BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

BITS Pilani
Pilani Campus

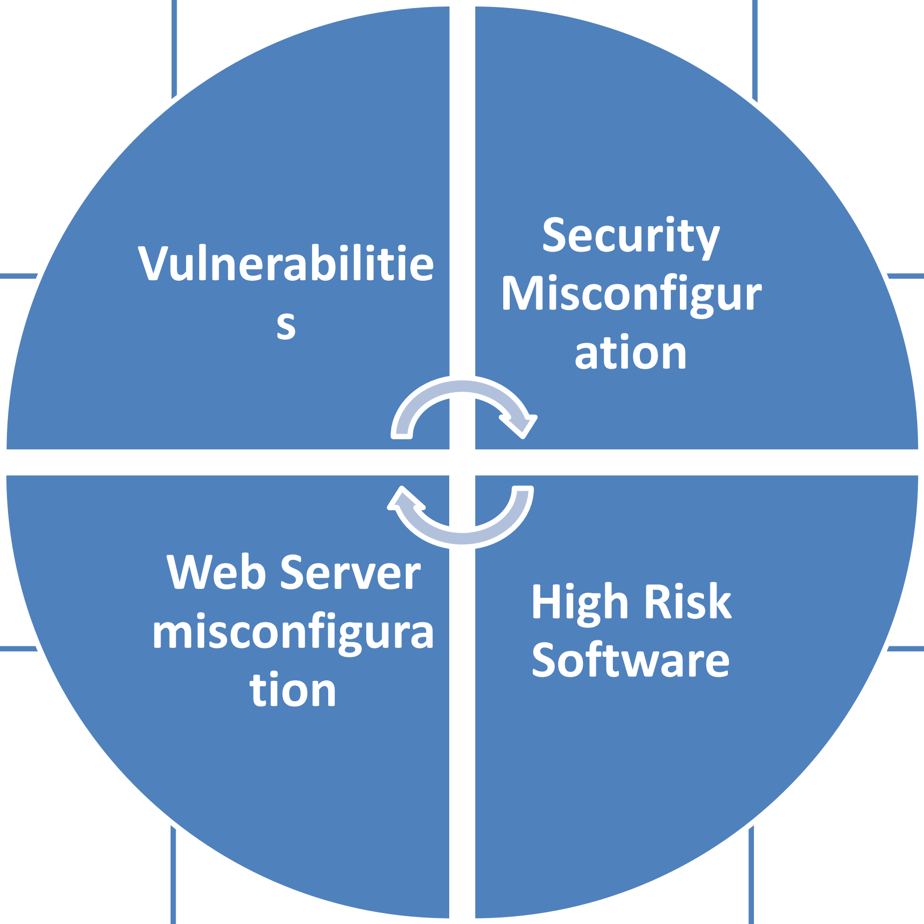
SSZG575: Vulnerabilities Assessment
Session No: 03

Agenda

- Vulnerability Identification
- Vulnerability Assessment
- Use cases
  - Vulnerability database listing
  - Vulnerability assessment video - Nessus
  - Password cracking video – Cane and Abel

Introduction

360 Degree View of Security Exposure



Vulnerabilities

- OS Vulnerabilities
- Third party Vulnerabilities
- Zero Day Vulnerabilities

Security Misconfiguration

- Default credentials
- Firewall misconfigurations
- Unused users and groups
- Elevated privileges
- Open shares

Web Server misconfiguration

- DDoS related misconfigurations
- UNused web pages
- Misconfigured HTTP headers and options
- Directory traversal
- Expired SSL/TLS
- Cross-site scripting

