series/Number:	NIST Special Publication 800-40 Version 2.0
Title:	Creating a Patch and Vulnerability Management Program
Publication Date(s):	November 2005
Withdrawal Date:	July 2013
Withdrawal Note:	SP 800-40 is superseded by the publication of SP 800-40 Revision 3 (July 2013).

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	NIST Special Publication 800-40 Revision 3
Title:	Guide to Enterprise Patch Management Technologies
Author(s):	Murugiah Souppaya, Karen Scarfone
Publication Date(s):	July 2013
URL/DOI:	http://dx.doi.org/10.6028/NIST.SP.800-40r3



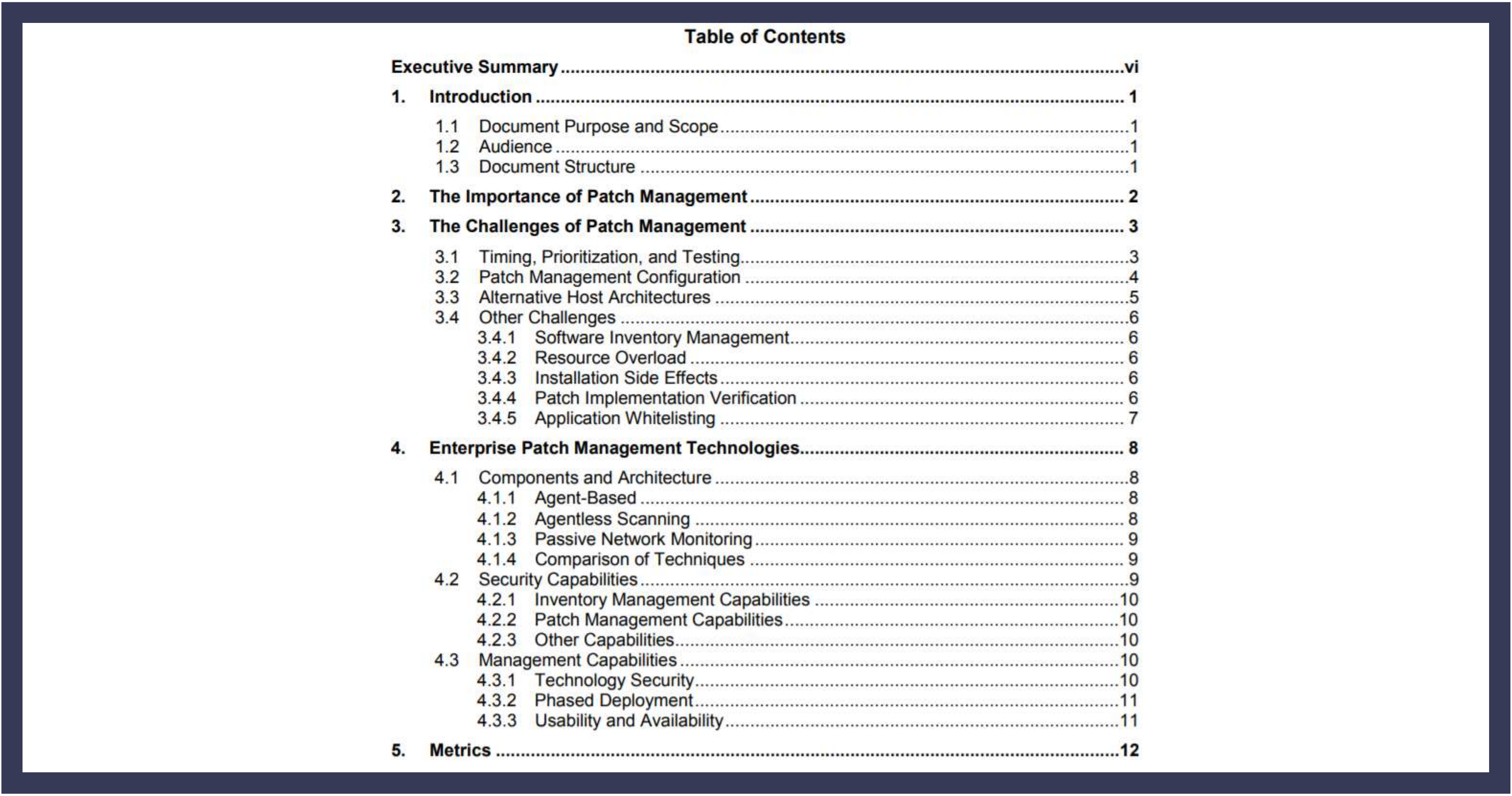


Table of Contents

Vulnerability Management vs Patching

- **Vulnerability Management** is the process of **identifying**, cataloging, remediating, and mitigating vulnerabilities found in software or hardware.

- *Software vulnerabilities* are the most common and typically solved by network isolation, **patching**, or configuration management.

- Vulnerabilities are normally identified using a scanner or endpoint agent to detect and identify known vulnerabilities.

Vulnerability Management vs Patching

Patch Management is the process of **identifying**, testing and deploying patches for operating systems or applications on devices to ensure systems stay up to date.

Patches are pieces of code added to the existing software code to improve functionality or to remove vulnerabilities discovered in the software.

Patch management tools help orchestrate patch deployment by prioritizing patches and systems they should be installed on.

Vulnerability Management vs Patching

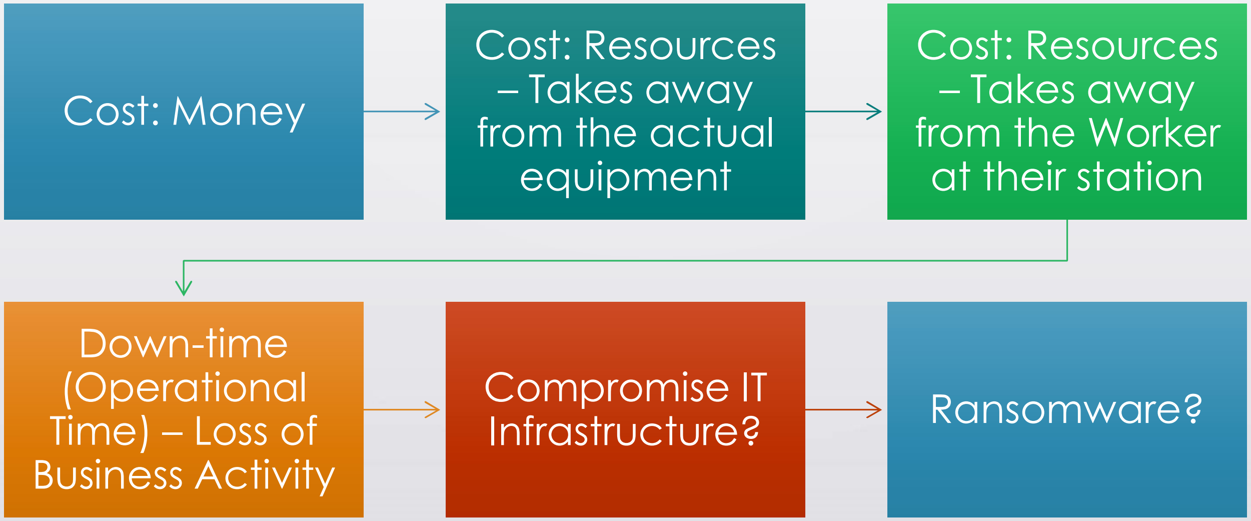
Vulnerability Mgmt.

