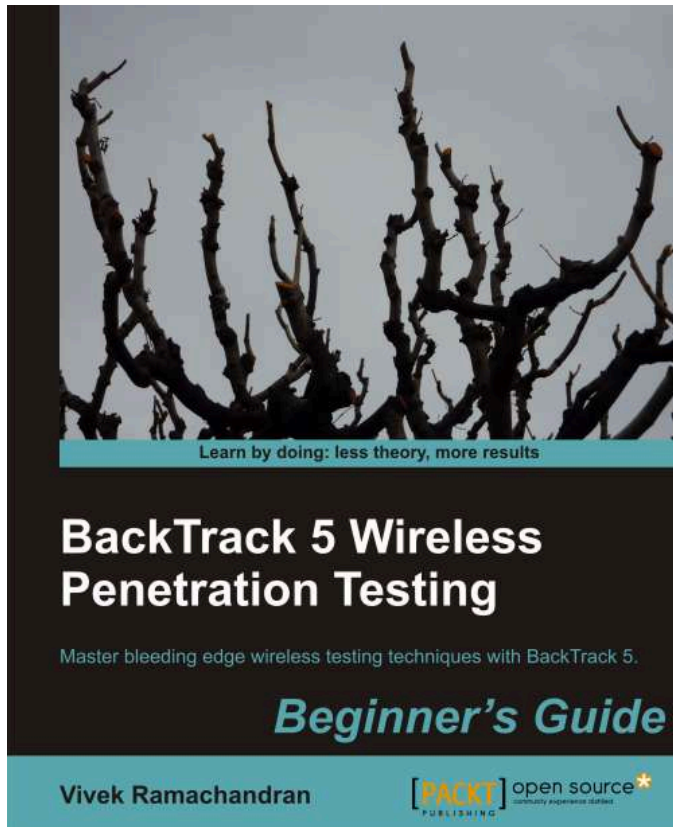


Wi-Fi Malware for Fun and Profit


Vivek Ramachandran
Founder, SecurityTube.net




Who am I? (Shameless Self Promotion)




- 802.1x Cat6k, Cisco
- Broke WEP Cloaking (Defcon 15)
- Caffe Latte Attack (Toorcon 9)
- Microsoft Security Shootout
- “Backtrack 5 Wireless Penetration Testing” published


www.SecurityTube.net


SecurityTube Welcome Guest [Login](#) | [Register](#) 

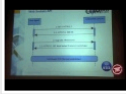
[Home](#) [Videos](#) [Groups](#) [Downloads](#) [Tools](#) [Donate](#) [Store](#)   


Latest Videos

**Car Cracking** Posted by SecurityTube_Bot
Posted 1 day, 2 hours ago
682 Views


**Bug hunting in Windows Mobile** Posted by SecurityTube_Bot
Posted 1 day, 2 hours ago
250 Views


**Ted Talk: Misha Glenny - Hire the Hackers!** Posted by SecurityTube_Bot
Posted 2 days, 12 hours ago
1081 Views, 2 Comments


**HTML5 Web Security** Posted by SecurityTube_Bot
Posted 3 days, 2 hours ago
607 Views


**PHP : Buffer Over Flow Helper** Posted by Lagripe-Dz
Posted 4 days, 8 hours ago
711 Views, 3 Comments


New Members

 **raj.gotte**
Joined 2 hours, 48 minutes ago

 **luke**
Joined 4 hours, 30 minutes ago

 **stpiere**
Joined 4 hours, 50 minutes ago

 **Ranganath**
Joined 7 hours, 31 minutes ago

 **jordan40987**
Joined 11 hours, 40 minutes ago

<http://www.securitytube.net/downloads>

Software Requirements

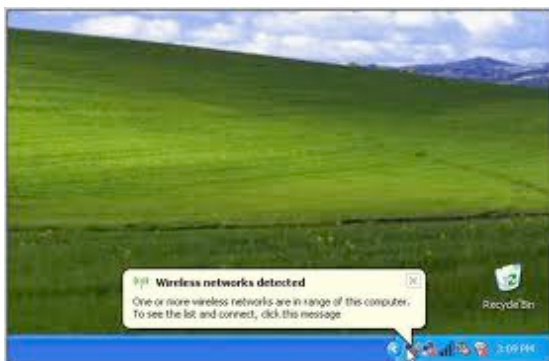
- Windows 7 laptop with in-built Wi-Fi or external adapter
- Backtrack \geq 4 in Virtualbox
- External USB card capable of Packet Injection

If you do not have all / part of the setup, you can still follow the class

Agenda

- Wireless Client Behavior
- Software Access Points
 - Linux
 - Windows
- Abusing Windows Soft Access Points
 - Backdoors
 - Worms and Botnets
- Future Roadmap

