



# Hacking Tips & Tricks

**OWASP**

May 7, 2011

**M.Ananthakrishnan**  
**CEH LPT ECSA CCSA CPISI ITIL**  
**Manager – Infosec Governance**  
**Hexaware Technologies Limited**  
m.aananth@gmail.com  
+91 8939913933

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

**The OWASP Foundation**  
<http://www.owasp.org>

# Agenda

- Security Incidents
- Vulnerability Assessment
- Wireless Hacking
- Bluetooth Hacking
- Advance password hacking

# Cash is not the only motive



A99 Operation Empire State Rebellion - Communication #  
by AmpedStatus

#OpESR

## APT – What is it?

A human being or organization, who operates a campaign of intellectual property theft using cyber-methods – Malware, malware, malware



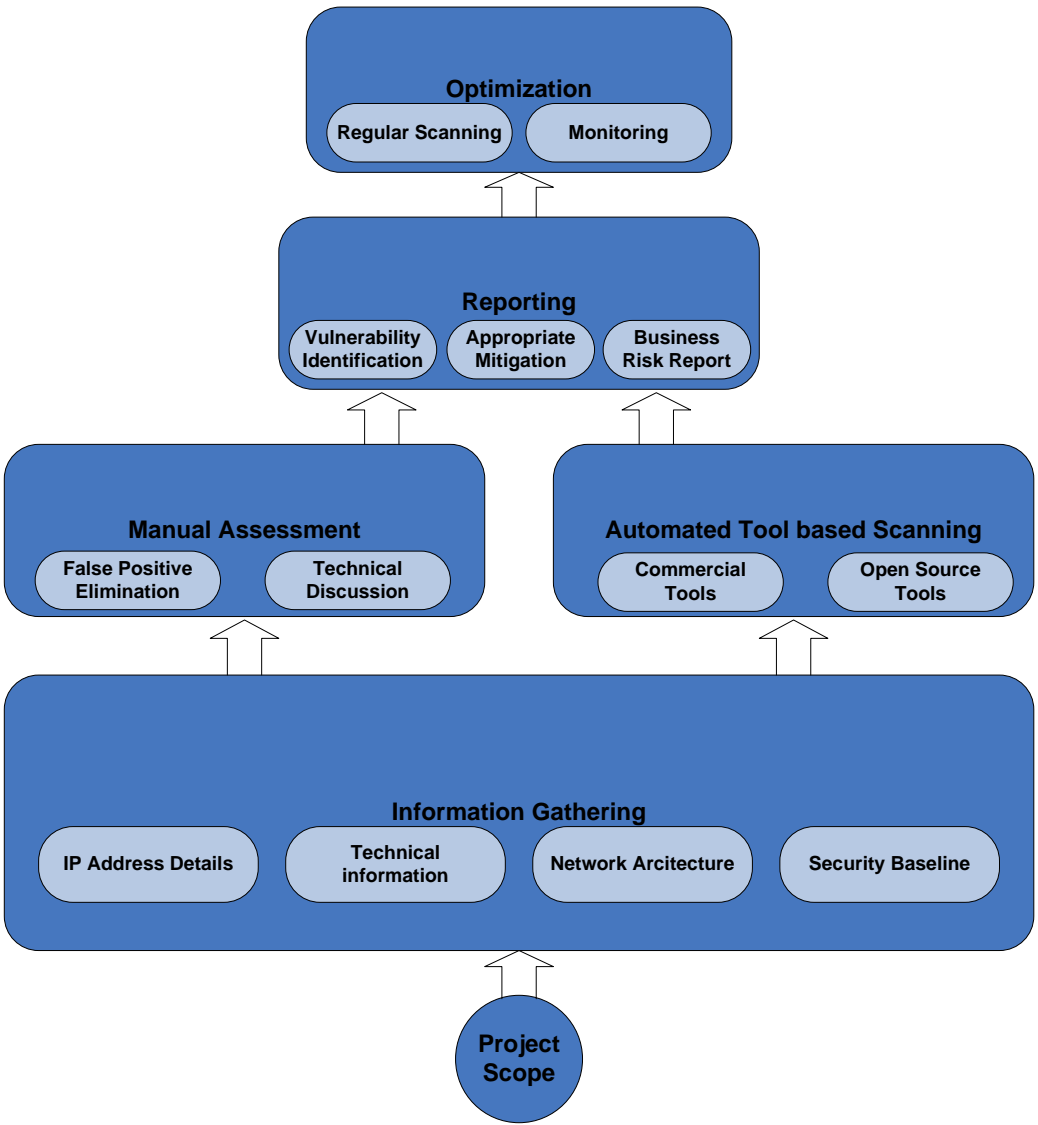
PayPal



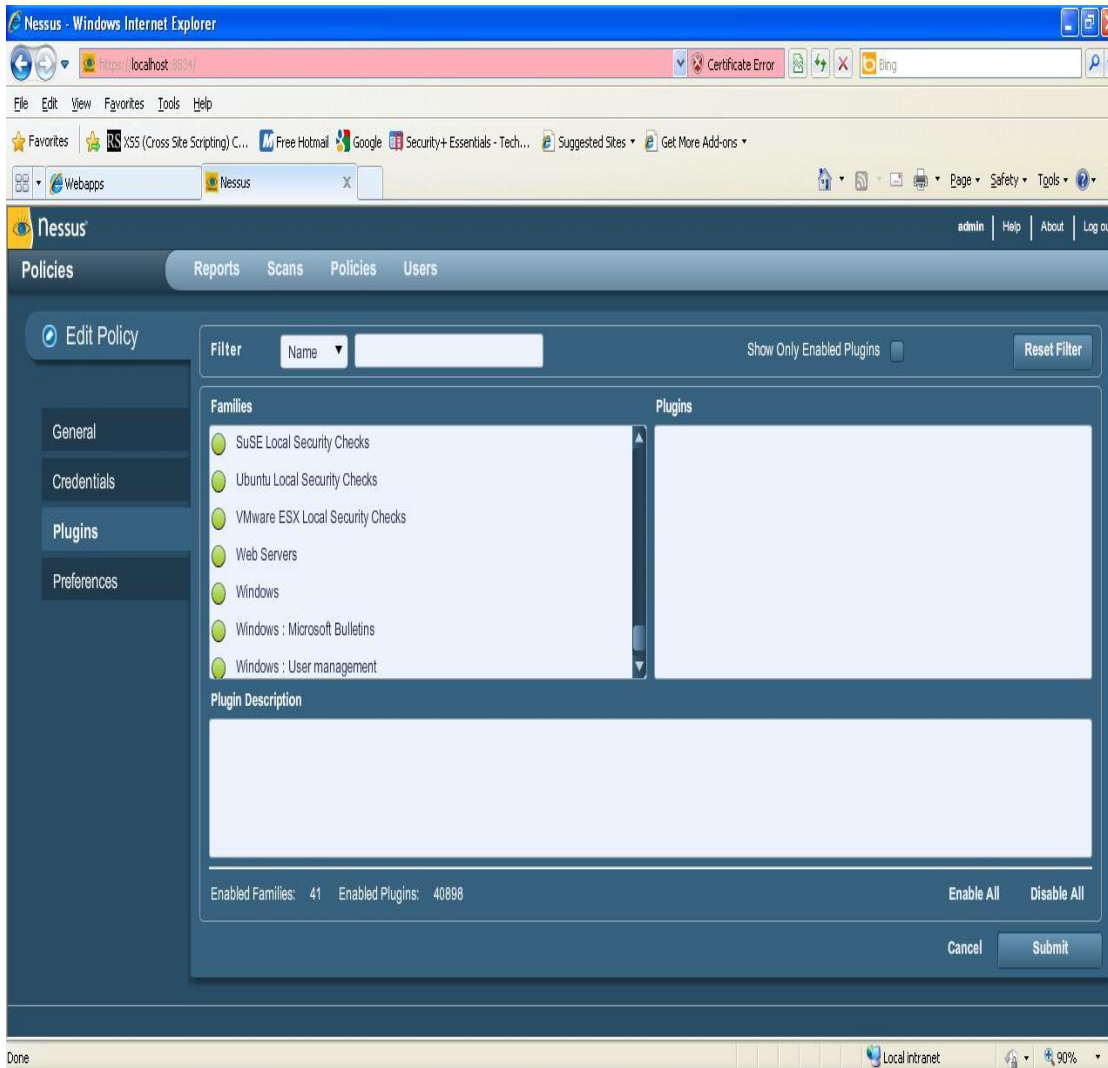
*The bad guys STILL HAVE their zero day, STILL HAVE their vectors, and STILL HAVE their malware*



