BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Vulnerability Assessment
Session: 03

Agenda

- What is Vulnerability Assessment?
- Vulnerability Assessment Process
  - Vulnerability Identification
  - Analysis
  - Risk Assessment
  - Remedian
- Vulnerability Database Listing
- Kali Linux Overview
- Password Cracking Tools – Crunch & RainbowCrack
- Nmap tool

Security Exposure View

Vulnerabilities

- OS Vulnerabilities
- Third party Vulnerabilities
- Zero Day Vulnerabilities

Security Misconfiguration

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

High Risk Software

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

Web Server Misconfiguration

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

As an Ethical Hacker it's important to understand the vulnerability scenario and advise/design appropriate remedial solutions.

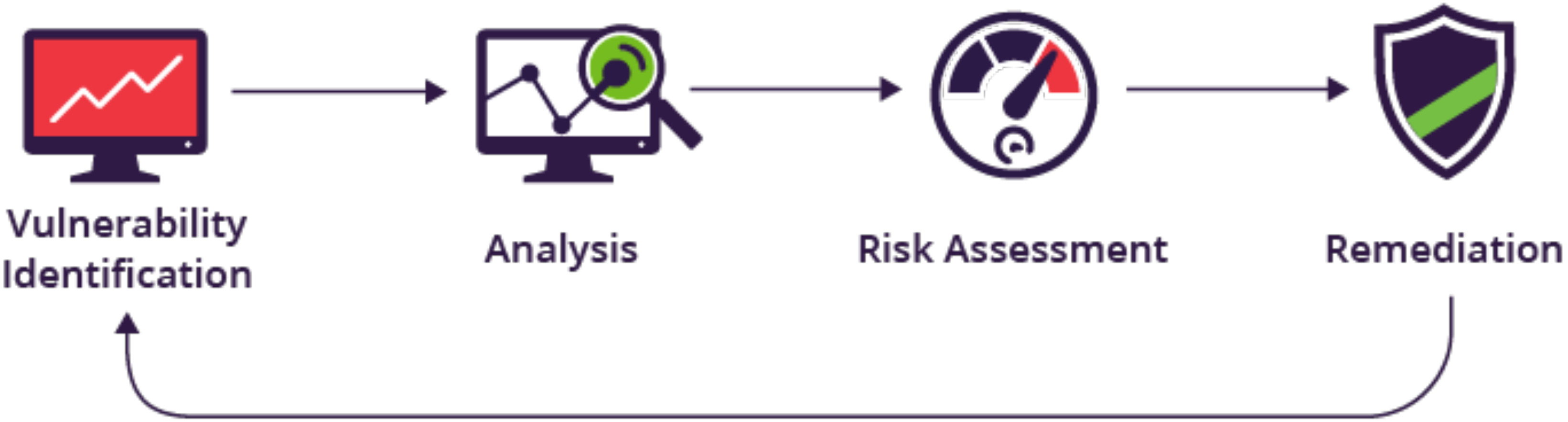
What is a Vulnerability Assessment?

- Vulnerability assessment is a systematic review of security weaknesses in an information system.
- VA is the process of identifying, quantifying, and prioritizing (ranking) the vulnerabilities in a system.
- VA exercise:
  - Evaluates if the system is susceptible to any known vulnerabilities
  - Assigns severity levels to those vulnerabilities
  - Recommends remediation or mitigation, if required.
- 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

Vulnerability Assessment Types

Assessment Type	Description
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

- Objective of this step is to prepare a comprehensive list of IT assets (applications, servers, networks etc) and their vulnerabilities.
- Identify threats that are possible or likely could be perpetrated
- Process involves testing the security health of applications, servers and other systems by scanning them with automated tools or testing and evaluating them manually.
- Use vulnerability databases, vendor vulnerability notifications, asset management systems etc
- Use Threat Intelligence feeds to identify security weaknesses.

Vulnerability Identification Approach

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

Public Vulnerability Databases

Database	URL
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
Spokeo – Social Data aggregator	www.spokeo.com

Vulnerability Analysis

- Objective of this step is to identify the source and root cause of the vulnerabilities identified.
- Involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability.
  - Root cause of a vulnerability could be an old version of an open source library.
  - Provides a clear path for remediation – upgrading the library.