Background – Understanding Wi-Fi Client Software

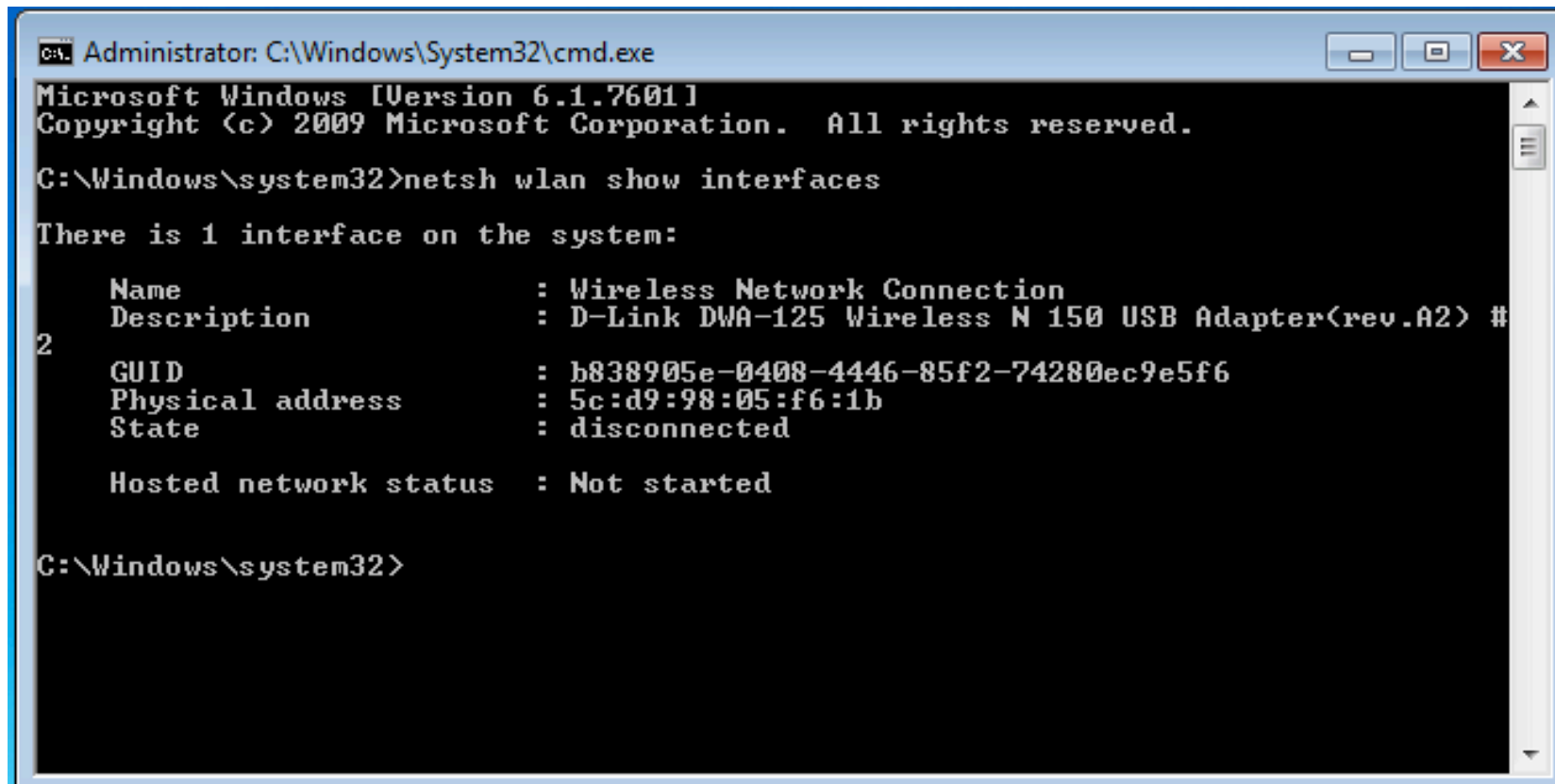


- Allows Client to connect to an Access Point
- First time user approves it, Auto-Connect for future instances
- Details are stored in Configuration Files

Understanding Wi-Fi Clients

- Scanning the air for stored profiles
 - Profiling the clients based on searches
 - Different clients behave differently
-
- Demo

See All Wi-Fi Interfaces



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netsh wlan show interfaces

There is 1 interface on the system:

    Name                : Wireless Network Connection
    Description          : D-Link DWA-125 Wireless N 150 USB Adapter<rev.A2> #
2
    GUID                 : b838905e-0408-4446-85f2-74280ec9e5f6
    Physical address     : 5c:d9:98:05:f6:1b
    State                 : disconnected

    Hosted network status : Not started

C:\Windows\system32>
```

Netsh wlan show interfaces

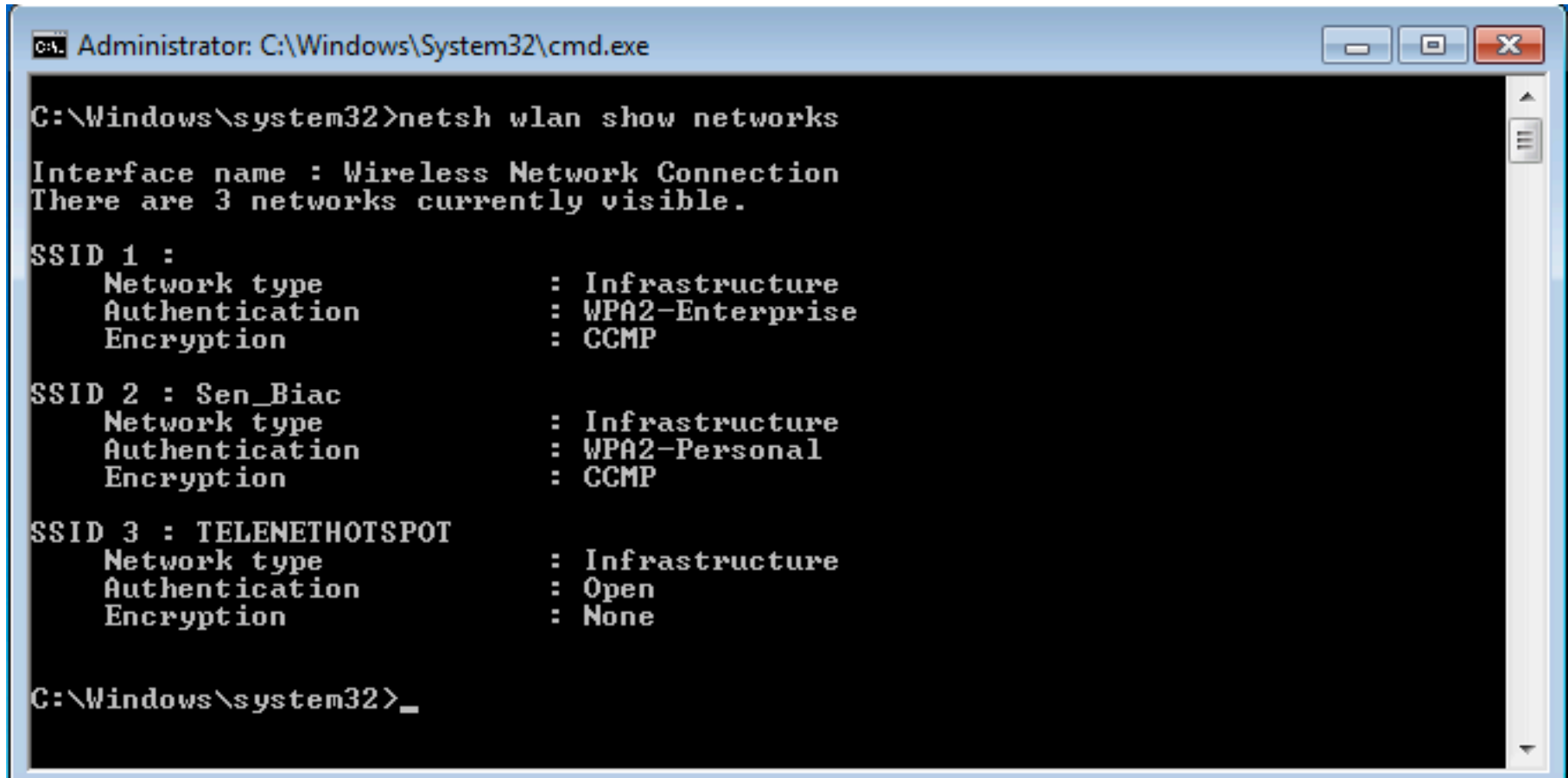
Drivers and Capabilities

```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>netsh wlan show drivers
Interface name: Wireless Network Connection

Driver           : D-Link DWA-125 Wireless N 150 USB Adapter<rev.A2
Vendor           : D-Link Corporation
Provider         : D-Link Corporation
Date             : 10/15/2009
Version          : 3.0.7.0
INF file         : C:\Windows\INF\oem2.inf
Files            : 4 total
                  C:\Windows\system32\DRIVERS\Dnetr28u.sys
                  C:\Windows\system32\drivers\vwifibus.sys
                  C:\Windows\system32\RaCoInst.dll
                  C:\Windows\system32\RaCoInst.dat
Type             : Native Wi-Fi Driver
Radio types supported : 802.11b 802.11g 802.11n
FIPS 140-2 mode supported : Yes
Hosted network supported : Yes
Authentication and cipher supported in infrastructure mode:
  Open           None
  Open           WEP-40bit
  Open           WEP-104bit
```

Netsh wlan show drivers

Scan for Available Networks



```
C:\Windows\system32>netsh wlan show networks

Interface name : Wireless Network Connection
There are 3 networks currently visible.