High Risk Software

- End-of-life software
- Remote desktop sharing software
- Peer-to-peer software

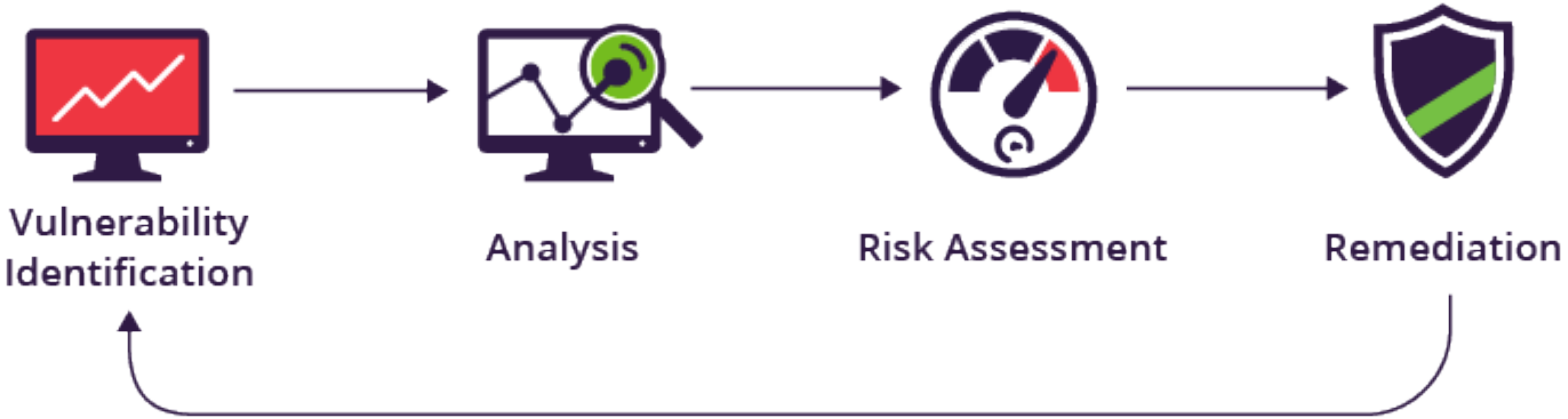
What is a Vulnerability Assessment?

- A vulnerability assessment is a systematic review of security weaknesses in an information system.
- Evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.
- Threats that can be prevented by vulnerability assessment are:
  - SQL injection, XSS and other code injection attacks.
  - Escalation of privileges due to faulty authentication mechanisms.
  - Insecure defaults – software that ships with insecure settings, such as a guessable admin password
- VA is process of identifying, quantifying, and prioritizing (ranking) the vulnerabilities in a system

Types of Vulnerability Assessment

- **Host Assessment:** The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
- **Network and Wireless Assessment:** The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.
- **Database Assessment:** The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization’s infrastructure.
- **Application Scans:** The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

Vulnerability Assessment Process



- Vulnerability Identification
- Analysis
- Risk Assessment
- Remediation

Vulnerability Identification

- How each of the threats that are possible or likely could be perpetrated, and list the organization’s assets and their vulnerabilities
- The objective of this step is to draft a comprehensive list of an application’s vulnerabilities.
- Security analysts test the security health of applications, servers or other systems by scanning them with automated tools, or testing and evaluating them manually.
- Analysts also rely on vulnerability databases, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses.

Vulnerability Identification

- **Methodology for identifying vulnerabilities**
  - Start with commonly available vulnerability lists.
  - Work with the system owners or other individuals with knowledge of the system or organization, start to identify the vulnerabilities that apply to the system.
  - Specific vulnerabilities can be found by reviewing vendor web sites and public vulnerability archives
    - Common Vulnerabilities and Exposures (CVE - http://cve.mitre.org)
    - National Vulnerability Database (NVD - http://nvd.nist.gov)

Vulnerability Databases

Spokeo – Social Data aggregator:	www.spokeo.com
Common Vulnerabilities and Exposures (CVE):	http://cve.mitre.org
National Vulnerability Database (NVD):	http://nvd.nist.gov
NVD Full Listing:	https://nvd.nist.gov/vuln/full-listing

Vulnerability Analysis

- The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one.
- It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability.
  - For example, the root cause of a vulnerability could be an old version of an open source library.
  - This provides a clear path for remediation – upgrading the library.