- Vulnerability tools are only a discovery mechanism.
- These tools only discover the issues and leave it to the organizations to remediate them.

Vulnerability Mgmt. Relation to Patch Mgmt.

- A typical workflow would have security operations scanning and detecting a vulnerability, creating a ticket with IT and waiting for IT to both patch and communicate the patch's success back to security operations to close the loop.

Why is Vulnerability Mgmt. So Important? & What Concerns Organizations May Have?



Cost: Money

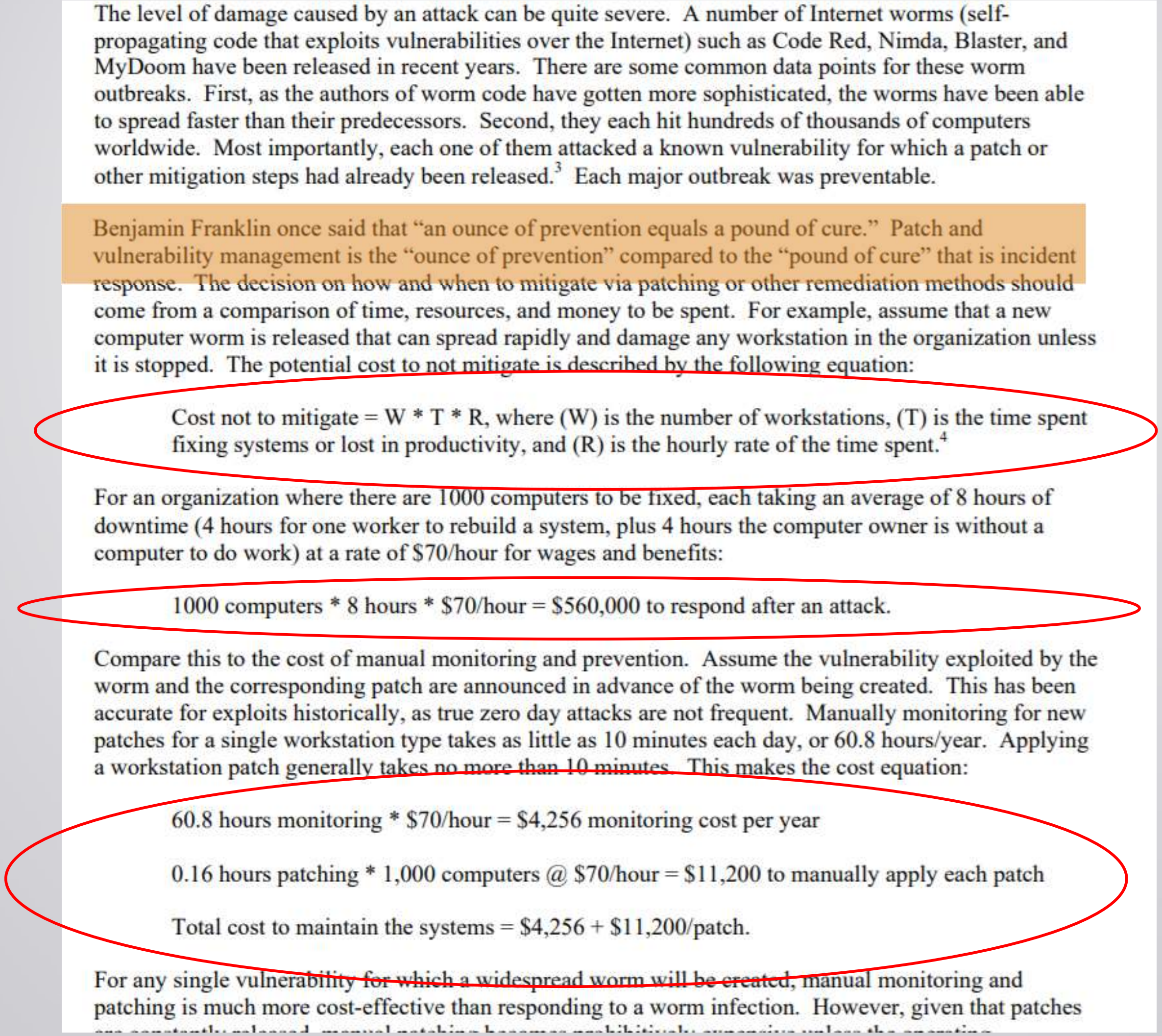
Cost: Resources – Takes away from the actual equipment

Cost: Resources – Takes away from the Worker at their station

Down-time (Operational Time) – Loss of Business Activity

Compromise IT Infrastructure?

Ransomware?



The level of damage caused by an attack can be quite severe. A number of Internet worms (self-propagating code that exploits vulnerabilities over the Internet) such as Code Red, Nimda, Blaster, and MyDoom have been released in recent years. There are some common data points for these worm outbreaks. First, as the authors of worm code have gotten more sophisticated, the worms have been able to spread faster than their predecessors. Second, they each hit hundreds of thousands of computers worldwide. Most importantly, each one of them attacked a known vulnerability for which a patch or other mitigation steps had already been released.[3] Each major outbreak was preventable.