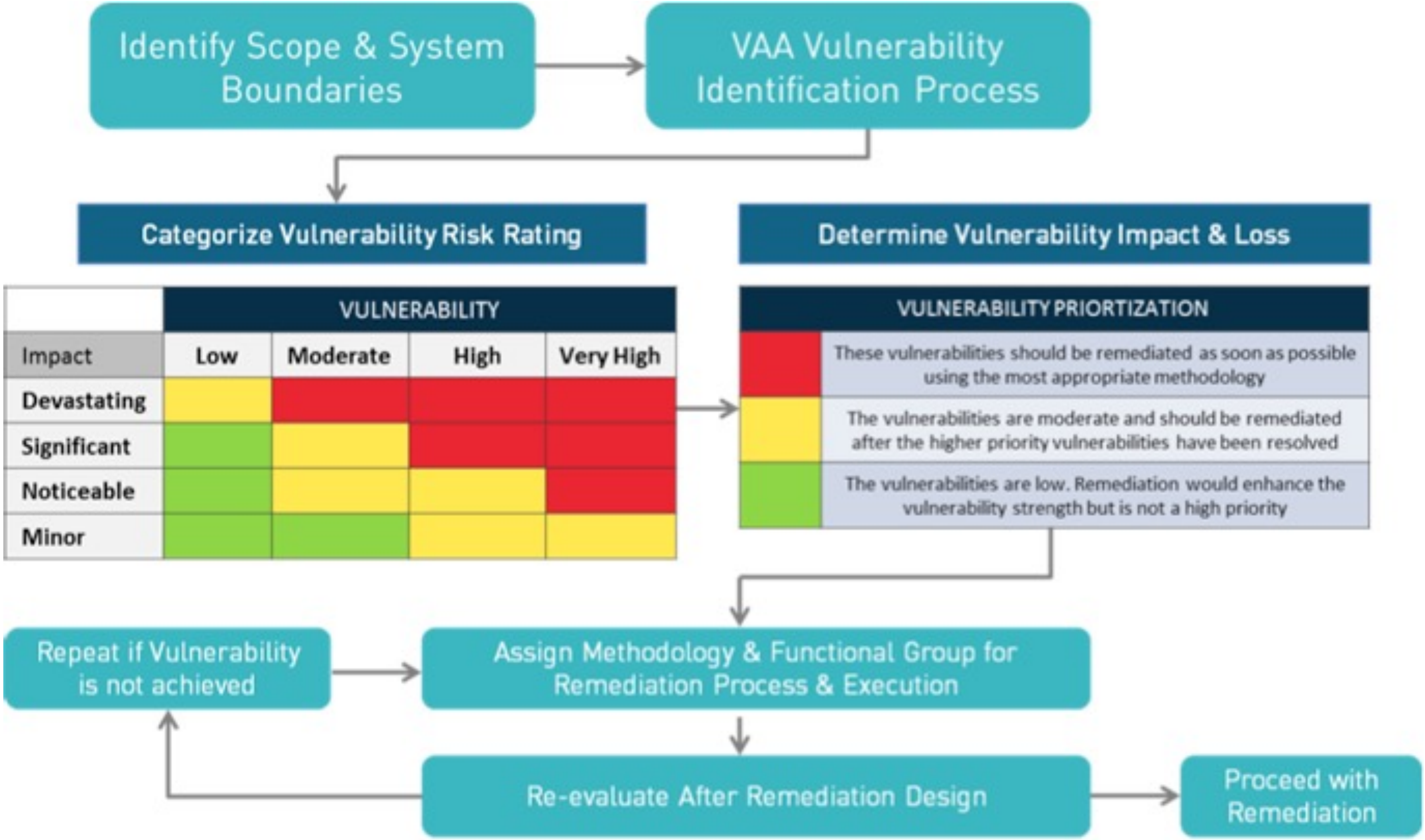
Risk Assessment

- Objective of this step to prioritize 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