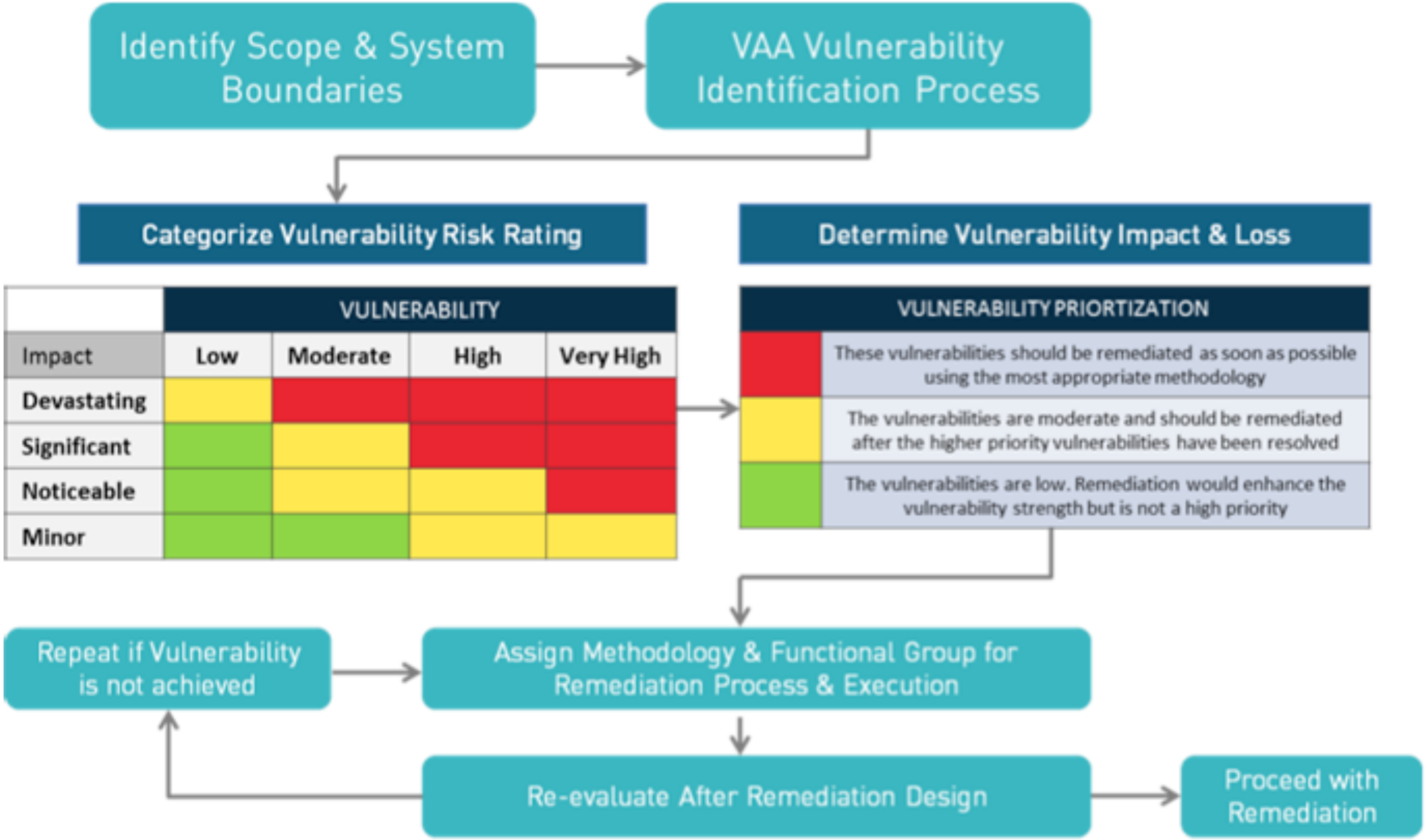
Risk Assessment

- The objective of this step is the prioritizing of vulnerabilities.
- Security analysts assign a rank or severity score to each vulnerability, based on such factors as:
  - Which systems are affected.
  - What data is at risk.
  - Which business functions are at risk.
  - Ease of attack or compromise.
  - Severity of an attack.
  - Potential damage as a result of the vulnerability.