SSID 1 :
  Network type           : Infrastructure
  Authentication         : WPA2-Enterprise
  Encryption             : CCMP

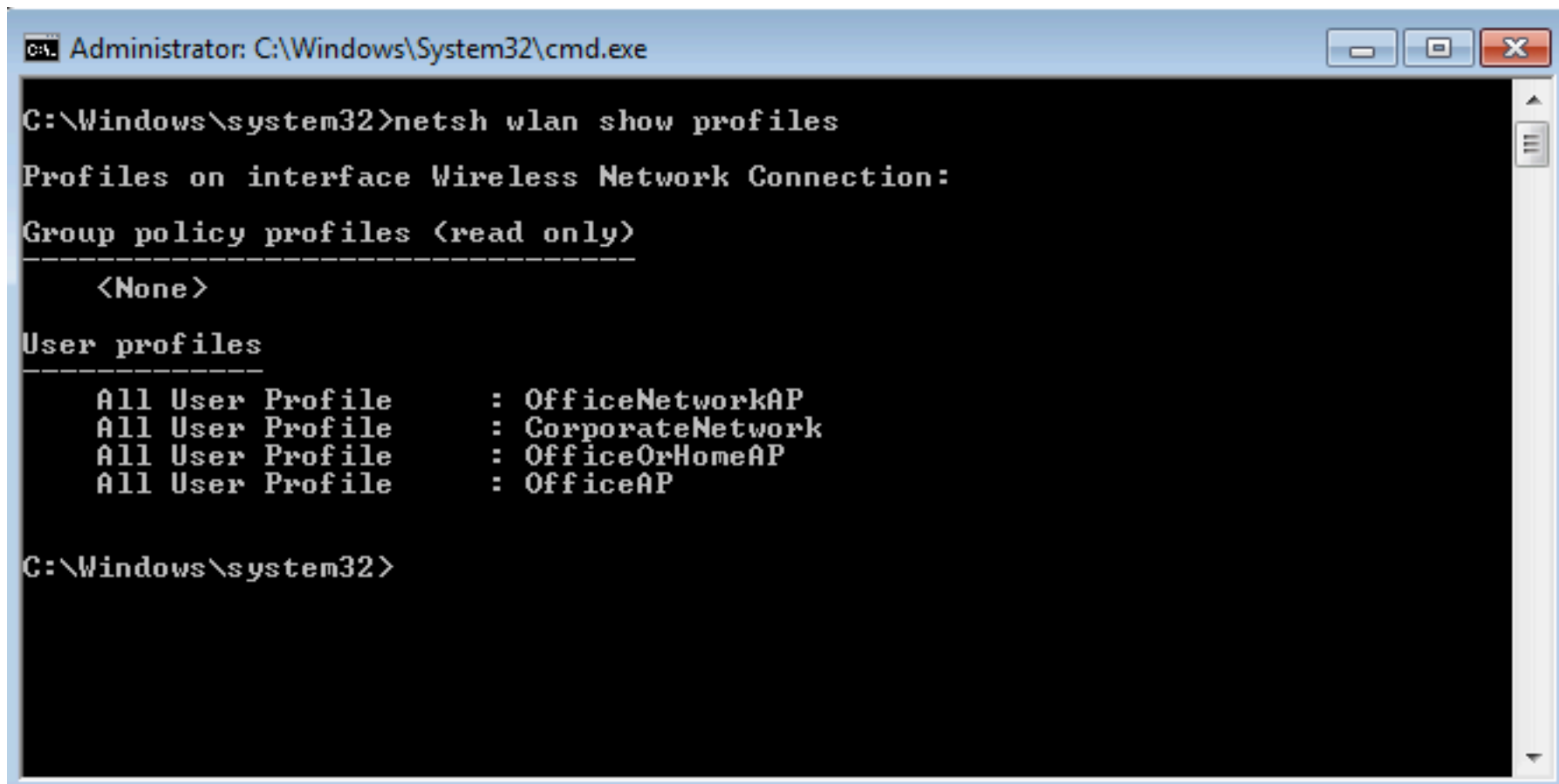
SSID 2 : Sen_Biac
  Network type           : Infrastructure
  Authentication         : WPA2-Personal
  Encryption             : CCMP

SSID 3 : TELENETHOTSPOT
  Network type           : Infrastructure
  Authentication         : Open
  Encryption             : None