Benjamin Franklin once said that "an ounce of prevention equals a pound of cure." Patch and vulnerability management is the "ounce of prevention" compared to the "pound of cure" that is incident response. The decision on how and when to mitigate via patching or other remediation methods should come from a comparison of time, resources, and money to be spent. For example, assume that a new computer worm is released that can spread rapidly and damage any workstation in the organization unless it is stopped. The potential cost to not mitigate is described by the following equation:

> Cost not to mitigate = W * T * R, where (W) is the number of workstations, (T) is the time spent fixing systems or lost in productivity, and (R) is the hourly rate of the time spent.[4]

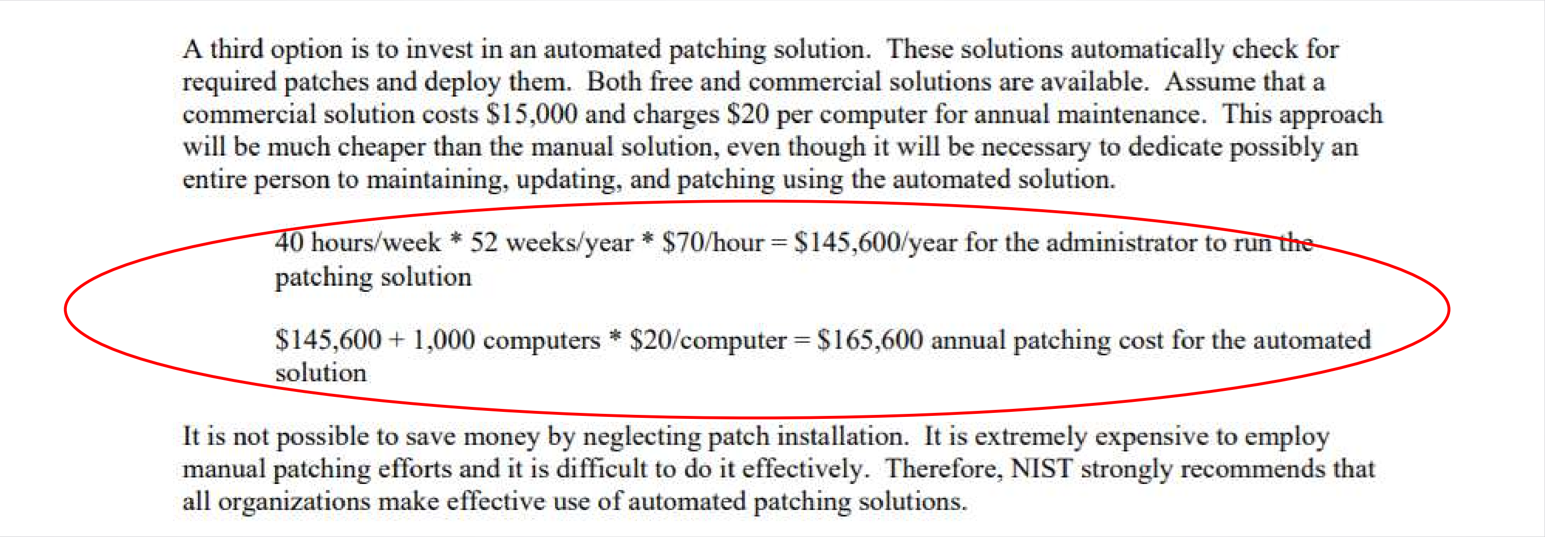
For an organization where there are 1000 computers to be fixed, each taking an average of 8 hours of downtime (4 hours for one worker to rebuild a system, plus 4 hours the computer owner is without a computer to do work) at a rate of $70/hour for wages and benefits:

> 1000 computers * 8 hours * $70/hour = $560,000 to respond after an attack.

Compare this to the cost of manual monitoring and prevention. Assume the vulnerability exploited by the worm and the corresponding patch are announced in advance of the worm being created. This has been accurate for exploits historically, as true zero day attacks are not frequent. Manually monitoring for new patches for a single workstation type takes as little as 10 minutes each day, or 60.8 hours/year. Applying a workstation patch generally takes no more than 10 minutes. This makes the cost equation:

> 60.8 hours monitoring * $70/hour = $4,256 monitoring cost per year
>
> 0.16 hours patching * 1,000 computers @ $70/hour = $11,200 to manually apply each patch
>
> Total cost to maintain the systems = $4,256 + $11,200/patch.

For any single vulnerability for which a widespread worm will be created, manual monitoring and patching is much more cost-effective than responding to a worm infection. However, given that patches are constantly released, manual patching becomes prohibitively expensive unless the operating



A third option is to invest in an automated patching solution. These solutions automatically check for required patches and deploy them. Both free and commercial solutions are available. Assume that a commercial solution costs $15,000 and charges $20 per computer for annual maintenance. This approach will be much cheaper than the manual solution, even though it will be necessary to dedicate possibly an entire person to maintaining, updating, and patching using the automated solution.

> 40 hours/week * 52 weeks/year * $70/hour = $145,600/year for the administrator to run the patching solution
>
> $145,600 + 1,000 computers * $20/computer = $165,600 annual patching cost for the automated solution

It is not possible to save money by neglecting patch installation. It is extremely expensive to employ manual patching efforts and it is difficult to do it effectively. Therefore, NIST strongly recommends that all organizations make effective use of automated patching solutions.

The Vulnerability Scanner

- They identify vulnerabilities on their hosts and networks
- It uses a large databases of vulnerabilities to identify vulnerabilities associated with commonly used *operating systems* and applications

- **Two Types**
  - **Host scanners**: used for identifying specific operating system and application misconfigurations and vulnerabilities
  - **Network scanners**: used for identifying open ports, vulnerable software, and misconfigured services

The Vulnerability Scanner

- **Two Types:**
  - **Host scanners**: used for identifying specific operating system and application misconfigurations and vulnerabilities

QUALYS

nessus

  - **Network scanners**: used for identifying open ports, vulnerable software, and misconfigured services

NMAP

The Vulnerability Scanner

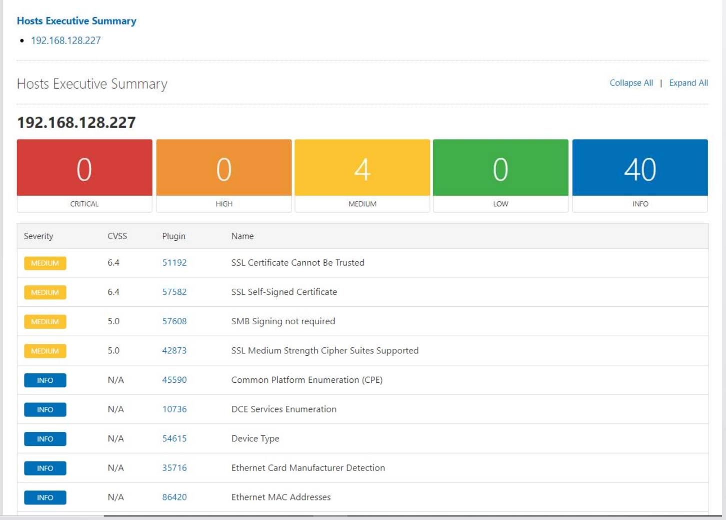
Pros:

- Proactively **identify vulnerabilities**
- Provide a fast and easy way to measure exposure
- Automatically fix discovered vulnerabilities
- Identify out-of-date software versions
- Validate compliance with an organizational security policy
- **Generate alerts and reports** about identified vulnerabilities

Cons:

- Depend on regular updating of the **vulnerability database**
- Tend to have a high false positive error rate
- May generate significant amounts of network traffic
- May cause a denial of service (DoS) of hosts, because scanner probing may cause a system to crash inadvertently

Nessus



Hosts Executive Summary

- 192.168.128.227

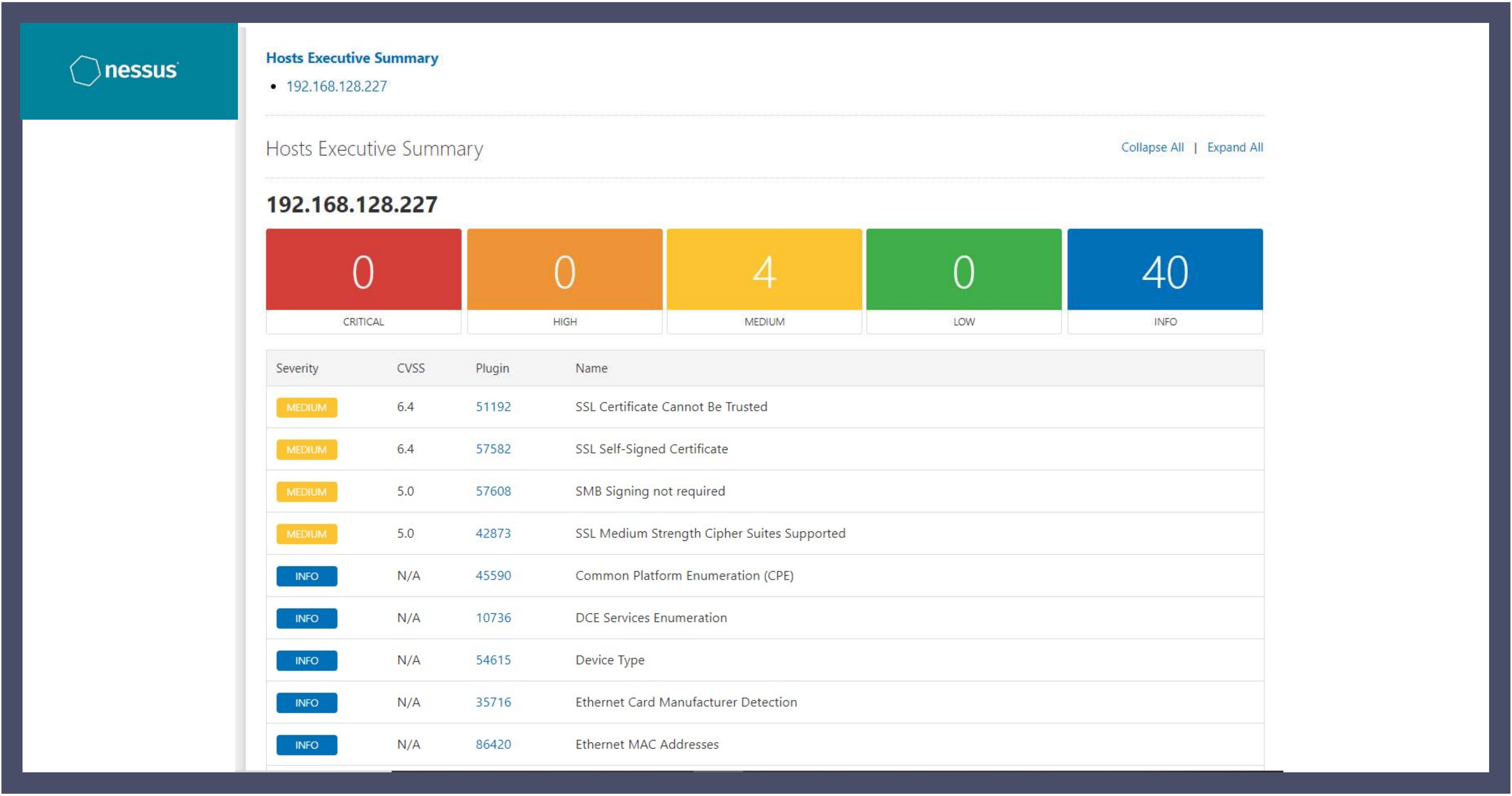
Hosts Executive Summary

192.168.128.227

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	40

Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses

- Scans devices on a given network
- Interprets result in a nicely produced report
- Uses the CVSS - the Common Vulnerability Scoring System
- And is very detailed