Vulnerability Remediation

- The objective of this step is the closing of security gaps.
- It’s a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.
- Specific remediation steps include:
  - Introduction of new security procedures, measures or tools.
  - Update of operational or configuration changes.
  - Development and implementation of a vulnerability patch.
- Vulnerability assessment is an on-going activity - repeat it at regular intervals (recommended once in a year).
- It is also critical to foster cooperation between security, operation and development teams – a process known as DevOps

Vulnerability Assessment Process Flow



Identify Scope & System Boundaries

VAA Vulnerability Identification Process

Categorize Vulnerability Risk Rating

	VULNERABILITY			
Impact	Low	Moderate	High	Very High
Devastating	🟨	🟥	🟥	🟥
Significant	🟩	🟨	🟥	🟥
Noticeable	🟩	🟨	🟨	🟥
Minor	🟩	🟩	🟨	🟨

Determine Vulnerability Impact & Loss

VULNERABILITY PRIORTIZATION	
🟥	These vulnerabilities should be remediated as soon as possible using the most appropriate methodology
🟨	The vulnerabilities are moderate and should be remediated after the higher priority vulnerabilities have been resolved
🟩	The vulnerabilities are low. Remediation would enhance the vulnerability strength but is not a high priority

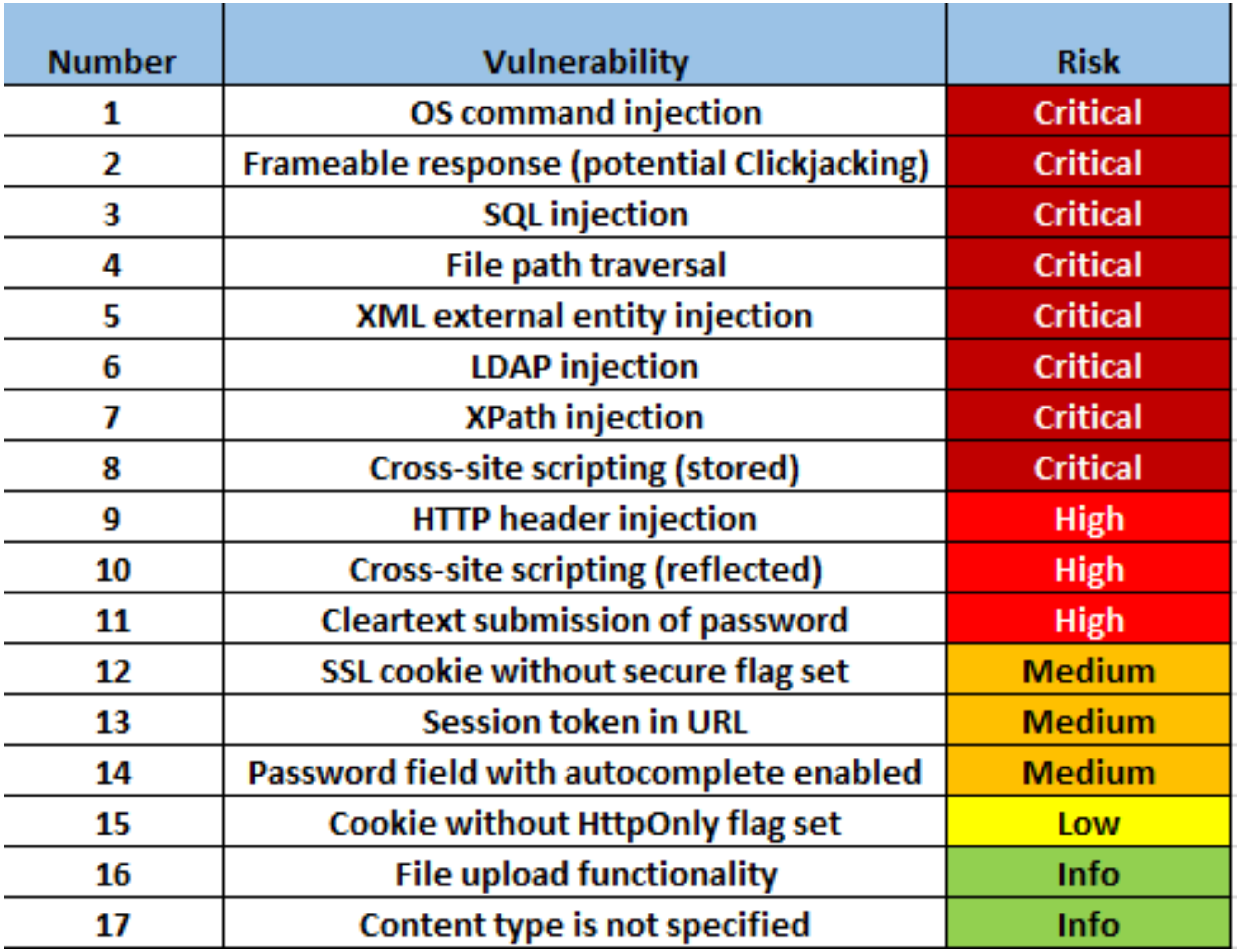
Assign Methodology & Functional Group for Remediation Process & Execution