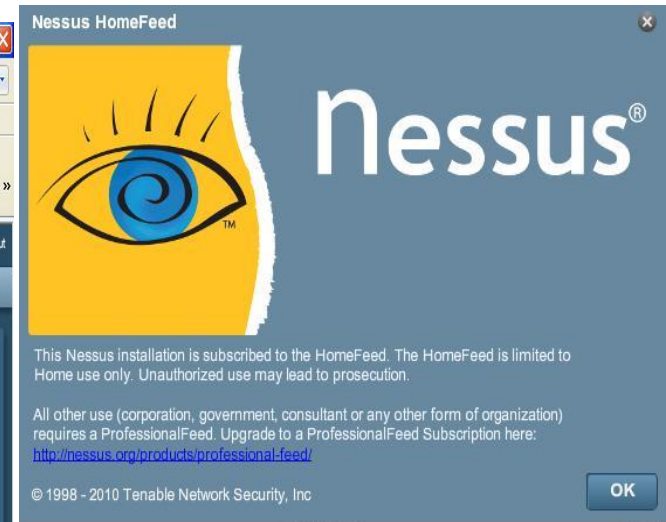
# Vulnerability Assessment Methodology & Tools



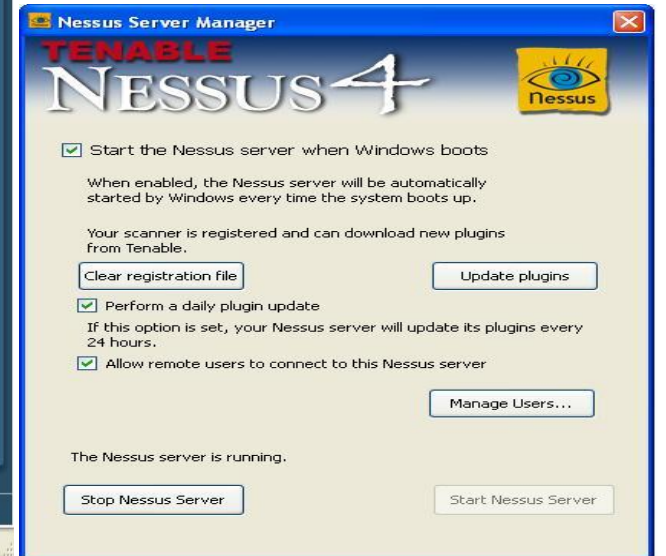
# Vulnerability Assessment Methodology & Tools



The screenshot shows the Nessus web interface in a Windows Internet Explorer browser window. The address bar shows 'http://localhost:8834/'. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The Nessus interface has a navigation bar with 'Policies', 'Reports', 'Scans', 'Policies', and 'Users'. The main content area is titled 'Edit Policy' and features a filter section with a 'Name' dropdown and a 'Reset Filter' button. Below the filter are two columns: 'Families' and 'Plugins'. The 'Families' column lists several categories with radio buttons: SuSE Local Security Checks, Ubuntu Local Security Checks, VMware ESX Local Security Checks, Web Servers, Windows, Windows : Microsoft Bulletins, and Windows : User management. The 'Plugins' column is currently empty. At the bottom of the interface, it shows 'Enabled Families: 41' and 'Enabled Plugins: 40898'. There are buttons for 'Enable All', 'Disable All', 'Cancel', and 'Submit'.