C:\Windows\system32>_
```

Netsh wlan show networks

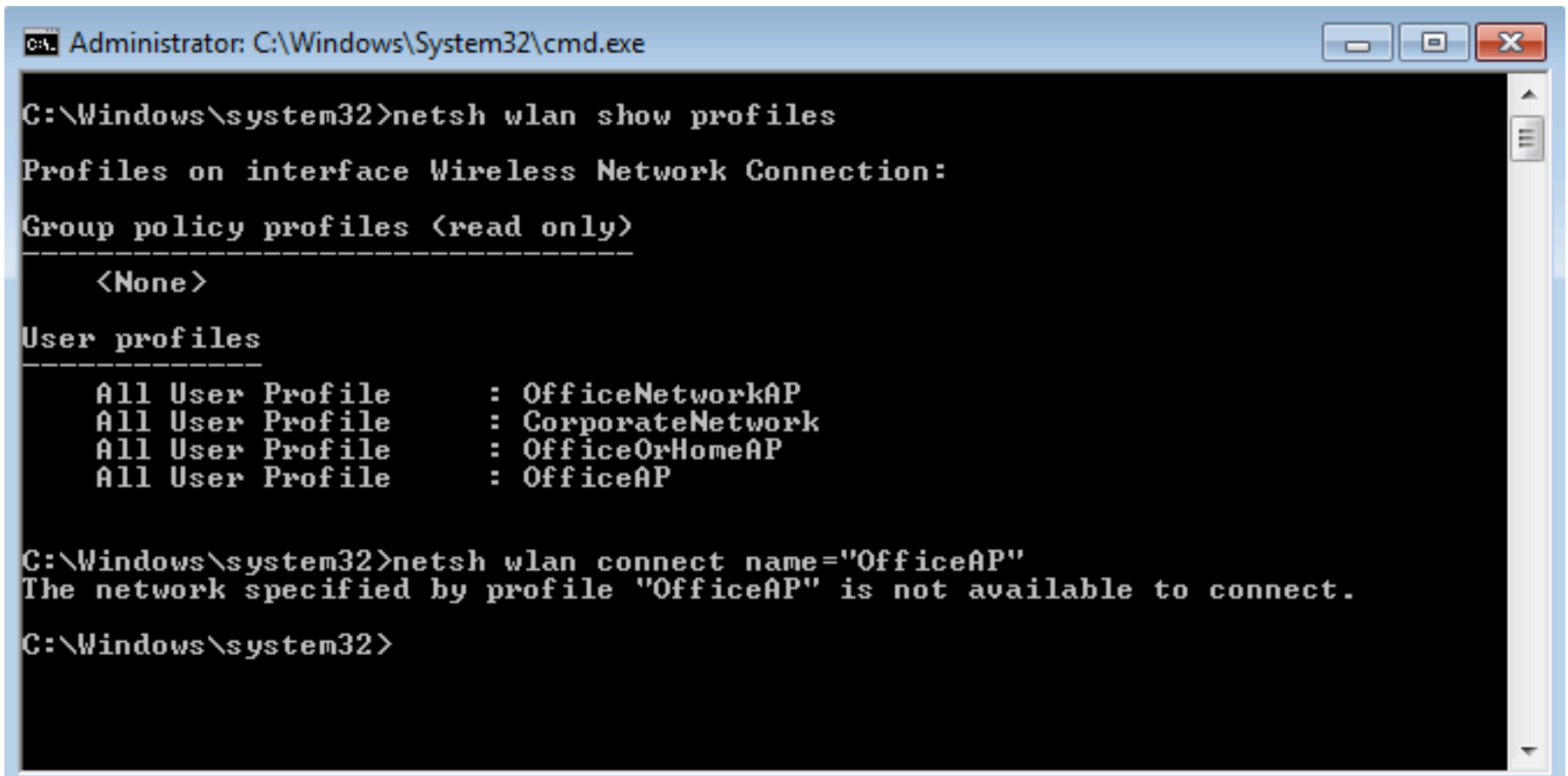
View Existing Profiles



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>netsh wlan show profiles
Profiles on interface Wireless Network Connection:
Group policy profiles (read only)
-----
<None>
User profiles
-----
All User Profile      : OfficeNetworkAP
All User Profile      : CorporateNetwork
All User Profile      : OfficeOrHomeAP
All User Profile      : OfficeAP
C:\Windows\system32>
```

Netsh wlan show profiles

Starting a Profile



```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>netsh wlan show profiles

Profiles on interface Wireless Network Connection:

Group policy profiles (read only)
-----
<None>

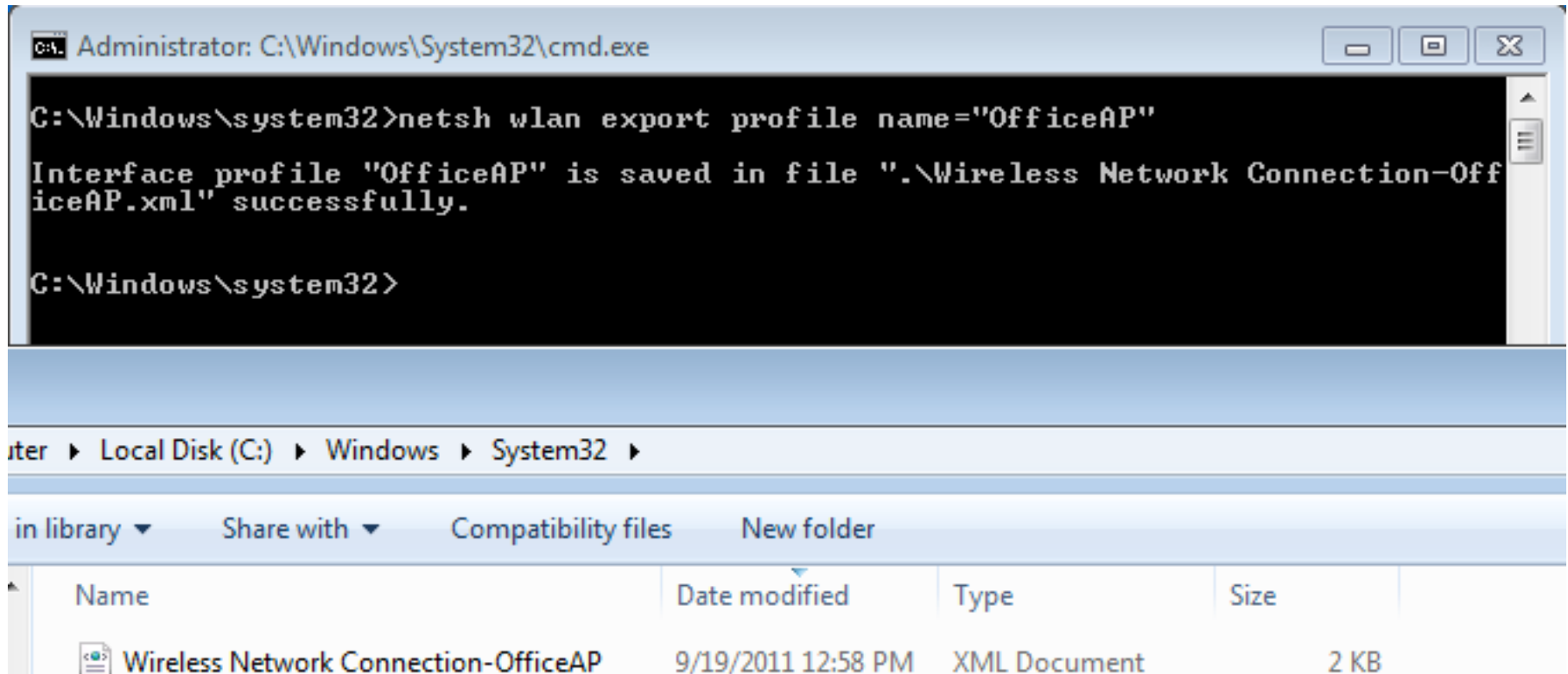
User profiles
-----
All User Profile      : OfficeNetworkAP
All User Profile      : CorporateNetwork
All User Profile      : OfficeOrHomeAP
All User Profile      : OfficeAP

C:\Windows\system32>netsh wlan connect name="OfficeAP"
The network specified by profile "OfficeAP" is not available to connect.

C:\Windows\system32>
```

Netsh wlan connect name="vivek"

Export a Profile



Netsh wlan export profile name="vivek"

Creating an Access Point on a Client Device



- Requirement for special drivers and supported cards
- Custom software used – HostAPd, Airbase-NG
- More feasible on Linux based systems

Linux Soft AP

- Airbase-NG
- HostAPd
- ...