Repeat if Vulnerability is not achieved

Re-evaluate After Remediation Design

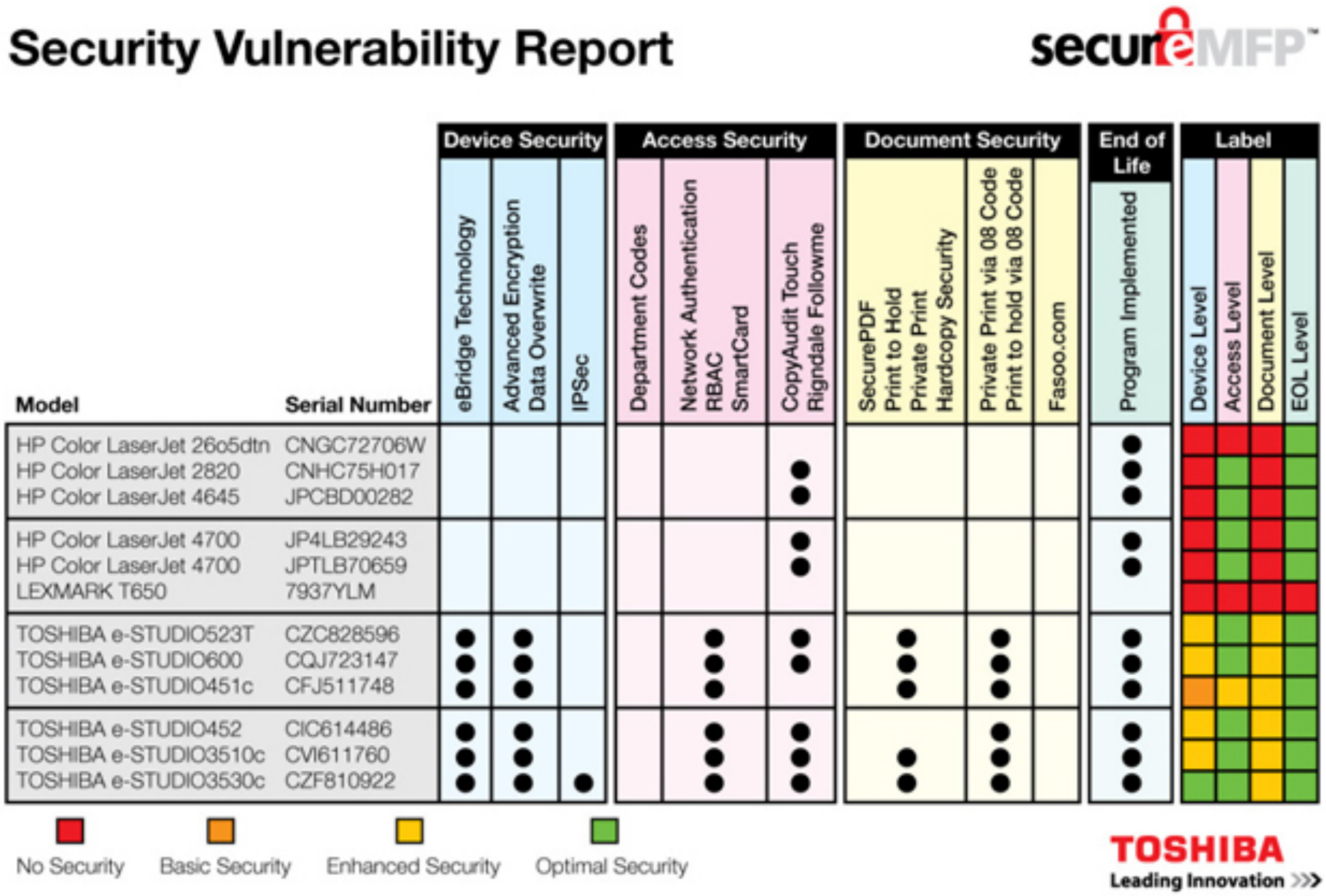
Proceed with Remediation

Vulnerability Report Example



Number	Vulnerability	Risk
1	OS command injection	Critical
2	Frameable response (potential Clickjacking)	Critical
3	SQL injection	Critical
4	File path traversal	Critical
5	XML external entity injection	Critical
6	LDAP injection	Critical
7	XPath injection	Critical
8	Cross-site scripting (stored)	Critical
9	HTTP header injection	High
10	Cross-site scripting (reflected)	High
11	Cleartext submission of password	High
12	SSL cookie without secure flag set	Medium
13	Session token in URL	Medium
14	Password field with autocomplete enabled	Medium
15	Cookie without HttpOnly flag set	Low
16	File upload functionality	Info
17	Content type is not specified	Info

Vulnerability Report Example



Security Vulnerability Report

secureMFP™

		Device Security			Access Security			Document Security			End of Life	Label			