The screenshot shows the Nessus HomeFeed splash screen. It features the Nessus logo, which is a stylized eye with a blue spiral, set against a yellow background. To the right of the logo, the word 'Nessus' is written in a large, white, sans-serif font. Below the logo and text, there is a paragraph of text: 'This Nessus installation is subscribed to the HomeFeed. The HomeFeed is limited to Home use only. Unauthorized use may lead to prosecution.' Below this text is another paragraph: 'All other use (corporation, government, consultant or any other form of organization) requires a ProfessionalFeed. Upgrade to a ProfessionalFeed Subscription here: <http://nessus.org/products/professional-feed/>'. At the bottom of the splash screen, there is a copyright notice: '© 1998 - 2010 Tenable Network Security, Inc' and an 'OK' button.



The screenshot shows the Nessus Server Manager dialog box. The title bar reads 'Nessus Server Manager'. The main content area has a large 'TENABLE NISSUS 4' logo. Below the logo, there are three checked options: 'Start the Nessus server when Windows boots', 'Perform a daily plugin update', and 'Allow remote users to connect to this Nessus server'. The first option has a sub-description: 'When enabled, the Nessus server will be automatically started by Windows every time the system boots up.' The second option has a sub-description: 'Your scanner is registered and can download new plugins from Tenable.' The third option has a sub-description: 'If this option is set, your Nessus server will update its plugins every 24 hours.' There are buttons for 'Clear registration file', 'Update plugins', and 'Manage Users...'. At the bottom, there is a status bar that says 'The Nessus server is running.' and buttons for 'Stop Nessus Server' and 'Start Nessus Server'.

# Wireless Usages & vulnerabilities

Wireless technology is becoming popular and at the same time has introduced several security issues. It's a cost effective solution and mobility ,Easy sharing, the same advantages turned to be the security threats.

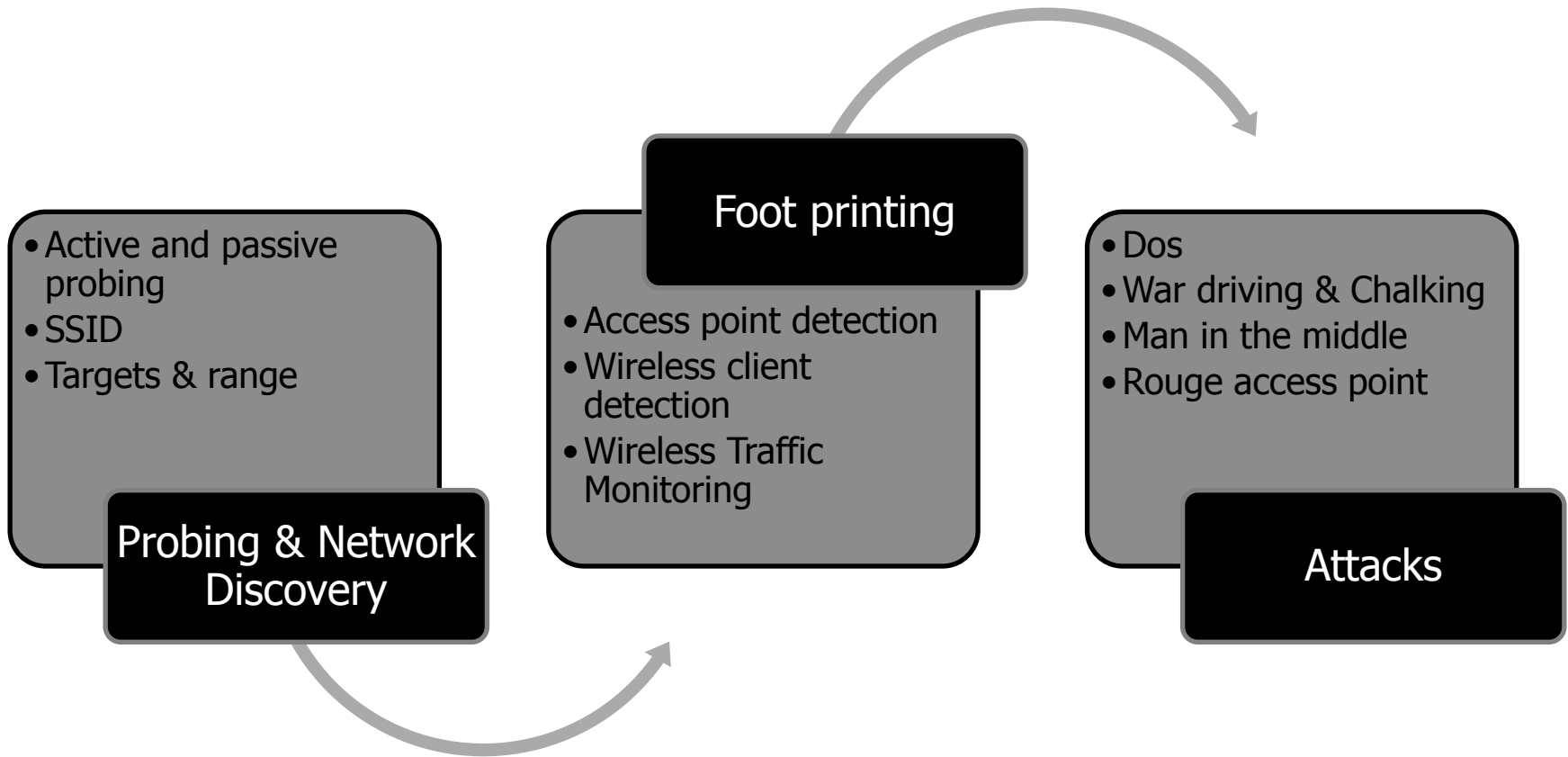
**Various Wireless standards :** 802.11a , 802.11b , 802.11g , 802.11i , 802.16