Hosts Executive Summary

- 192.168.128.227

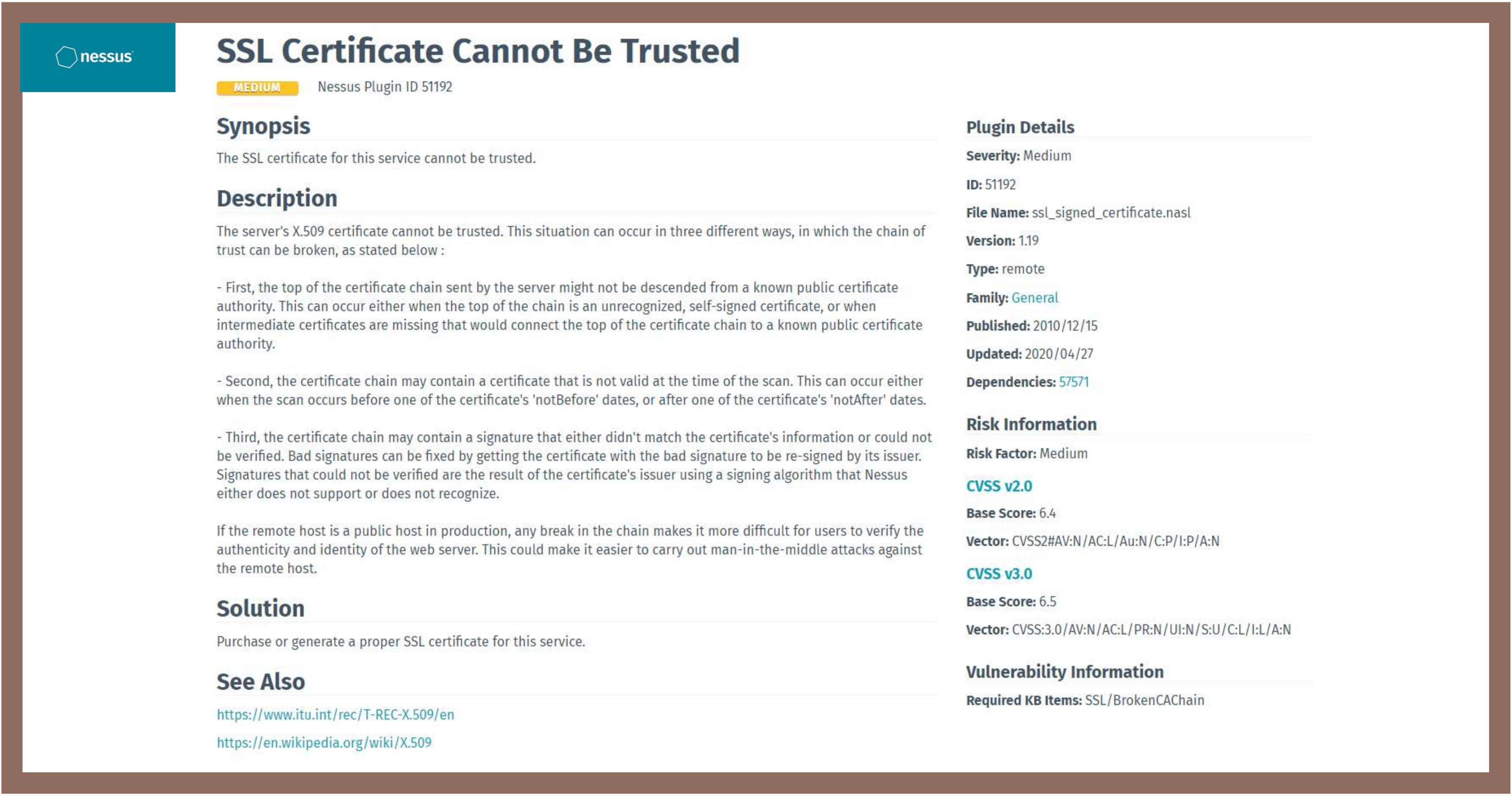
Hosts Executive Summary

Collapse All | Expand All

192.168.128.227

0	0	4	0	40
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses



SSL Certificate Cannot Be Trusted

MEDIUM Nessus Plugin ID 51192

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Plugin Details

Severity: Medium

ID: 51192

File Name: ssl_signed_certificate.nasl

Version: 1.19

Type: remote

Family: General

Published: 2010/12/15

Updated: 2020/04/27

Dependencies: 57571

Risk Information

Risk Factor: Medium

CVSS v2.0

Base Score: 6.4

Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