- Objective of this step is to close the security gaps.
- Requires joint effort by security, development and operations teams
- Determine the most effective path for remediation or mitigation of each vulnerability.
- Remediation steps may 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 – to be repeated at regular intervals (recommended once in a year).
- Foster cooperation between security, operation and development teams (DevSecOps)

Vulnerability Assessment Process Flow



Identify Scope & System Boundaries

VAA Vulnerability Identification Process

Categorize Vulnerability Risk Rating

Determine Vulnerability Impact & Loss

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

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

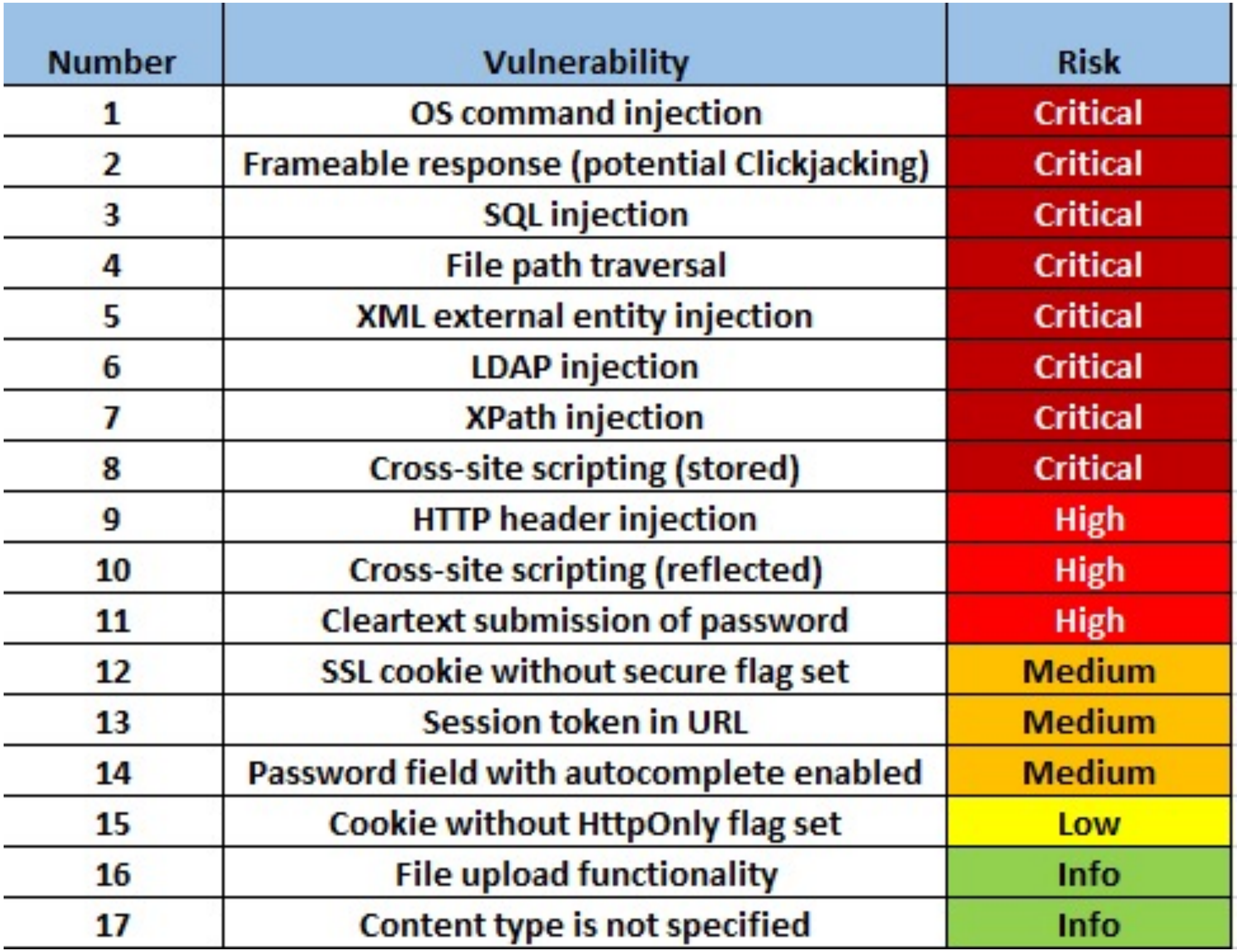
Repeat if Vulnerability is not achieved

Assign Methodology & Functional Group for Remediation Process & Execution

Re-evaluate After Remediation Design

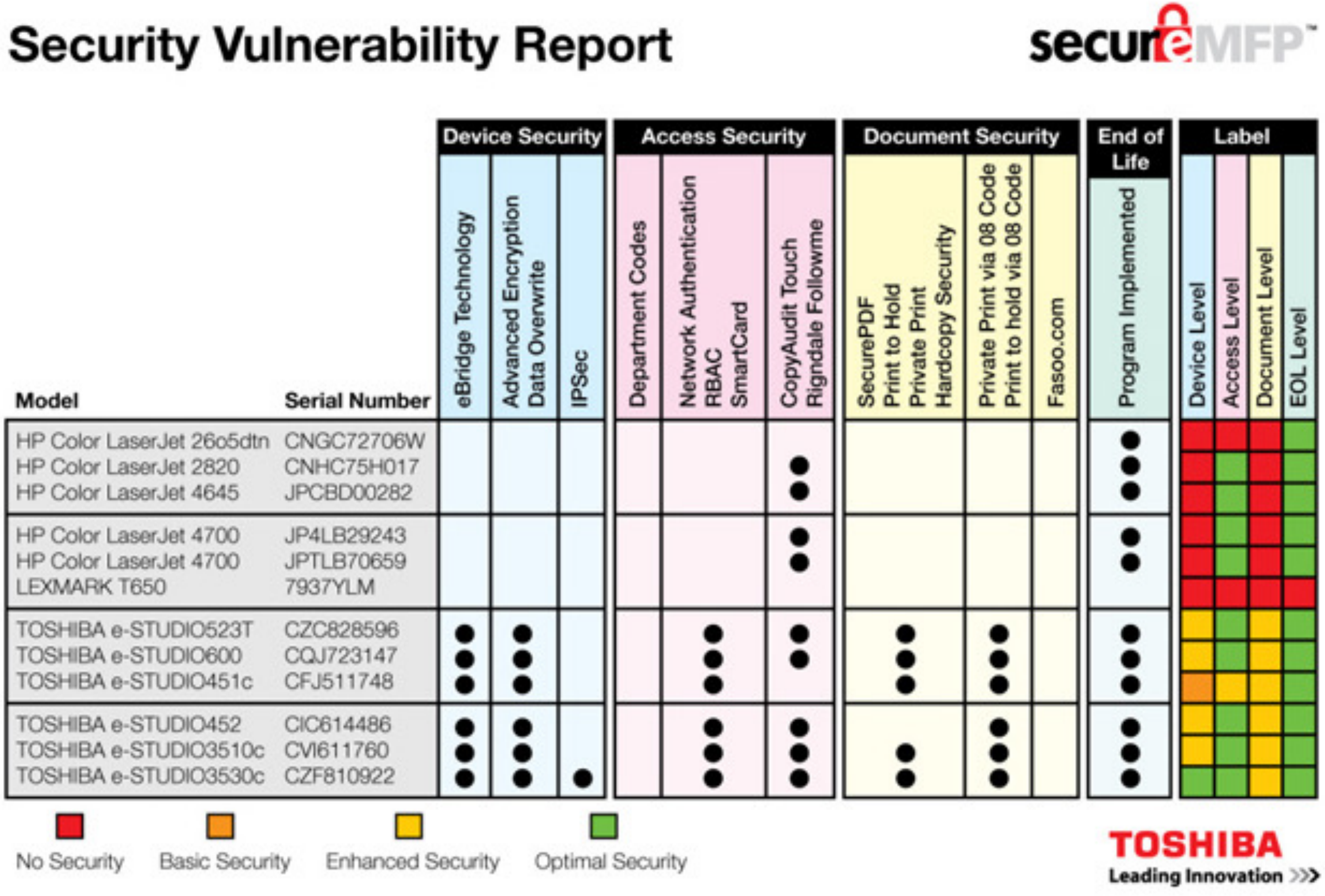
Proceed with Remediation

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™

Model	Serial Number	Device Security			Access Security			Document Security			End of Life	Label			
		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 IT systems.
- 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 register.