Model	Serial Number	eBridge Technology	Advanced Encryption Data Overwrite	IPSec	Department Codes	Network Authentication RBAC SmartCard	CopyAudit Touch Rigndale Followme	SecurePDF Print to Hold Private Print Hardcopy Security	Private Print via 08 Code Print to hold via 08 Code	Fasoo.com	Program Implemented	Device Level	Access Level	Document Level	EOL Level
HP Color LaserJet 26o5dtn	CNGC72706W										●	🟥	🟥	🟥	🟩
HP Color LaserJet 2820	CNHC75H017						●				●	🟥	🟩	🟥	🟩
HP Color LaserJet 4645	JPCBD00282						●				●	🟥	🟩	🟥	🟩
HP Color LaserJet 4700	JP4LB29243						●				●	🟥	🟩	🟥	🟩
HP Color LaserJet 4700	JPTLB70659						●				●	🟥	🟩	🟥	🟩
LEXMARK T650	7937YLM											🟥	🟥	🟥	🟥
TOSHIBA e-STUDIO523T	CZC828596	●	●			●	●	●	●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO600	CQJ723147	●	●			●	●	●	●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO451c	CFJ511748	●	●			●		●	●		●	🟧	🟨	🟨	🟩
TOSHIBA e-STUDIO452	CIC614486	●	●			●	●		●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO3510c	CVI611760	●	●			●	●	●	●		●	🟨	🟩	🟨	🟩
TOSHIBA e-STUDIO3530c	CZF810922	●	●	●		●	●	●	●		●	🟩	🟩	🟨	🟩