Generation 2.0 of Client Software – Hosted Network

- Available Windows 7 and Server 2008 R2 onwards
- Virtual adapters on the same physical adapter
- SoftAP can be created using virtual adapters
 - DHCP server included

“With this feature, a Windows computer can use a single physical wireless adapter to connect as a client to a hardware access point (AP), while at the same time acting as a software AP allowing other wireless-capable devices to connect to it.”

<http://msdn.microsoft.com/en-us/library/dd815243%28v=vs.85%29.aspx>

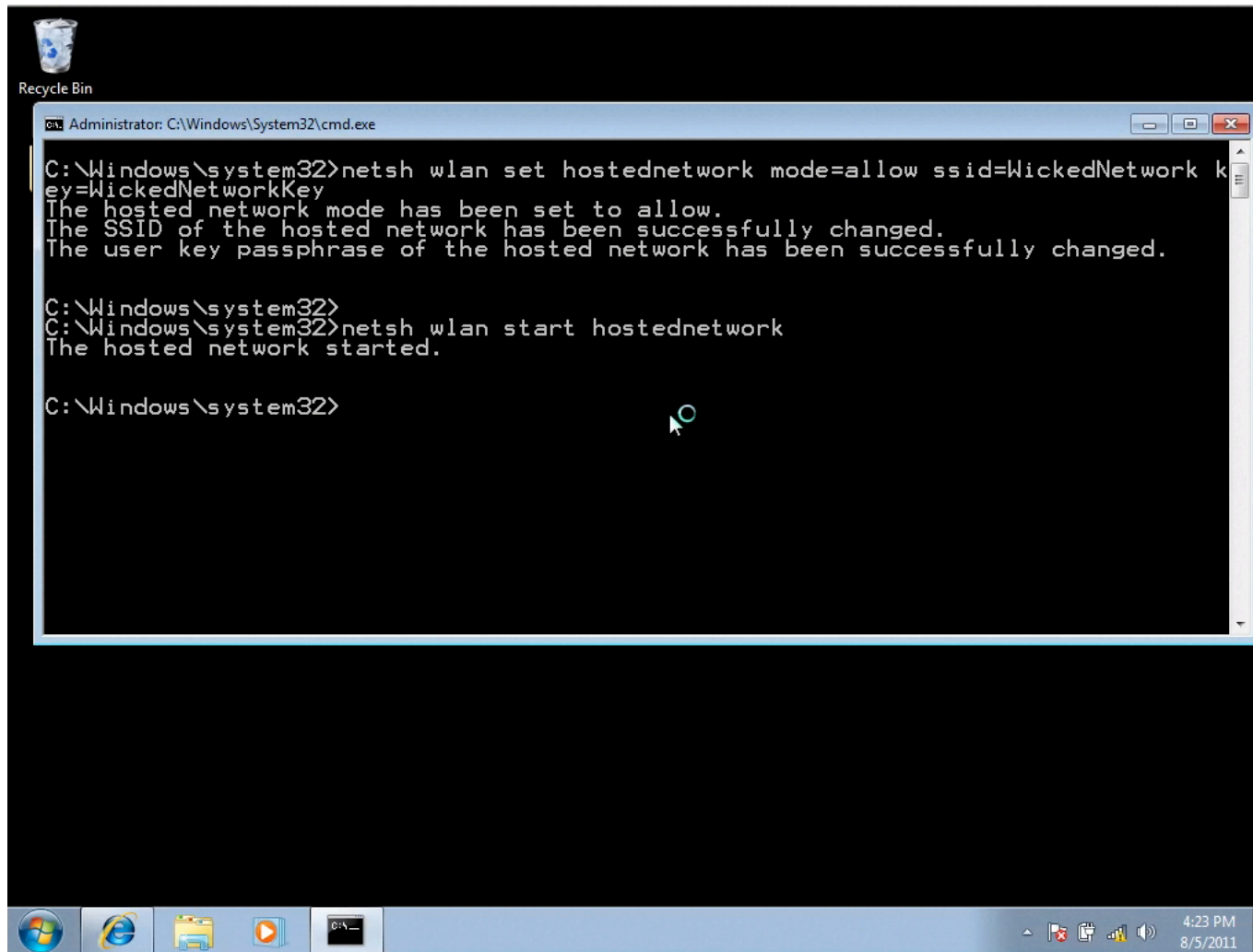
Feature Objective

- To allow creation of a wireless Personal Area Network (PAN)
 - Share data with devices
- Network connection sharing (ICS) with other devices on the network

Demonstration

Demo of Hosted Network

Creating a Hosted Network



The screenshot shows a Windows XP desktop environment. In the top-left corner, there is a Recycle Bin icon. The taskbar at the bottom contains several icons: Start button, Internet Explorer, My Computer, Media Center, and a command prompt icon. The system tray in the bottom-right corner shows the time as 4:23 PM on 8/5/2011, along with icons for network, volume, and power.