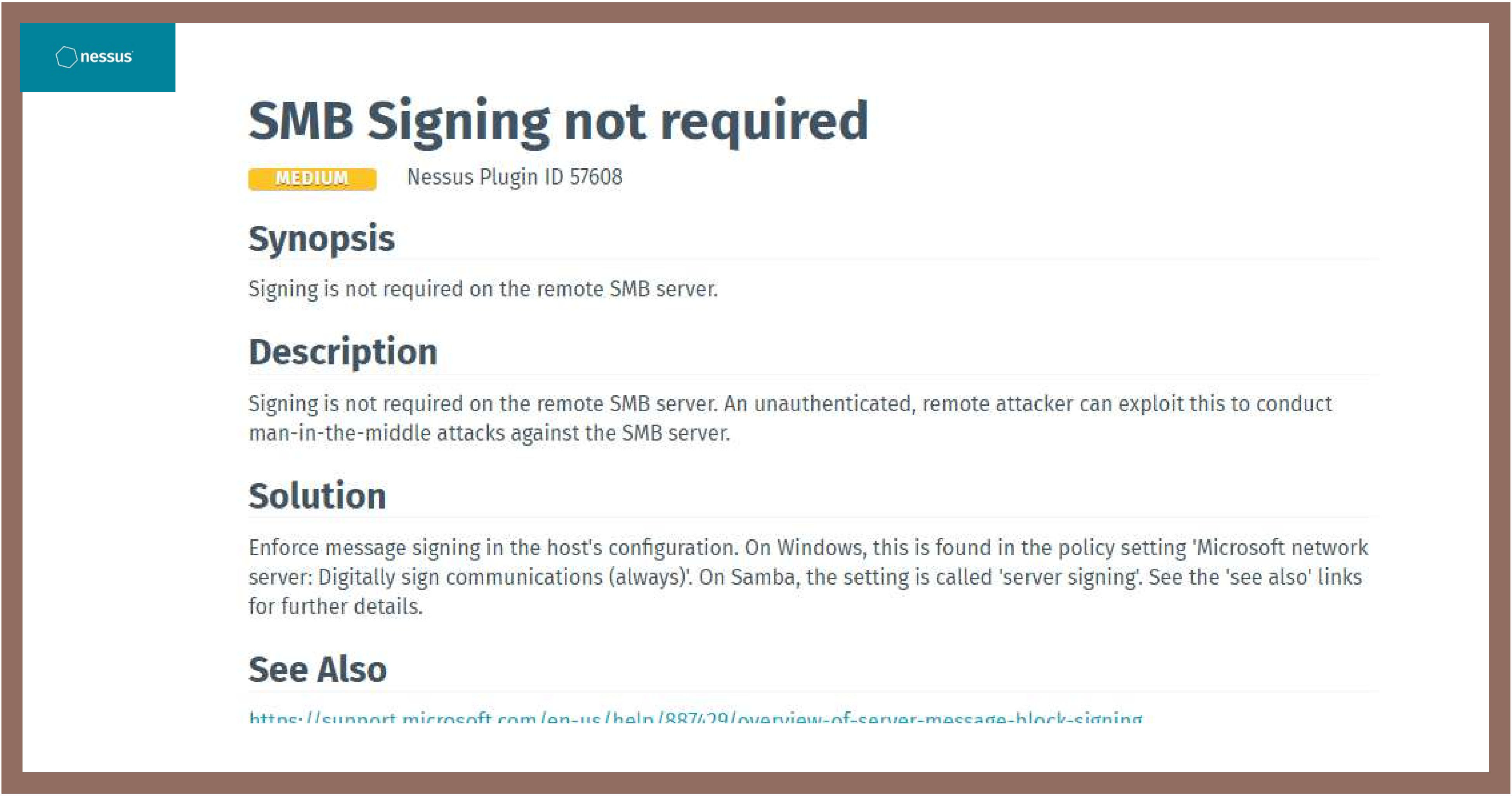
CVSS v3.0

Base Score: 6.5

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Vulnerability Information

Required KB Items: SSL/BrokenCAChain



SMB Signing not required

MEDIUM Nessus Plugin ID 57608

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

Nessus

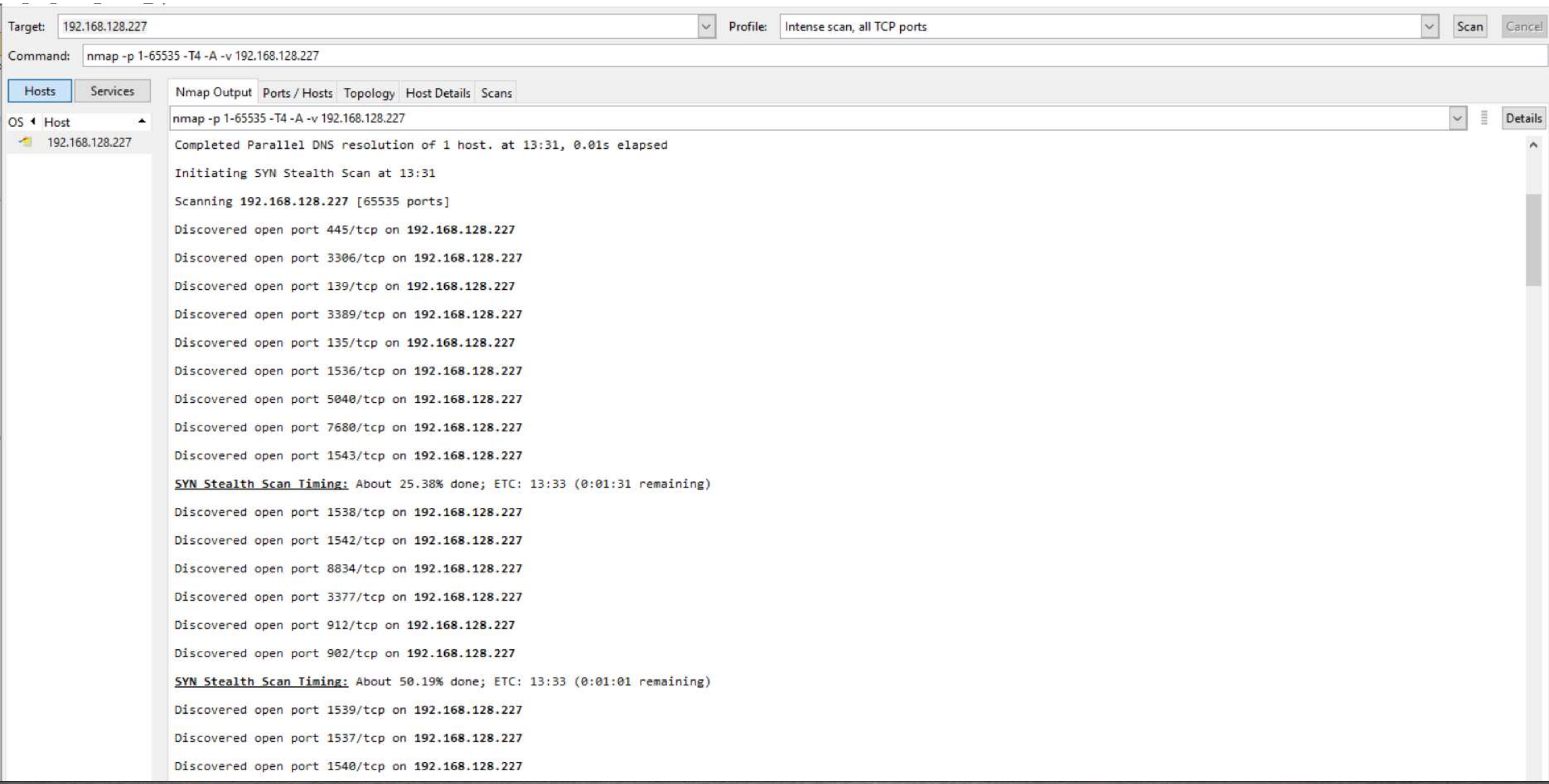
- ***Identifies*** vulnerabilities that exist on the designated host/ systems, in accordance with the repository.

- These are some of the visible vulnerabilities that can be targeted with attacks (vectors) via attackers or other penetration tools like ***Metasploit***.
  - Which was also briefly discussed by guest speaker Mr. Konstantinos

