

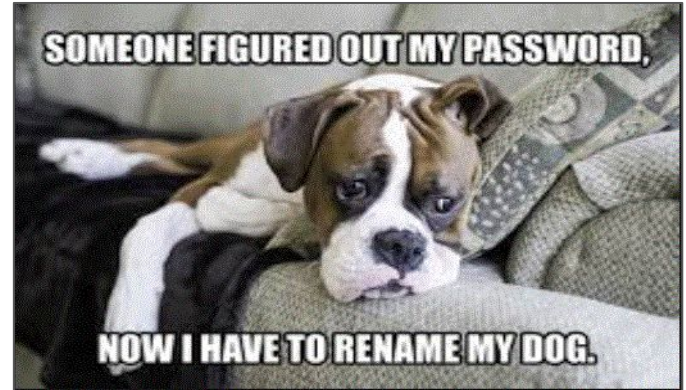


Vulnerability Management

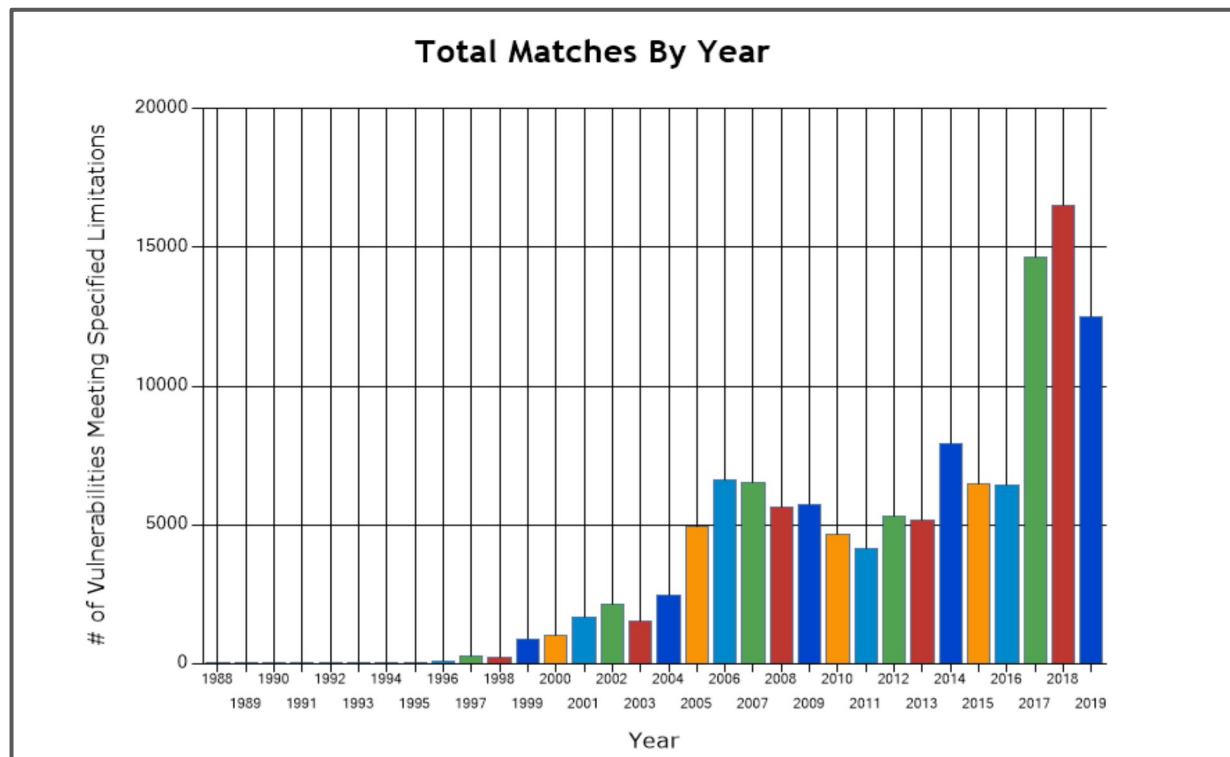
Spring 2021
Jay Chen

What is a vulnerability?

