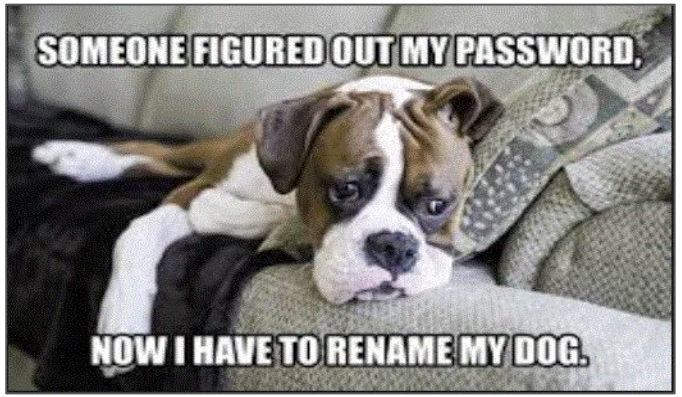
Vulnerability Management

Spring 2020

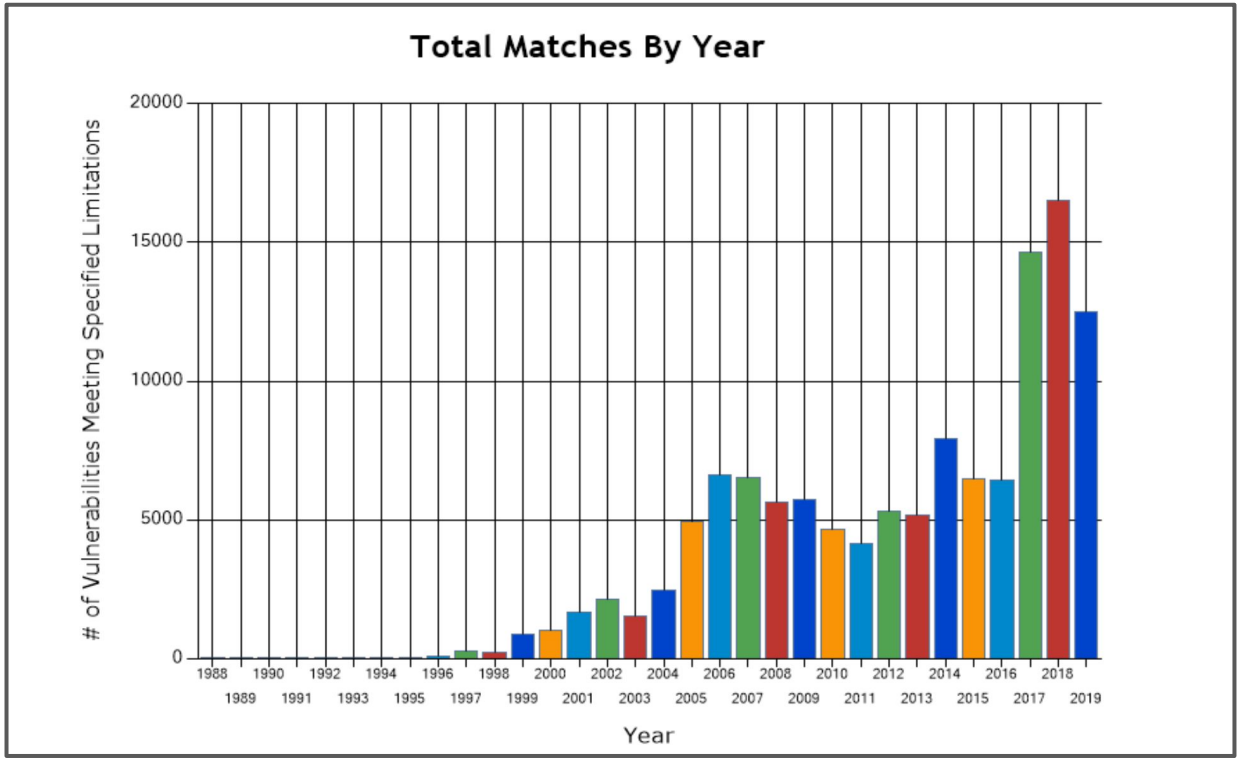
Jay Chen

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

- Network Vulnerability
- Application Vulnerability
- Misconfigured Server (Open Ports)
- Unsupported Operating System (EOL)
- Outdated Applications
- Default Credentials