Nmap

Network Mapper

Scan for the ports and services



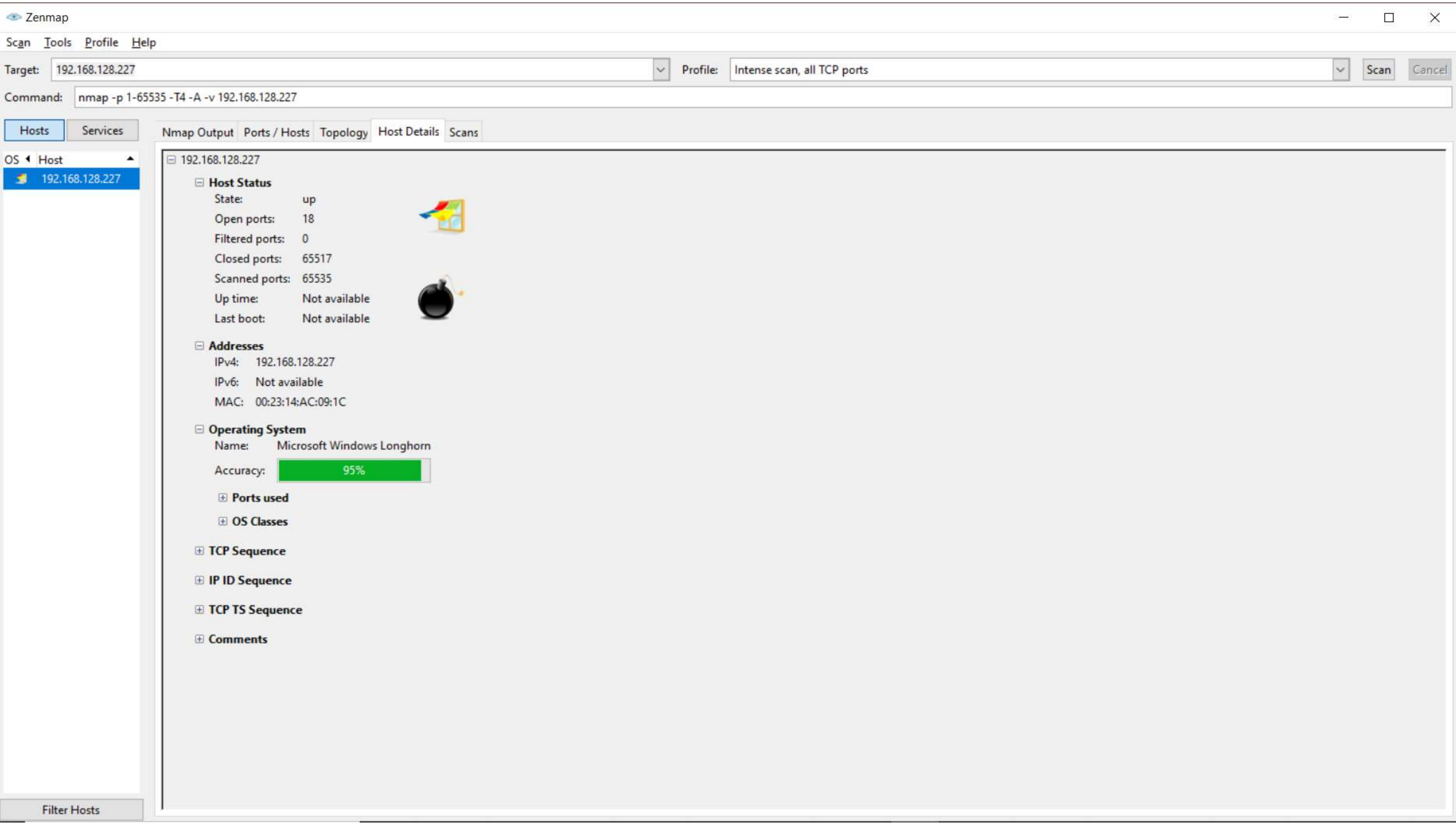
Target: 192.168.128.227

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.128.227

```
nmap -p 1-65535 -T4 -A -v 192.168.128.227
```

```
Completed Parallel DNS resolution of 1 host. at 13:31, 0.01s elapsed
Initiating SYN Stealth Scan at 13:31
Scanning 192.168.128.227 [65535 ports]
Discovered open port 445/tcp on 192.168.128.227
Discovered open port 3306/tcp on 192.168.128.227
Discovered open port 139/tcp on 192.168.128.227
Discovered open port 3389/tcp on 192.168.128.227
Discovered open port 135/tcp on 192.168.128.227
Discovered open port 1536/tcp on 192.168.128.227
Discovered open port 5040/tcp on 192.168.128.227
Discovered open port 7680/tcp on 192.168.128.227
Discovered open port 1543/tcp on 192.168.128.227
SYN Stealth Scan Timing: About 25.38% done; ETC: 13:33 (0:01:31 remaining)
Discovered open port 1538/tcp on 192.168.128.227
Discovered open port 1542/tcp on 192.168.128.227
Discovered open port 8834/tcp on 192.168.128.227
Discovered open port 3377/tcp on 192.168.128.227
Discovered open port 912/tcp on 192.168.128.227
Discovered open port 902/tcp on 192.168.128.227
SYN Stealth Scan Timing: About 50.19% done; ETC: 13:33 (0:01:01 remaining)
Discovered open port 1539/tcp on 192.168.128.227
Discovered open port 1537/tcp on 192.168.128.227
Discovered open port 1540/tcp on 192.168.128.227
```