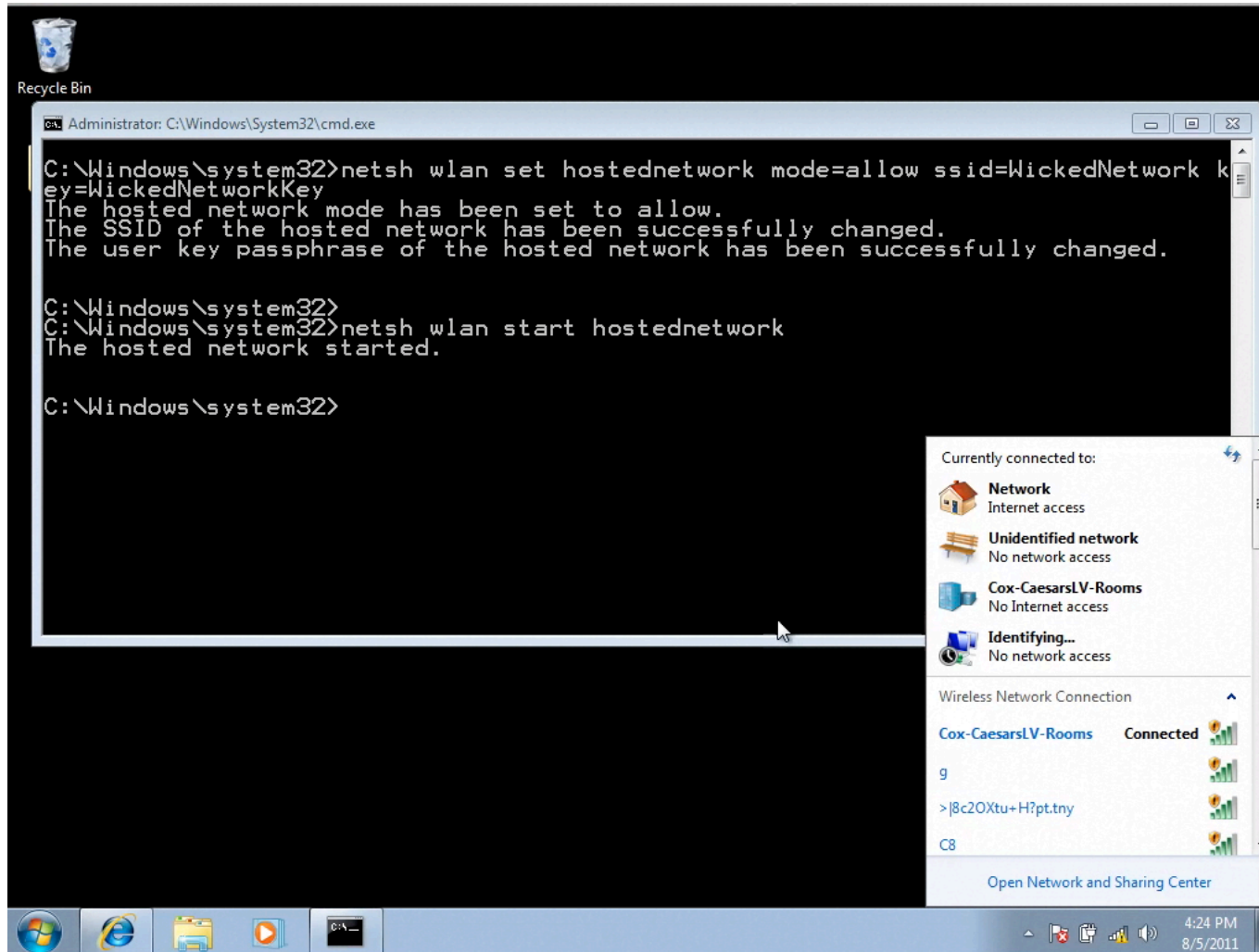
The central focus is a command prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The window contains the following text:

```
C:\Windows\system32>netsh wlan set hostednetwork mode=allow ssid=WickedNetwork key=WickedNetworkKey
The hosted network mode has been set to allow.
The SSID of the hosted network has been successfully changed.
The user key passphrase of the hosted network has been successfully changed.

C:\Windows\system32>
C:\Windows\system32>netsh wlan start hostednetwork
The hosted network started.

C:\Windows\system32>
```

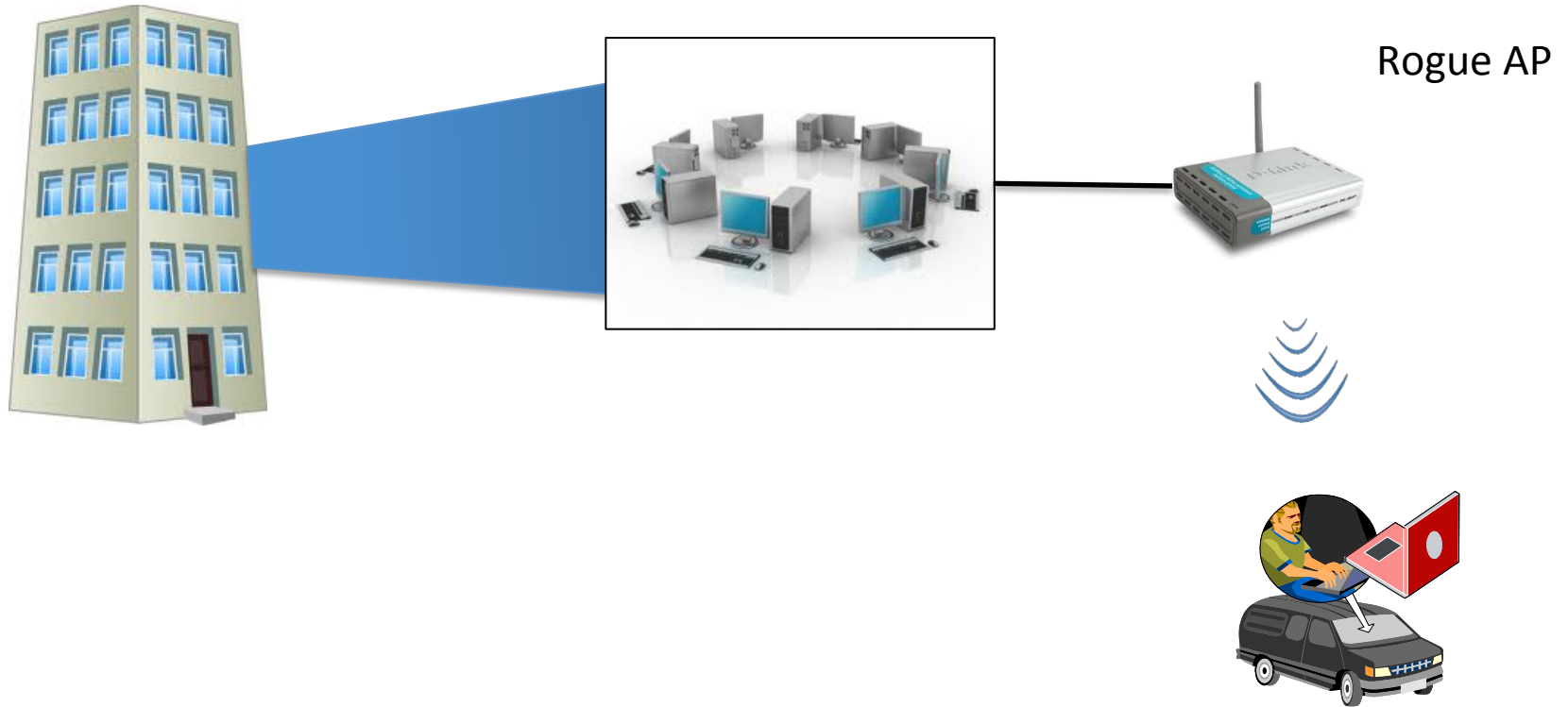
Client still remains connected to hard AP!