- A **vulnerability** is a cybersecurity flaw in a system that leave it open to attack.
- A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.



How many vulnerabilities are there?



- NIST National Vulnerability Database
- 123,622 documented vulnerabilities
- Last 3 years: 43,662

Types of vulnerability

- Operating System Vulnerability
- Network Vulnerability
- Application Vulnerability
- Misconfigured Server (Open Ports)
- Default Credentials



Common Types of Vulnerability Impact

- Elevation of Privilege
- Information Disclosure
- Denial of Service
- Remote Code Execution



Common Vulnerability Scoring System

- Vulnerability are scored using CVSS scoring standard and given a severity between 0 and 10.

Scores	Severity
0.0	None/Informational
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10.0	Critical

<https://chandanbn.github.io/cvss/>

Vulnerability Example: BlueKeep



- BlueKeep (CVE-2019-0708)
- <https://nvd.nist.gov/vuln/detail/CVE-2019-0708>
- <https://www.rapid7.com/db/?type=metasploit>

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3.0 legend)

Impact Score: 5.9

Exploitability Score: 3.9

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): High

Integrity (I): High

Availability (A): High

Major Vulnerability Review 2020-2021

- **CVE-2020-1472 (NetLogon)**

- Elevation of Privilege vulnerability affecting domain controller.
Successful exploitation could allow for a complete takeover of a Windows domain.

- **CVE-2020-1350 (SIGRed)**

- Remote Code Execution vulnerability affecting DNS servers.
Successful exploitation could for code execution under the local system account.

- **SolarWinds Orion Platform (SUNBURST)**

- Vulnerable versions of SolarWinds Orion contained a malware backdoor known as SUNBURST

- **CVE-2021-26855 (Proxylogon/Hafnium)**

- Authentication bypass vulnerability on Microsoft Exchange Servers, which could lead to Code Execution.

Vulnerability Intelligence Gathering

- [IBM X-Force Vulnerability Feed](#)
- [DHS CISA](#)
- [BleepingComputer](#)
- [Shodan.io](#)
- Vendor Website
 - [Cisco](#)
 - [Microsoft](#)



What is vulnerability assessment?

- Process of defining, identifying, classifying, and prioritizing vulnerability in computer systems, applications, and network infrastructures.



**Vulnerability
Identification**



Analysis



**Risk
Assessment**



Remediation

Asset Prioritization

- **Critical Assets**

- IT assets that are essential to a company's day to day operations.