Popular Vulnerability Assessment Tools

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

Vulnerability Assessment Actions

- Vulnerability assessment remedial solution(s)
- Patch management
- Security configuration management
- Web server hardening
- High risk software audit
- Zero day vulnerability mitigation

Vulnerability Assessment Benefits

- Clear view of vulnerabilities and risks
  - Which systems are at risk
  - What potential problems exist
- What are common technical issues in current IT systems?
- Cheapest of the various assessment options
- Repeatable and quantitative information

Vulnerability Assessment Disadvantages

- Can identify a lot of issues – some could be false positive
- Often lacks contextual risk information
  - Generic risk rankings
  - May not indicate the severity in environment
- May not include expert advice/involvement

Recommended Roadmap for VA

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

Hacking Database

Shodan Database

- A search engine that can:
  - Identify a specific device, such as computer, router, server etc
  - Can specify a variety of filters, such as metadata from system banners.
- Example: You can search for a specific system, such as a Cisco 3850, running a version of software such as IOS Version 15.0(1)EX.
- URL Link: https://www.shodan.io

Google Hacking Database (GHDB)

- GHDB Exploit Database is maintained by **Offensive Security**.
- A non-profit project that is provided as a public service.
- A CVE compliant archive of public exploits and corresponding vulnerable software
- Developed for use by penetration testers and vulnerability researchers.
- A repository for exploits and proof-of-concepts rather than advisories
- A valuable resource for those who need actionable data right away.

Google Hacking Database (GHDB)

- A categorized index of Internet search engine queries designed to uncover interesting and usually sensitive information available publicly on the Internet.
- “Google Hacking” was popularized in 2000 by Johnny Long, a professional hacker,
  - He began cataloging these queries in a database known as the Google Hacking Database
  - He was supported by countless hours of community member effort, documented in the book ‘Google Hacking For Penetration Testers’
  - He coined the term “Googledork” to refer to “a foolish or inept person as revealed by Google“
  - Objective was to draw attention to the fact that this was not a “Google problem”
    - Result of an unintentional misconfiguration or a program installed by the user.

Google Hacking Database (GHDB)

- Google Hacking
  - Over time, the term “dork” became shorthand for a search query that located sensitive information
  - “dorks” were included with may web application vulnerability releases to show examples of vulnerable web sites.
  - After nearly a decade of hard work by the community, Johnny turned the GHDB over to **Offensive Security** in November 2010
  - Now maintained as an extension of the **Exploit Database**.

- Ref: https://www.exploit-db.com/google-hacking-database

Kali Linux

Kali Linux Overview

- Earlier known as **BackTrack Linux**
- Kali Linux is a Debian based Linux distribution aimed at advanced Penetration Testing and Security Auditing.
- Kali Linux contains several hundred tools
  - Geared towards various information security tasks
  - Can be sued for Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
- Kali Linux is developed, funded and maintained by **Offensive Security**

- Ref: Kali.org

Kali Linux Features

- 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
- Multilingual support
- Highly customizable
- ARMEL (Advance RISC Machines EABI – older processor) and ARMHF (ARM Hard Float – newer processor) support – Raspberry Pi & BeagleBone Black
- Industry standard for open source penetration testing platform