## **Vulnerabilities :**

- ❖ Default Configuration
- ❖ Weak passwords
- ❖ Physically insecure locations
- ❖ Rogue access points
- ❖ Lack of network monitoring
- ❖ Insufficient network performance
- ❖ MAC address filtering
- ❖ Inadequate encryption standards
- ❖ War Driving
- ❖ Easy to eavesdrop
- ❖ Unsecured holes in the Network



# Wireless Attacking Methodology



# How to Prevent Wireless Hacks

- Access Point Monitoring
- Wireless Client Monitoring
- General Wireless Traffic Monitoring
- Wireless IDS
- Frequent security testing

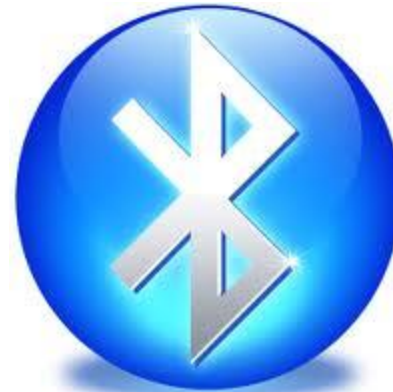


# Bluetooth Usages & Vulnerabilities

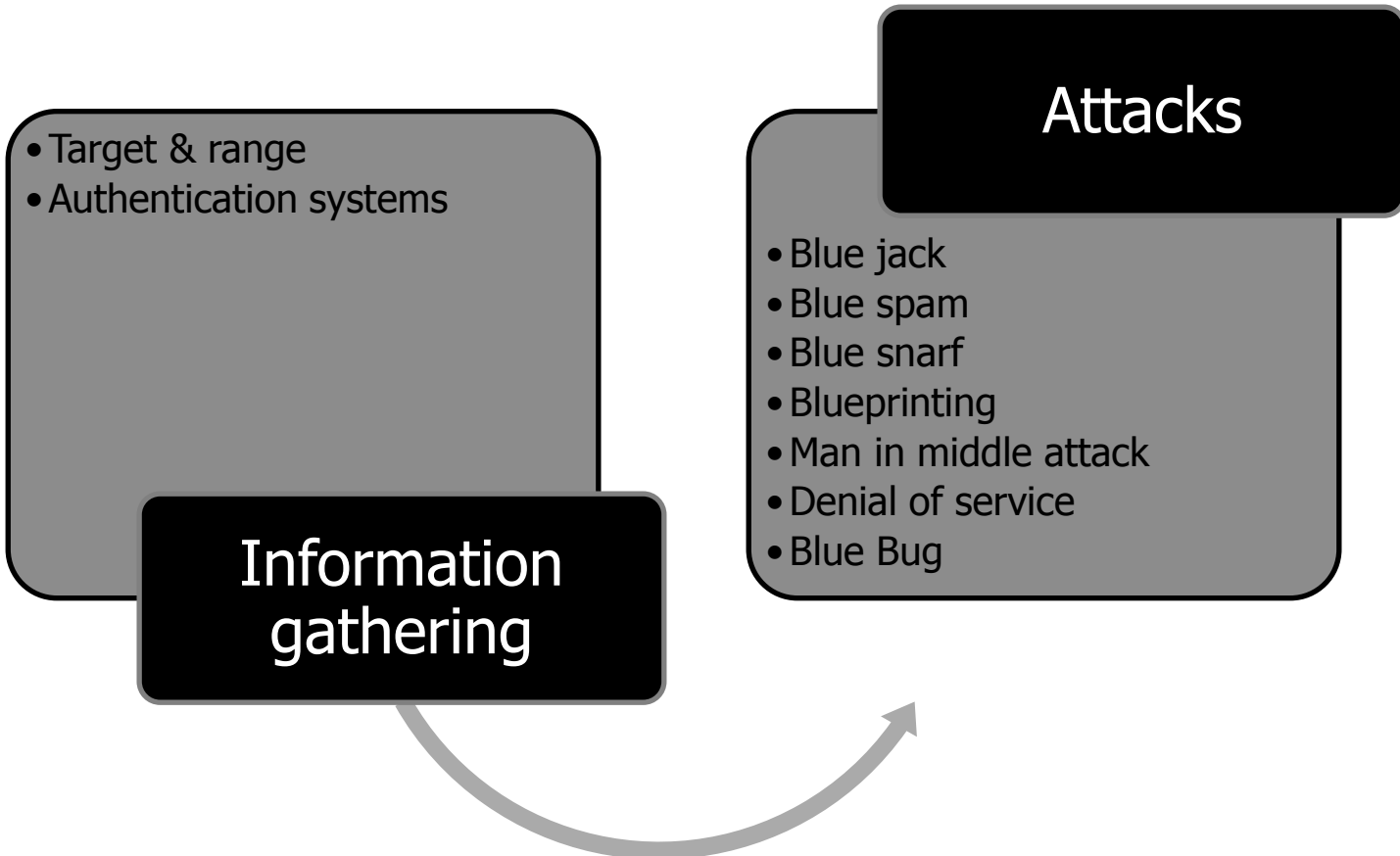
Bluetooth technology is becoming popular short-range radio link designed to connect portable and/or fixed electronic devices. Bluetooth specification defines security at the link level, allowing flexibility in the application security design. Bluetooth system provides for three basic security services: 1) Confidentiality 2) Authentication 3) Authorization

## Vulnerabilities :

- ❖ Default Configuration
- ❖ Weak PINS
- ❖ Eavesdropping and Impersonation
- ❖ No user authentication
- ❖ Unsecure Master keys
- ❖ Physically insecure locations