🟥 No Security 🟧 Basic Security 🟨 Enhanced Security 🟩 Optimal Security

TOSHIBA
Leading Innovation >>>

Vulnerability Assessment Tools

- Vulnerability assessment tools are designed to automatically scan for new and existing threats that can target your application.
- Types of tools include:
  - Web application scanners that test and simulate known attack patterns.
  - Protocol scanners that search for vulnerable protocols, ports and network services.
  - Network scanners that help visualize networks and discover warning signals like stray IP addresses, spoofed packets and suspicious packet generation from a single IP address.
- Recommended to schedule regular, automated scans of all critical IT systems.
- Output of these scans must be fed into the organization’s ongoing vulnerability assessment process/register.

Vulnerability Assessment Tools

- Popular open source tools are:
  - OpenVAS - by Greenbone Networks
  - Nexpose or InsightVM (cloud-based) – by Rapid7
  - Retina CS Community – by BeyondTrust
  - Burp Suite Community Edition - by PortSwigger
  - Nikto - by Netsparker
  - OWASP Zed Attack Proxy (ZAP)
- Popular Licensed tools are:
  - Acunetix
  - beSecure (AVDS)
  - Comodo HackerProof
  - Intruder
  - Netsparker
  - Tenable Nessus Professional
  - Tripwire IP360

Vulnerability Assessment Actions

- Vulnerability assessment
- Patch management
- Security configuration management
- Web server hardening
- High risk software audit
- Zero day vulnerability mitigation

Vulnerability Assessment Advantages

- Clearly defined scope
  - Which systems are evaluated
  - What potential problems are evaluated
- Identifies most common technical issues
- Cheapest of the assessment options
- Repeatable and quantitative

Vulnerability Assessment Disadvantages

- Can identify a lot of issues
- Often lacks contextual risk information
  - Generic risk rankings
  - May not indicate the severity in *your* environment
- May not include expert advice/involvement

Recommended Prioritization

- Internal vulnerability assessment
- External vulnerability assessment
- Security assessment
- Penetration test

Kali Linux Overview

- Kali Linux is a Debian based Linux distribution aimed at advanced Penetration Testing and Security Auditing.
- Kali Linux contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
- Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

Kali Linux Overview (kali.org)

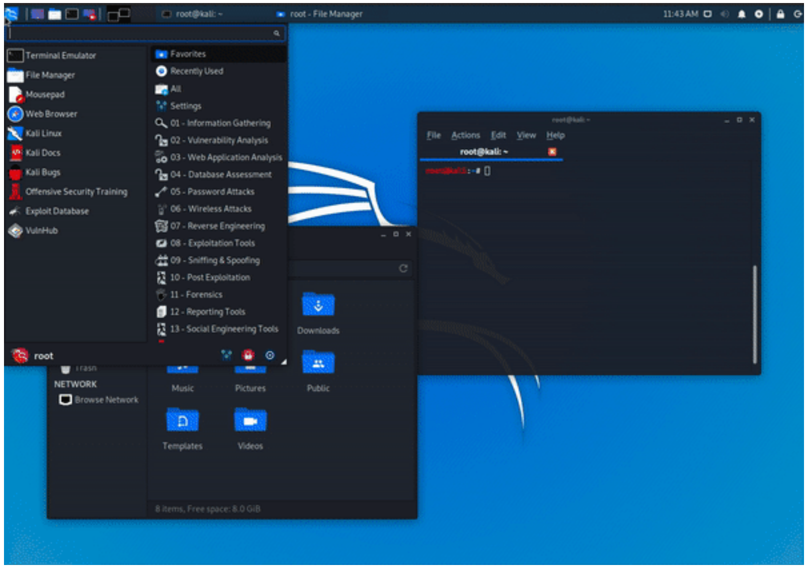
- Over 600 penetration testing tools included
- Open source GIT tree
- FHS (Filesystem Hierarchy Standard) compliant
- Wide ranging wireless device support
- Custom kernel patched for injection
- Secure development environment
- Multi-lingual support
- GPG signed packages and repositories
- Highly customizable
- ARMEL and ARMHF support

What is different about Kali?