Kali Linux Special Features

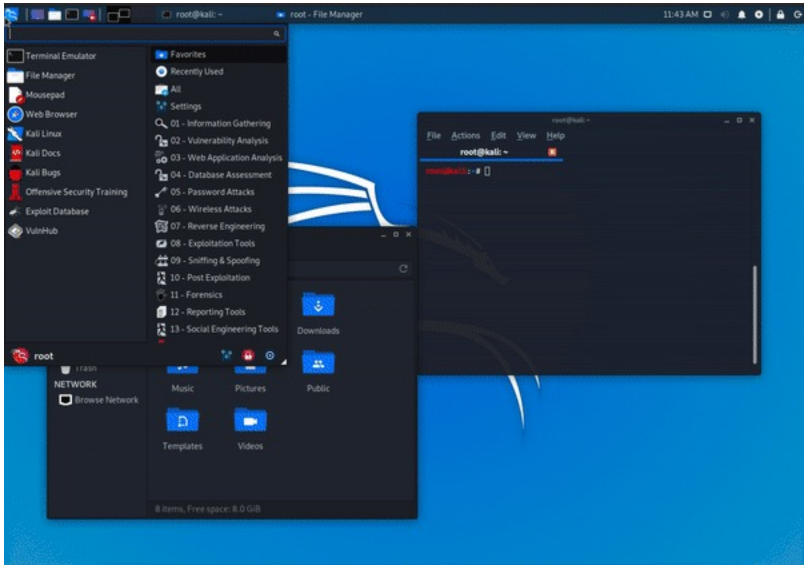
- Full customization of Kali ISO
- Live USB boot
- Kali Undercover
- Win-KeX
- Kali NetHunter
- Kali Everywhere
- Kali ARM

Customization of Kali ISO

- Use of metapackages **optimized** for specific needs of a security professional
- Highly accessible **ISO customization process** for an optimized version of Kali for specific needs.
- Kali Linux is heavily integrated with live-build, allowing high flexibility in customizing and tailoring every aspect of Kali Linux ISO images.
- Sample available with
  - Kali's **basic example build recipes**,
  - **Kali ISO of doom recipe**, - demonstrates the types and complexity of customizations possible
  - Build a self installing, reverse VPN auto-connecting, network bridging Kali image - for the perfect hardware backdoor.

Kali Undercover

- **Kali Undercover** is a set of scripts that changes the look and feel of Kali Linux desktop environment to **Windows 10** desktop environment, like *magic*.
- Released with Kali Linux 2019.4 with a concept in mind, *to* hide in plain sight.
- Helps to avoid shoulder surfing



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

Live USB Boot

- Allows to place Kali onto a USB device, and boot without touching the host operating system
  - Perfect also for any forensics work.
- With **persistence volume(s)** there is an option to pick what file system to use when Kali starts up allowing for files to be saved in between sessions, creating multiple profiles.
- Each **persistence volume can be encrypted** essential feature for security.
- Provides **LUKS nuke option**, allowing to quickly control the destruction of data.

Win-KeX

- Provides a Kali Desktop Experience for Windows Subsystem for Linux (WSL)
- **Window mode**: start a Kali Linux desktop in a dedicated window
- **Seamless mode**: share the Windows desktop between Windows and Kali apps and menus
- Sound support
- Unprivileged and Root session support
- Shared clipboard for cut and paste support between Kali Linux and Windows apps
- **Multi-session support:** root window & non-priv window & seamless sessions concurrently

Kali NetHunter

- Open-source Android penetration testing platform for Android devices
- Allowing for access to the Kali toolset from various supported Android devices
- Custom kernel that **supports 802.11 wireless injection** and preconfigured connect back VPN services
- Covers multiple items, such as a **ROM overlay** for multiple devices, **NetHunter App**, as well as **NetHunter App Store**.
- Can boot into a "**full desktop**" using chroot & containers, as well as "**Kali NetHunter Desktop Experience (KeX)**".

Kali Everywhere

- A version of Kali that supports multitude of devices:
  - ARM
  - Bare Metal
  - Cloud (AWS, Azure)
  - Containers (Docker, LXD)
  - Virtual Machines (VirtualBox, VMware)
  - WSL
  - and others

Kali ARM

- Supporting over a dozen different ARM devices and common hardware such as Raspberry Pi, Odroid, Beaglebone, and more.
- Offers **pre-generated images**, ready to be used as well as **build-scripts** to produce more.
- Very active in the ARM arena and constantly adding new interesting hardware to Kali repertoire.

What is different about Kali?

- Kali Linux is specifically designed to meet the requirements of professional penetration testing and security auditing.
- Core changes have been implemented in Kali Linux to support these needs:
  - **Network services disabled by default:** Kali Linux contains
    - systemd hooks that disable network services by default.
    - 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:** Kali Linux maintains the integrity by
    - Using absolute minimum set of upstream software
    - 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.