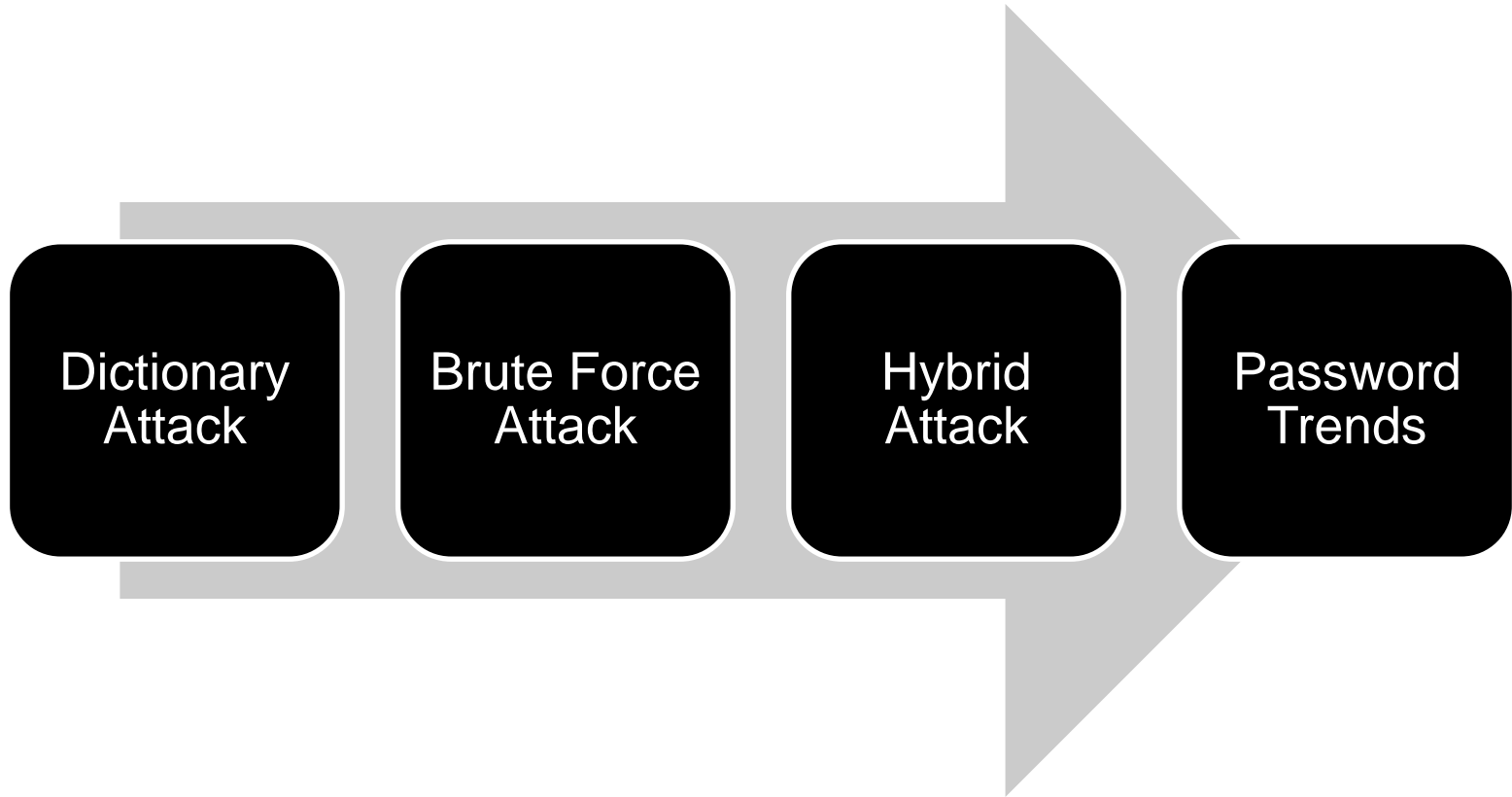
# Bluetooth Attacking & Methodology



# How to Prevent Bluetooth Hacks

- ❑ Switch off blue tooth when not in use
- ❑ Strong PIN codes – long & dynamic
- ❑ Vendor configuration removal
- ❑ Non – Discoverable Mode after paring
- ❑ Switch off – unnecessary SCO/eSCO links

# Password Hacking



# Ways to Prevent Applications from password Hacks

- ❑ Remove Guessable & vendor default
- ❑ URL String Password Disclosure
- ❑ Remove from cookies
- ❑ Account information in an Encryption database

## Best practices

- ❖ Do not add a single digit or symbol before or after a word – for example, “microsoft1”
- ❖ Do not double up a single word – for example, “msoftmsoft”
- ❖ Do not simply reverse a word – for example, “tfosorcim”
- ❖ Do not remove the vowels– for example, “io”
- ❖ Key sequences that can be easily repeated - for example, “qwerty”, “asdf” etc.
- ❖ Do not garble letters– for example, converting e to 3, L to 1, o to 0, as in “z3ro – 10v3”

# Q & A