Vulnerability Example: BlueKeep

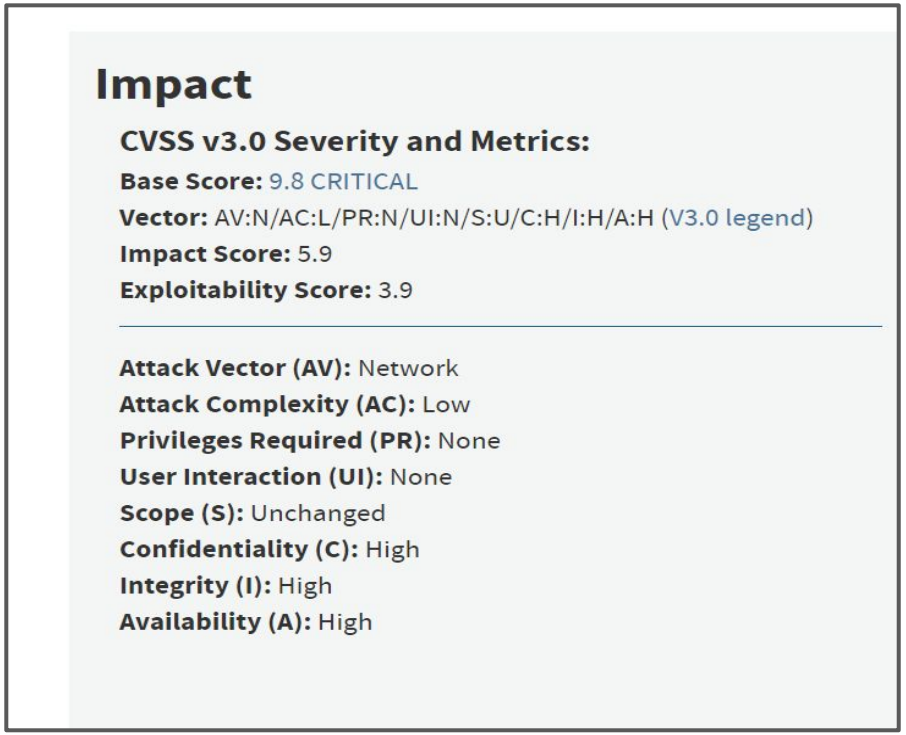
- BlueKeep (CVE-2019-0708)
- https://nvd.nist.gov/vuln/detail/CVE-2019-0708
- https://www.rapid7.com/db/?type=metasploit

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

Blue Keep Example



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

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=(AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C)

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

Continuous Vulnerability Management

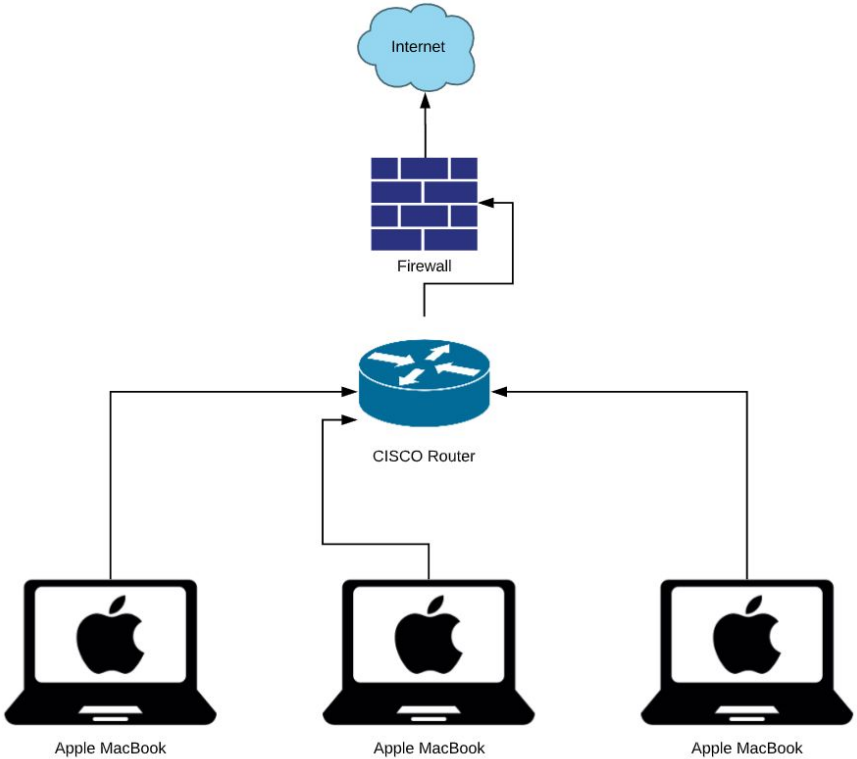
CIS Controls™ • CIS Control 3 *This is a basic Control*