Frequently Used Kali Commands

Command	Command function
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

Frequently Used Kali Commands…

Command	Command function
ipconfig	To display network interface details
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

Password Cracking Tool: Crunch

- To crack a password or a hash, a good wordlist is required which could break the password.
- Kali Linux tool Crunch can be used to generate a wordlist.
  - Can generate custom keywords based on wordlists.
  - Can generates a wordlist with permutation and combination.
  - Can use specific patterns and symbols to generate a wordlist.
- Command to use Crunch on Kali: **crunch**

Password Cracking Tool: RainbowCrack

- Rainbow crack is a tool that uses the time-memory trade-off technique in order to crack hashes of passwords.
  - Uses rainbow tables in order to crack hashes of passwords.
  - Generates all the possible plaintexts and computes and stores the hashes respectively.
  - Matches hash with the hashes of all the words in a wordlist.
  - When it finds the matching hashes, it results in password crack.
- Command to use RainbowCrack on Kali: **rcrack**

Nmap: Overview

- Nmap is an open source tool, used to discover hosts and services on a computer network by sending packets and analyzing the retrieved responses.
- Nmap offers features for probing computer networks, including host discovery and service and operating system detection.
- Nmap can provide information on targets, including reverse DNS names, device types, and MAC addresses.
  - **Host discovery:** Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
  - **Port scanning:** Enumerating the open ports on target hosts.
  - **OS detection:** Determining the operating system and hardware characteristics of network devices.
  - **Version detection:** Interrogating network services on remote devices to determine the application name and version number.
  - Scriptable interaction with the target support using the Nmap Scripting Engine (NSE).

Nmap: Usage

- Audit the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Audit the security of a network by identifying new servers.
- Identify open ports on a target host in preparation for auditing.
- Prepare network inventory, network mapping, and maintenance and asset management.
- Generate traffic to hosts on a network, response analysis and response time measurement.
- Find and exploit vulnerabilities in a network.
- Make DNS queries and sub-domain search

Nmap: Basic Commands

Goal	Command	Example
Scan a Single Target	nmap [target]	nmap 192.168.0.1
Scan Multiple Targets	nmap [target1, target2, etc	nmap 192.168.0.1 192.168.0.2
Scan a Range of Hosts	nmap [range of ip addresses]	nmap 192.168.0.1-10
Scan an Entire Subnet	nmap [ip address/cdir]	nmap 192.168.0.1/24
Scan Random Hosts	nmap -iR [number]	nmap -iR 0
Excluding Targets from a Scan	nmap [targets] – exclude [targets]	nmap 192.168.0.1/24 –exclude 192.168.0.100, 192.168.0.200
Excluding Targets Using a List	nmap [targets] – excludefile [list.txt]	nmap 192.168.0.1/24 – excludefile notargets.txt
Perform an Aggressive Scan	nmap -A [target]	nmap -A 192.168.0.1
Scan an IPv6 Target	nmap -6 [target]	nmap -6 1aff:3c21:47b1:0000:0000:0000:0000:2afe

Nmap: Discovery Commands

Goal	Command	Example
Perform a Ping Only Scan	nmap -sP [target]	nmap -sP 192.168.0.1
Don’t Ping	nmap -PN [target]	nmap -PN 192.168.0.1
TCP SYN Ping	nmap -PS [target]	nmap -PS 192.168.0.1
TCP ACK Ping	nmap -PA [target]	nmap -PA 192.168.0.1
UDP Ping	nmap -PU [target]	nmap -PU 192.168.0.1
SCTP INIT Ping	nmap -PY [target]	nmap -PY 192.168.0.1
ICMP Echo Ping	nmap -PE [target]	nmap -PE 192.168.0.1
ICMP Timestamp Ping	nmap -PP [target]	nmap -PP 192.168.0.1
CMP Address Mask Ping	nmap -PM [target]	nmap -PM 192.168.0.1
IP Protocol Ping	nmap -PO [target]	nmap -PO 192.168.0.1