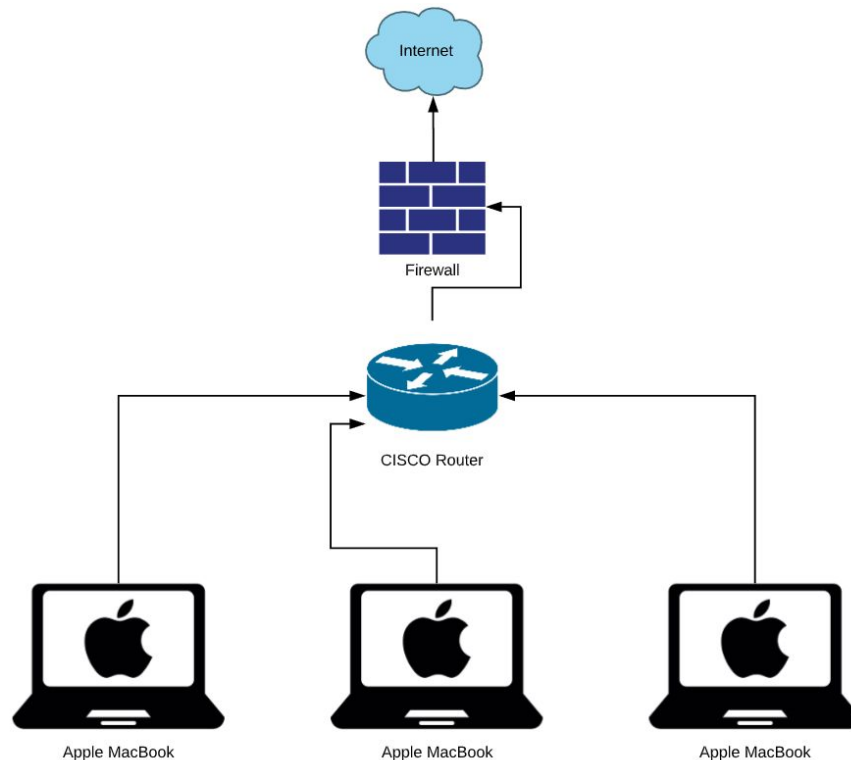
- **Common Critical Assets**

- Database Servers
- Domain Controllers
- DNS Servers
- Web Applications
- Remote Access Infrastructure/VPN
- Mail Servers

Vulnerability Assessment Example

BlueKeep CVSS 3.0 = **9.8 Critical**

Overall Risk Score = **1.0 Low**



















Continuous Vulnerability Management

 **CIS Controls™ • CIS Control 3** *This is a basic Control*

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

CIS Control 3: Continuous Vulnerability Management

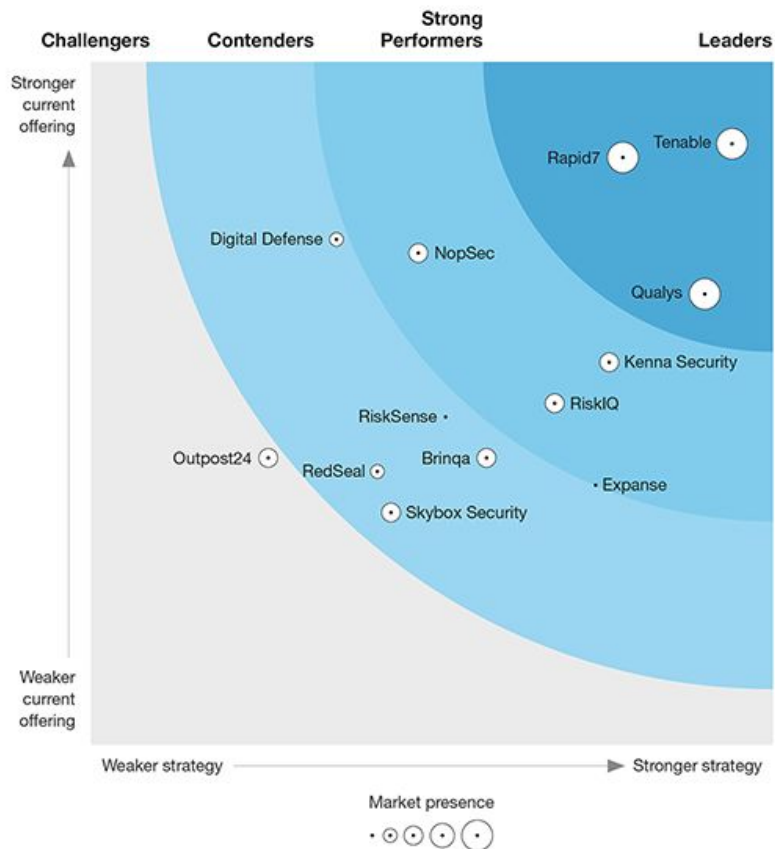
Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.			
3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.			
3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.			
3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			
3.6	Applications	Respond	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.			
3.7	Applications	Respond	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.			



How do you perform a vulnerability scan?

Vulnerability Risk Management

Q4 2019



What are the benefits of conducting a vulnerability scan?