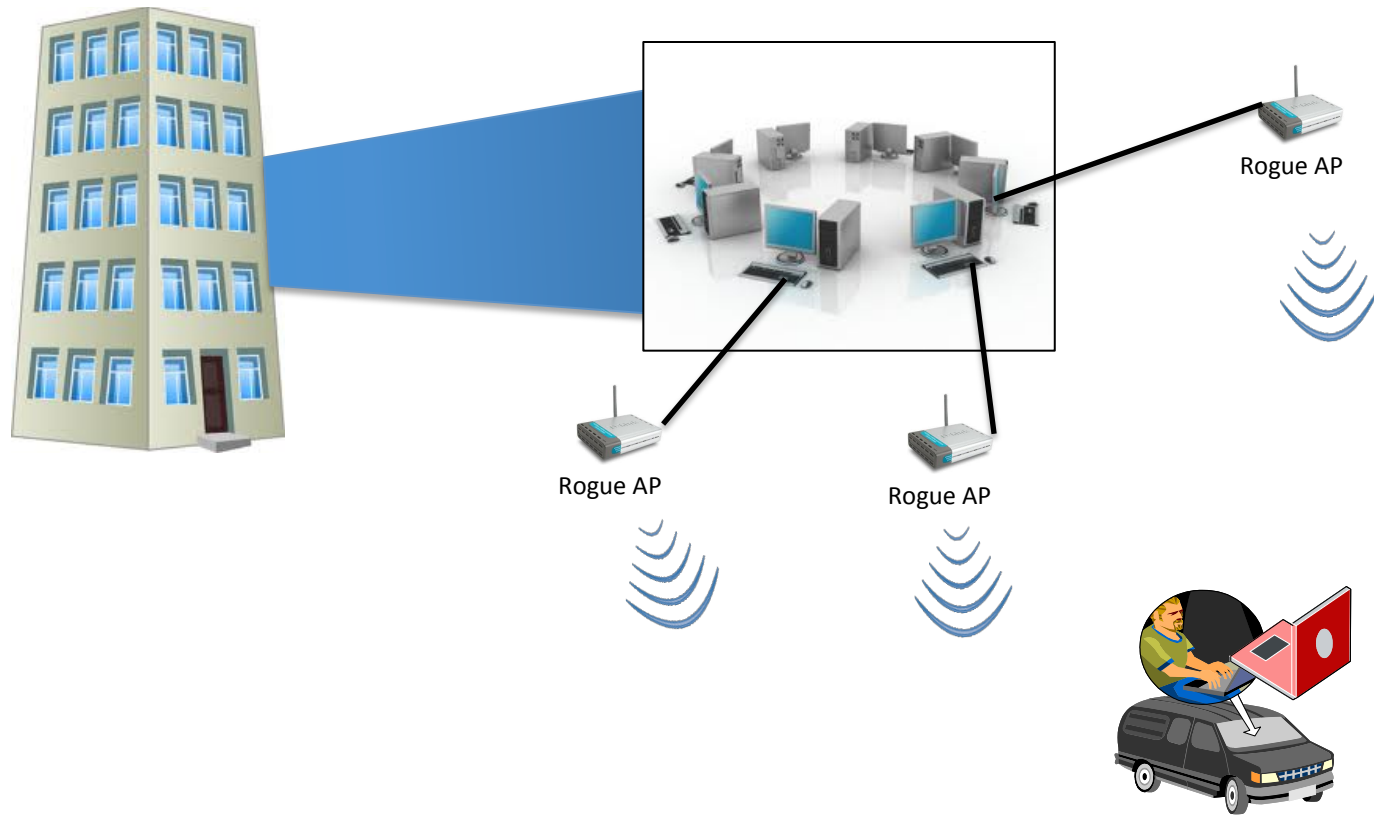
Wi-Fi Backdoor

- Easy for malware to create a backdoor
- They key could be:
 - Fixed
 - Derived based on MAC address of host, time of day etc.
- As host remains connected to authorized network, user does not notice a break in connection
- No Message or Prompt displayed

Understanding Rogue Access Points



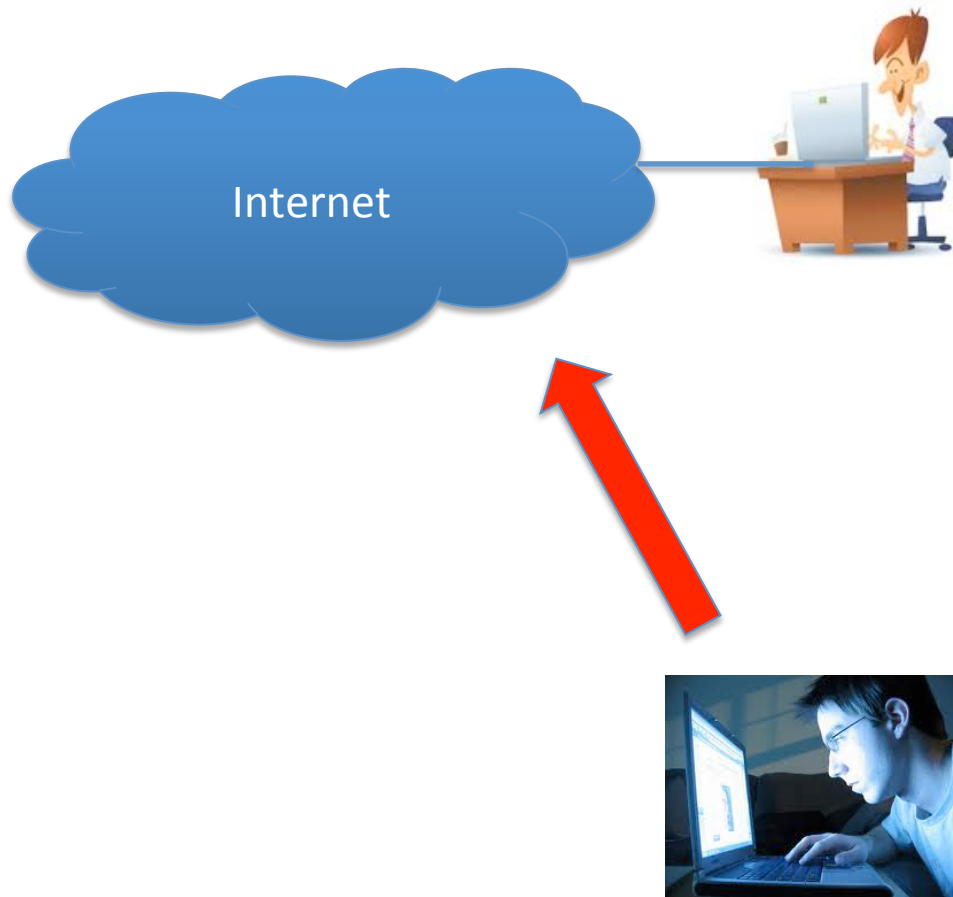
Makes a Rogue AP on every Client!



Best Part – No Extra Hardware!



Advantages?



Advantages?