Nmap: ARP Commands

ARP Ping	**nmap -PR [target]**	**nmap -PR 192.168.0.1**
Traceroute	nmap –traceroute [target]	nmap –traceroute 192.168.0.1
Force Reverse DNS Resolution	nmap -R [target]	nmap -R 192.168.0.1
Disable Reverse DNS Resolution	nmap -n [target]	nmap -n 192.168.0.1
Alternative DNS Lookup	nmap –system-dns [target]	nmap –system-dns 192.168.0.1
Manually Specify DNS Server(s)	nmap –dns-servers [servers] [target]	nmap –dns-servers 201.56.212.54 192.168.0.1
Create a Host List	nmap -sL [targets]	nmap -sL 192.168.0.1/24

Nmap: Advance Scanning Commands

Goal	Command	Example
TCP SYN Scan	nmap -sS [target]	nmap -sS 192.168.0.1
TCP Connect Scan	nmap -sT [target]	nmap -sT 192.168.0.1
UDP Scan	nmap -sU [target]	nmap -sU 192.168.0.1
TCP NULL Scan	nmap -sN [target]	nmap -sN 192.168.0.1
TCP FIN Scan	nmap -sF [target]	nmap -sF 192.168.0.1
Xmas Scan	nmap -sX [target]	nmap -sX 192.168.0.1
TCP ACK Scan	nmap -sA [target]	nmap -sA 192.168.0.1
Custom TCP Scan	nmap –scanflags [flags] [target]	nmap –scanflags SYNFIN 192.168.0.1
IP Protocol Scan	nmap -sO [target]	nmap -sO 192.168.0.1
Send Raw Ethernet Packets	nmap –send-eth [target]	nmap –send-eth 192.168.0.1
Send IP Packets	nmap –send-ip [target]	nmap –send-ip 192.168.0.1

Nmap: Port Scanning Commands

Goal	Command	Example
Perform a Fast Scan	nmap -F [target]	nmap -F 192.168.0.1
Scan Specific Ports	nmap -p [port(s)] [target]	nmap -p 21-25,80,139,8080 192.168.1.1
Scan Ports by Name	nmap -p [port name(s)] [target]	nmap -p ftp,http* 192.168.0.1
Scan Ports by Protocol	nmap -sU -sT -p U:[ports],T:[ports] [target]	nmap -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.0.1
Scan All Ports	nmap -p '*' [target]	nmap -p '*' 192.168.0.1
Scan Top Ports	nmap –top-ports [number] [target]	nmap –top-ports 10 192.168.0.1
Perform a Sequential Port Scan	nmap -r [target]	nmap -r 192.168.0.1

Nmap: Version Detection Commands

Goal	Command	Example
Operating System Detection	nmap -O [target]	nmap -O 192.168.0.1
Submit TCP/IP Fingerprints	www.nmap.org/submit/	
Fingerprints		
Attempt to Guess an Unknown OS	nmap -O –osscan guess [target]	nmap -O –osscan-guess 192.168.0.1
Service Version Detection	nmap -sV [target]	nmap -sV 192.168.0.1
Troubleshooting Version Scans	nmap -sV –version trace [target]	nmap -sV –version-trace 192.168.0.1
Perform a RPC Scan	nmap -sR [target]	nmap -sR 192.168.0.1

Nmap: Firewall Evasion Commands

Goal	Command	Example
augment Packets	nmap -f [target]	nmap -f 192.168.0.1
pacify a Specific MTU	nmap –mtu [MTU] [target]	nmap –mtu 32 192.168.0.
Use a Decoy	nmap -D RND:[number] [target]	nmap -D RND:10 192.168.0.1
le Zombie Scan	nmap -sI [zombie] [target]	nmap -sI 192.168.0.38
Manually Specify a Source Port	nmap –source-port [port] [target]	nmap –source-port 10 192.168.0.1
Append Random Data	nmap –data-length [size] [target]	nmap –data-length 2 192.168.0.1
Randomize Target Scan Order	nmap –randomize-hosts [target]	nmap –randomize-ho 192.168.0.1-20
Spoof MAC Address	nmap –spoof-mac [MAC|0|vendor] [target]	nmap –spoof-mac Cis 192.168.0.1
Send Bad Checksums	nmap –badsum [target]	nmap –badsum 192.168.0.1

Tool Demo

A. Vulnerability Assessment:

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

B. Password Cracking:

Caine and Abel video: https://www.youtube.com/watch?v=RyQL9AdxHqY

Thank You