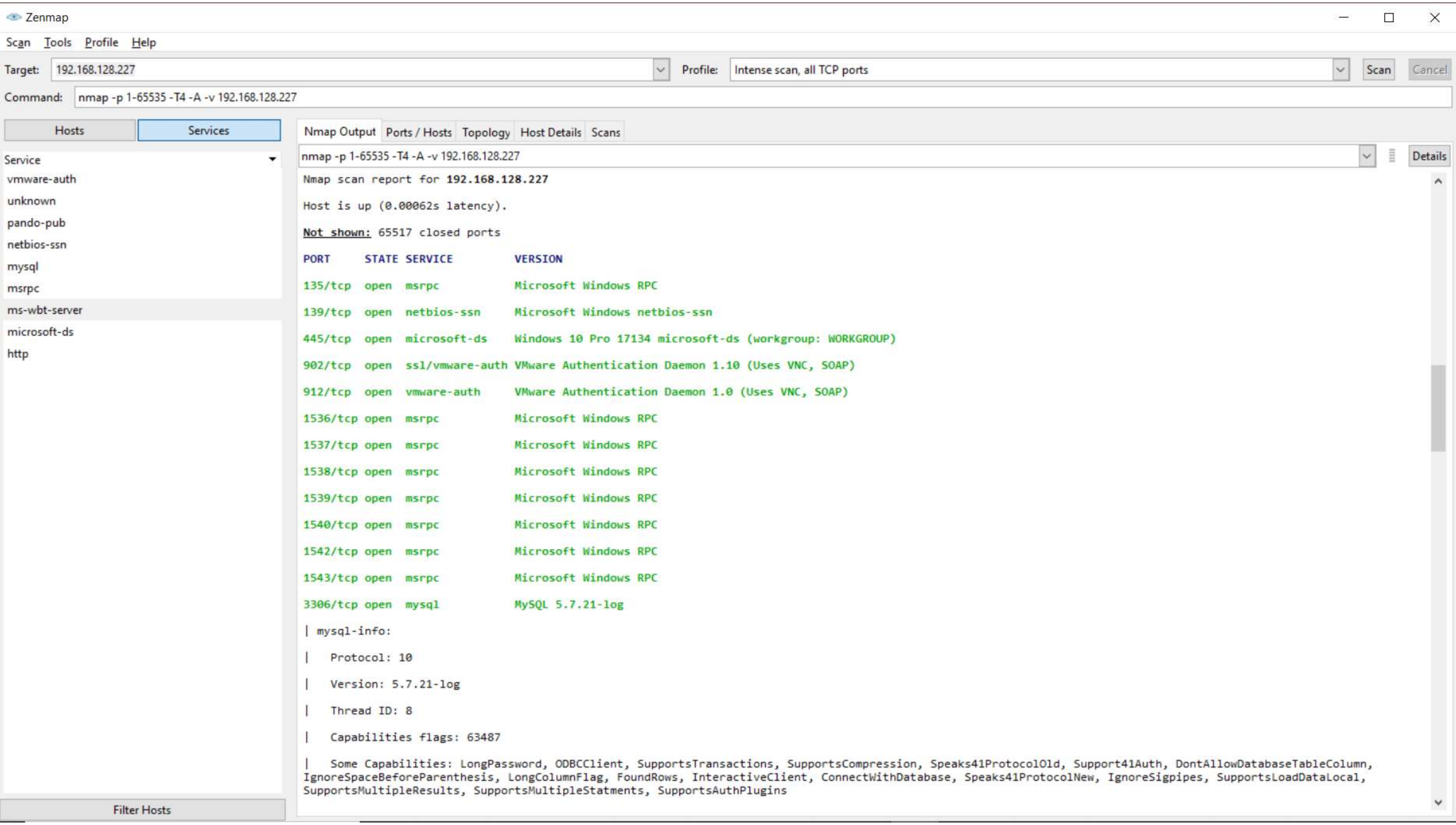
Target: 192.168.128.227

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.128.227

192.168.128.227

```
⊟ 192.168.128.227
    ⊟ Host Status
        State:          up
        Open ports:     18
        Filtered ports: 0
        Closed ports:   65517
        Scanned ports:  65535
        Up time:        Not available
        Last boot:      Not available
    ⊟ Addresses
        IPv4:  192.168.128.227
        IPv6:  Not available
        MAC:   00:23:14:AC:09:1C
    ⊟ Operating System
        Name:      Microsoft Windows Longhorn
        Accuracy:  95%
        ⊞ Ports used
        ⊞ OS Classes
    ⊞ TCP Sequence
    ⊞ IP ID Sequence
    ⊞ TCP TS Sequence
    ⊞ Comments
```



Target: 192.168.128.227

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.128.227

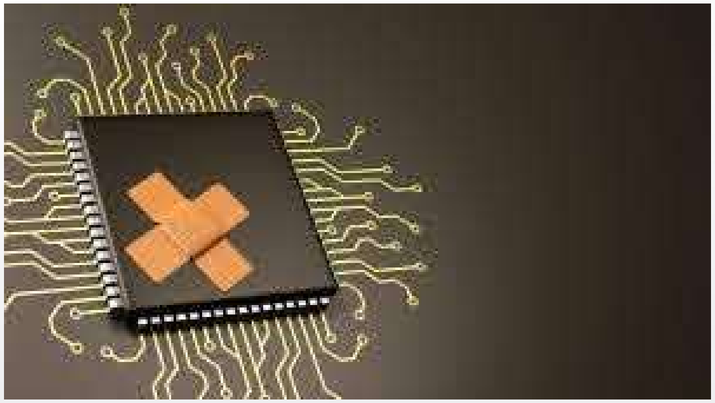
Service
vmware-auth
unknown
pando-pub
netbios-ssn
mysql
msrpc
ms-wbt-server
microsoft-ds
http

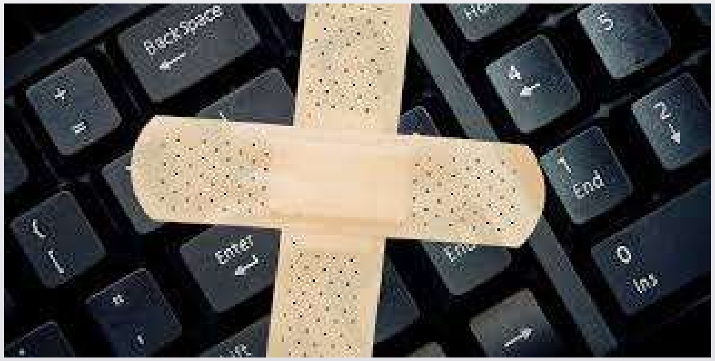
nmap -p 1-65535 -T4 -A -v 192.168.128.227

```
Nmap scan report for 192.168.128.227

Host is up (0.00062s latency).

Not shown: 65517 closed ports

PORT     STATE SERVICE         VERSION

135/tcp  open  msrpc           Microsoft Windows RPC

139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn

445/tcp  open  microsoft-ds    Windows 10 Pro 17134 microsoft-ds (workgroup: WORKGROUP)

902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)

912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)

1536/tcp open  msrpc           Microsoft Windows RPC

1537/tcp open  msrpc           Microsoft Windows RPC

1538/tcp open  msrpc           Microsoft Windows RPC

1539/tcp open  msrpc           Microsoft Windows RPC

1540/tcp open  msrpc           Microsoft Windows RPC

1542/tcp open  msrpc           Microsoft Windows RPC

1543/tcp open  msrpc           Microsoft Windows RPC

3306/tcp open  mysql           MySQL 5.7.21-log

| mysql-info:

|   Protocol: 10

|   Version: 5.7.21-log

|   Thread ID: 8

|   Capabilities flags: 63487

|   Some Capabilities: LongPassword, ODBCClient, SupportsTransactions, SupportsCompression, Speaks41ProtocolOld, Support41Auth, DontAllowDatabaseTableColumn,
IgnoreSpaceBeforeParenthesis, LongColumnFlag, FoundRows, InteractiveClient, ConnectWithDatabase, Speaks41ProtocolNew, IgnoreSigpipes, SupportsLoadDataLocal,
SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
```

Patching?

- Know what the weaknesses are with the assets
- Deploy corrective measures to take care of them:
  - Configuration?
  - Update?
  - Working with vendors to correct?





Key Takeaways from Today's Lecture

- What is Vulnerability Management?
- Tools Used?
- How it relates to Patching?
- Current Guidance on it?

Resources

NIST. July 2013. *SP 800-40 Version 2.0 (Creating a Patch and Vulnerability Management Program)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-40/version-20/archive/2005-11-16.

NIST. July 2013. *SP 800-40 Rev. 3 (Guide to Enterprise Patch Management Technologies)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-40/version-20/archive/2005-11-16.

Resources

Jay Goodman. February 20, 2020. *Patch Management vs Vulnerability Management*. Retrieved from https://blog.automox.com/what-is-patch-management.

SolarWinds. July 21, 2020. *What Is Vulnerability Patching? Guide to Patch and Vulnerabilities*. Retrieved from https://www.dnsstuff.com/vulnerability-and-patch-management.

QUESTIONS,
COMMENTS,
CONCERNS?