- Kali Linux is specifically geared to meet the requirements of professional penetration testing and security auditing. To achieve this, several core changes have been implemented in Kali Linux which reflect these needs:
  - **Network services disabled by default:** Kali Linux contains systemd hooks that disable network services by default. These hooks allow to install various services on Kali Linux, while ensuring that the distribution remains secure by default, no matter what packages are installed. Additional services such as Bluetooth are also blacklisted by default.
  - **Custom Linux kernel:** Kali Linux uses an upstream kernel, patched for wireless injection.
  - **A minimal and trusted set of repositories:** Maintaining the integrity of the Kali system is absolutely key hence the set of upstream software sources which Kali uses is kept to an absolute minimum. Many new Kali users are tempted to add additional repositories to their **sources.list**, but doing so runs a very serious risk of breaking Kali Linux installation.

Kali Undercover

- **Kali Undercover** is a set of scripts that changes the look and feel of your Kali Linux desktop environment to **Windows 10** desktop environment, like *magic*.
- It was released with Kali Linux 2019.4 with an important concept in mind, *to* hide in plain sight.
- Toggle Command: *kali-undercover*



```
root@kali:~# 
```

Frequently Used Kali Commands

pwd	Displays present working directory
ls	Lists directories and files in current directory
cd	Change current working directory
grep <keywork> <filename>	To find a keyword in file
mkdir <directory name>	Create a new directory
rmdir <directory name>	Remove a directory
mv <source> <destination>	To move a file
cp <source> <destination>	To copy a file
touch <filename>>	To create a new file
man <command name>	To display manual of a command
ping <ip address or DNS name>	To check the internet connection or to check whether the host is active or not
ipconfig	To display network interface details

Frequently Used Kali Commands…

wget <link to file>	To download a file
sudo apt install <package_name>	To install a package
sudo apt remove <package_name>	To remove a package
sudo apt-get upgrade	To upgrade packages in the system
sudo apt-get update	To fetch packages updates
whoami	To get the current username
sudo su	To change the current user to superuser or root
echo " Hello world!!! "	To print to terminal

Password Cracking Techniques

- Brute-force attack
- Dictionary attack
- Rainbow Table attack
- Traffic interception
- Password spraying
- Phishing
- Social Engineering
- Malware
- Shoulder surfing

Kali Password Cracking Tool: Crunch

- In order to crack a password or a hash, we need to have a good wordlist which could break the password.
- Kali Linux tool Crunch generates a good wordlist.
- It is used to generate custom keywords based on wordlists.
- It generates a wordlist with permutation and combination.
- We could use some specific patterns and symbols to generate a wordlist.
- Enter following command in the terminal: **crunch**

Kali Password Cracking Tool: RainbowCrack

- Rainbow crack is a tool that uses the time-memory trade-off technique in order to crack hashes of passwords.
- It uses rainbow tables in order to crack hashes of passwords.
- It generates all the possible plaintexts and computes and stores the hashes respectively.
- It matches hash with the hashes of all the words in a wordlist.
- When it finds the matching hashes, it results in cracked password.
- To use RainbowCrack, enter the following command in the terminal: **rcrack**

Vulnerability Tool Demo

Intruder VA Tool Video:

https://www.intruder.io/?utm_source=referral&utm_campaign=comparitech-vulnerability-assessment-penetration-testing-tools

Nessus Demo: https://www.youtube.com/watch?v=LByE7bS6J4M

Password Cracking: Cain and Abel

Caine and Abel video:

https://www.youtube.com/watch?v=RyQL9AdxHqY

Vulnerability Useful Links

Spokeo – Social Data aggregator: www.spokeo.com

Common Vulnerabilities and Exposures (CVE): http://cve.mitre.org

National Vulnerability Database (NVD): http://nvd.nist.gov

NVD Full Listing: https://nvd.nist.gov/vuln/full-listing

Thank You