- Identifying CVE vulnerabilities/misconfigurations
 - Open ports
 - Default accounts and password
 - Missing patches
 - EOL
- Passively testing security controls
 - Configuration audit
- Identifying a lack of security controls
 - End-Point Management
 - Patch management
 - Host-discovery
- Cybersecurity Compliance
 - PCI DSS, NIST, HIPAA

Types of Vulnerability Scans

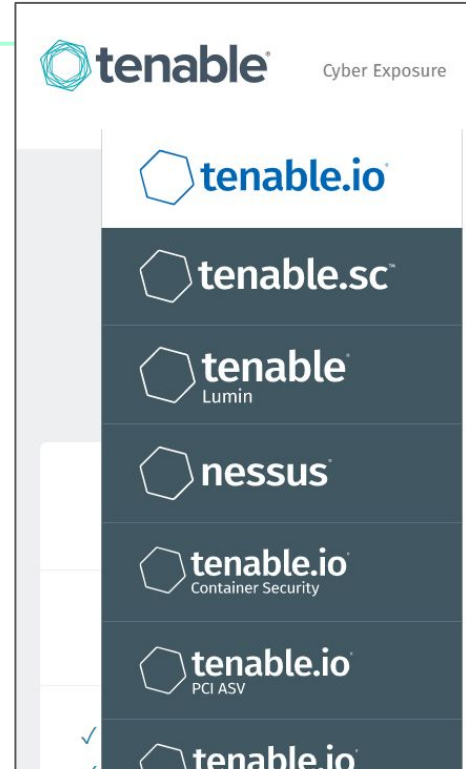
Credentialed	Non-credentialed
<ul style="list-style-type: none">• Authenticated• Require the user's credentials• Uncovers more vulnerabilities• Less false-positives• Longer configuration time	<ul style="list-style-type: none">• Non-Authenticated• Do not require the user's credentials• Many false-positives• Shorter configuration time• Usually done in penetration test

- Internal Vs. External Scanning
- Application Scanning
- PCI DSS Scans

What is Tenable Nessus?

- Nessus is a vulnerability scanner sold by Tenable Security.
- Nessus provide many different types of vulnerability scanners: cloud-based, agent-based, client-based, and essentials.

<https://www.tenable.com/plugins/nessus/125313>



45,000+
CVEs

100,000+
Plugins

100+
new plugins
released weekly

Tenable Nessus Features

Scan Templates

[← Back to Scans](#)

Scanner

Search Library



Advanced Dynamic Scan

Configure a dynamic plugin scan without recommendations.



Advanced Scan

Configure a scan without using any recommendations.



Audit Cloud Infrastructure

Audit the configuration of third-party cloud services.



Badlock Detection

Remote and local checks for CVE-2016-2118 and CVE-2016-0128.



Bash Shellshock Detection

Remote and local checks for CVE-2014-6271 and CVE-2014-7169.



Basic Network Scan

A full system scan suitable for any host.



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.



DROWN Detection

Remote checks for CVE-2016-0800.



Host Discovery

A simple scan to discover live hosts and open ports.



Intel AMT Security Bypass

Remote and local checks for CVE-2017-5689.



Internal PCI Network Scan

Perform an internal PCI DSS (11.2.1) vulnerability scan.



Malware Scan

Scan for malware on Windows and Unix systems.



MDM Config Audit

Audit the configuration of mobile device managers.



Mobile Device Scan

Assess mobile devices via Microsoft Exchange or an MDM.



Offline Config Audit

Audit the configuration of network devices.



PCI Quarterly External Scan

Approved for quarterly external scanning as required by PCI.



Policy Compliance Auditing

Audit system configurations against a known baseline.



SCAP and OVAL Auditing

Audit systems using SCAP and OVAL definitions.



Shadow Brokers Scan

Scan for vulnerabilities disclosed in the Shadow Brokers leaks.



Spectre and Meltdown

Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.



WannaCry Ransomware

Remote and local checks for MS17-010.



Web Application Tests

Scan for published and unknown web vulnerabilities.