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

Vulnerability Assessment Example

BlueKeep CVSS 3.0 = 9.8 Critical

Overall Risk Score = 1.0 Low



How do you perform a vulnerability scan?

tenable®

Qualys®

RAPID7

What are the benefits of conducting a vulnerability scan?

- Identifying CVE vulnerabilities/misconfigurations
  - Open ports
  - Default accounts and password
  - Default passwords
  - EOL

- Passively testing security controls
  - Configuration audit

- Identifying lack of security controls
  - Anti-Virus
  - Patch management
  - Host-discovery

Types of Vulnerability Scans

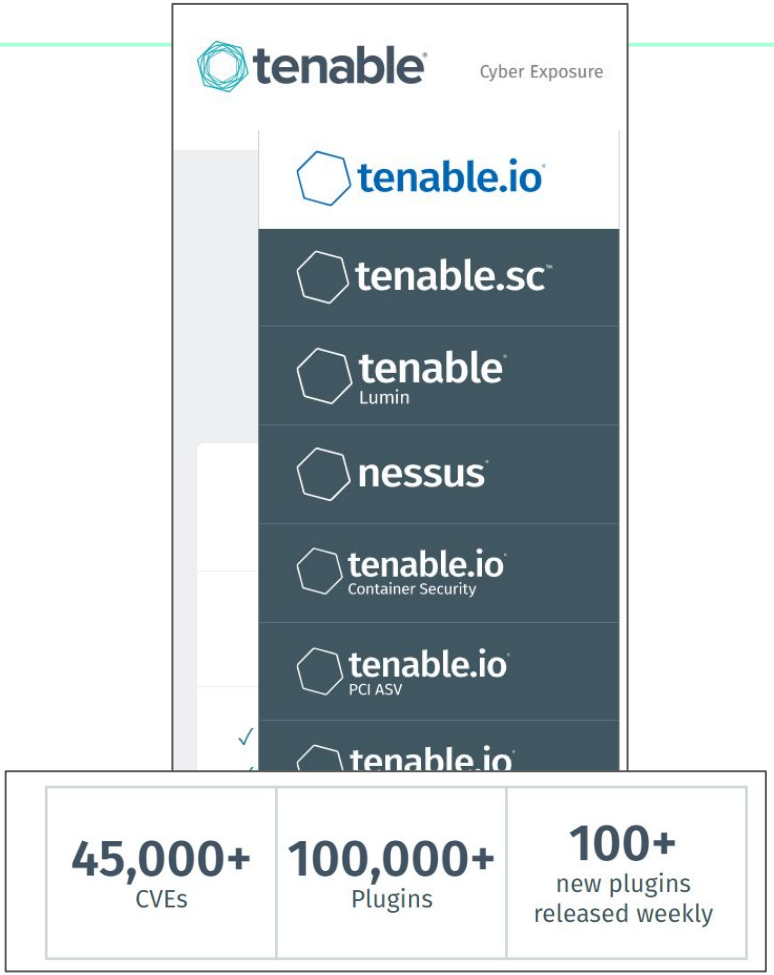
Credentialed	Non-credentialed
• Authenticated • Require the user's credentials • Uncovers more vulnerabilities • Less false-positives • Longer configuration time	• Non-Authenticated • Do not require the user's credentials • Many false-positives • Shorter configuration time • Usually done in penetration 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



Tenable Nessus Features