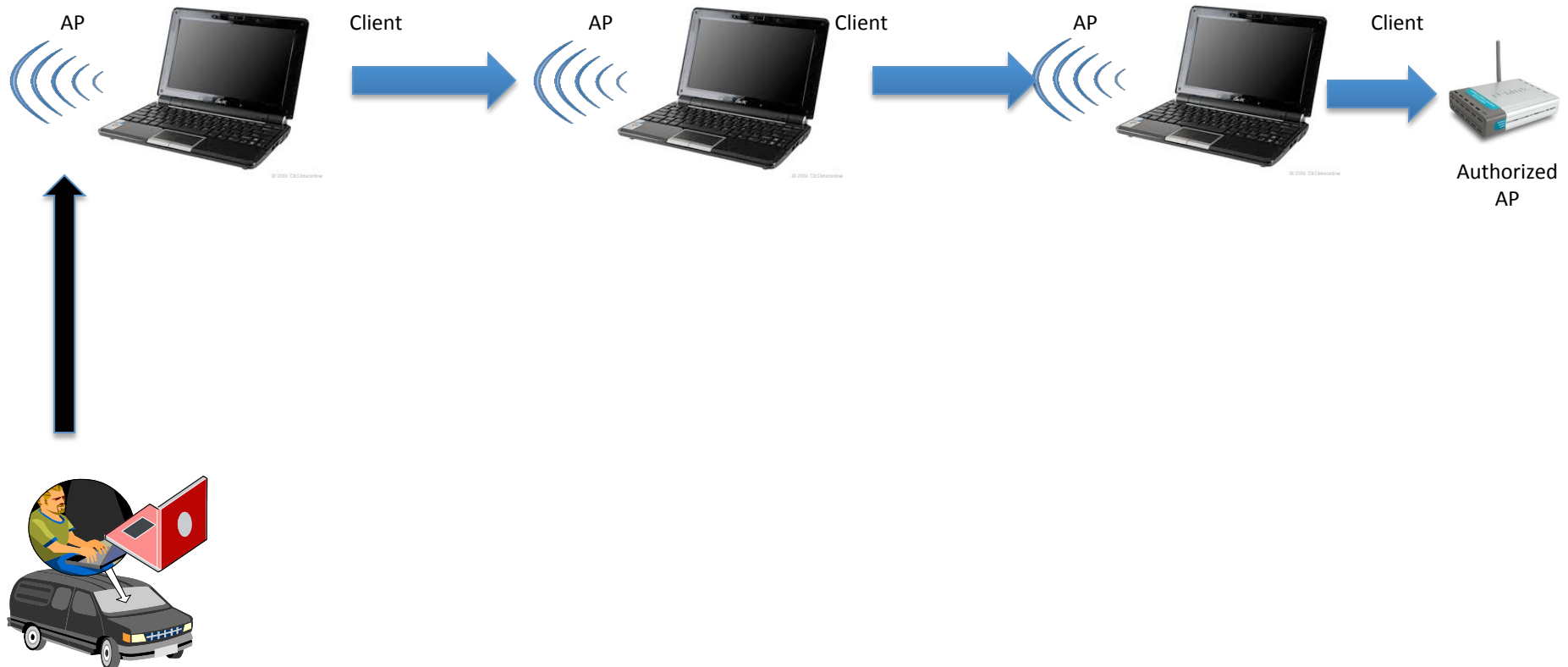
Why is this cool?

- Victim will never notice anything unusual unless he visits his network settings
 - has to be decently technical to understand
- Attacker connects to victim over a private network
 - no wired side network logs: firewalls, IDS, IPS
 - Difficult, if not impossible to trace back
 - Difficult to detect even while attack is ongoing 😊
- Abusing legitimate feature, not picked up by AVs, Anti-Malware
- More Stealth? Monitor air for other networks, when a specific network comes up, then start the Backdoor

Chaining Hosted Networks like a proxy?

- Each node has client and AP capability
- We can chain them to “hop” machines
- Final machine can provide Internet access
- Like Wi-Fi Repeaters

Chaining Infected Laptops



Package Meterpreter for full access?

- Once attacker connects to his victim, he would want to have access to everything
- Why not package a Meterpreter with this? 😊
- How about a Backdoor post-exploitation script for Metasploit? 😊

Demo

```
^ v x root@bt: ~
File Edit View Terminal Help
root@bt:~# msfpayload windows/shell_bind_tcp R | msfencode -t exe -o malpayload.exe
[*] x86/shikata_ga_nai succeeded with size 368 (iteration=1)

root@bt:~#
root@bt:~# █
```

Increasing Stealth

- Passive Monitoring for SSIDs available
- Trigger SSID causes Wicked Hosted Network to start and create application level backdoor
- Attacker connects and does his job
- Shuts off Trigger SSID and Malware goes to Passive Monitoring again

Karmetasploit

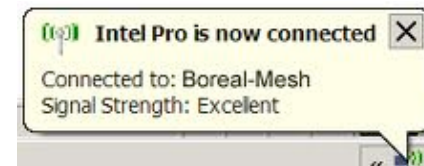
- Victim connects by mistake or misassociation
- Victim opens browser, Metasploit Browser_Autopwn exploits the system
- Hacker gets access!
- **Biggest Challenge** – Victim notices he is connected to the wrong network and disconnects himself

Enhancing Karmetasploit

- Upon Exploitation, create the hosted network backdoor
- User disconnects, but this hosted network still remains active
- Attacker connects via this network

What about older clients and other OSs?

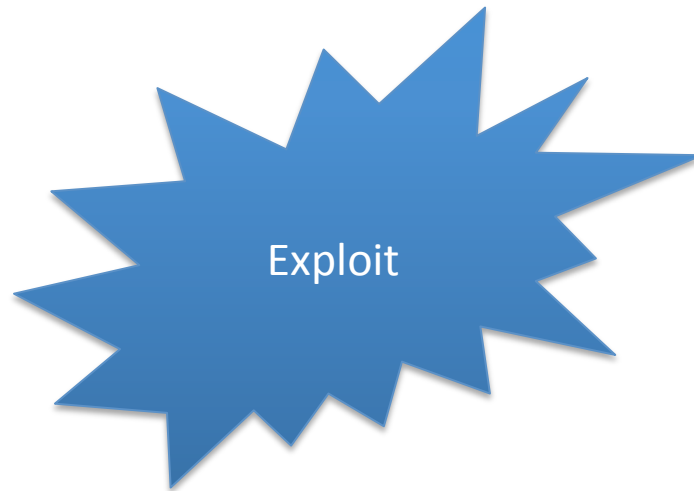
- Windows < 7, Mac OS do not have the Hosted Network or alike feature
 - Use Ad-Hoc networks
 - Use Connect Back mechanism 😊
 - When a particular SSID is seen, connect to it automatically
 - Blurb reporting “Connected to ABC”
 - Could we kill it? 😊



Dissecting Worm Functionality



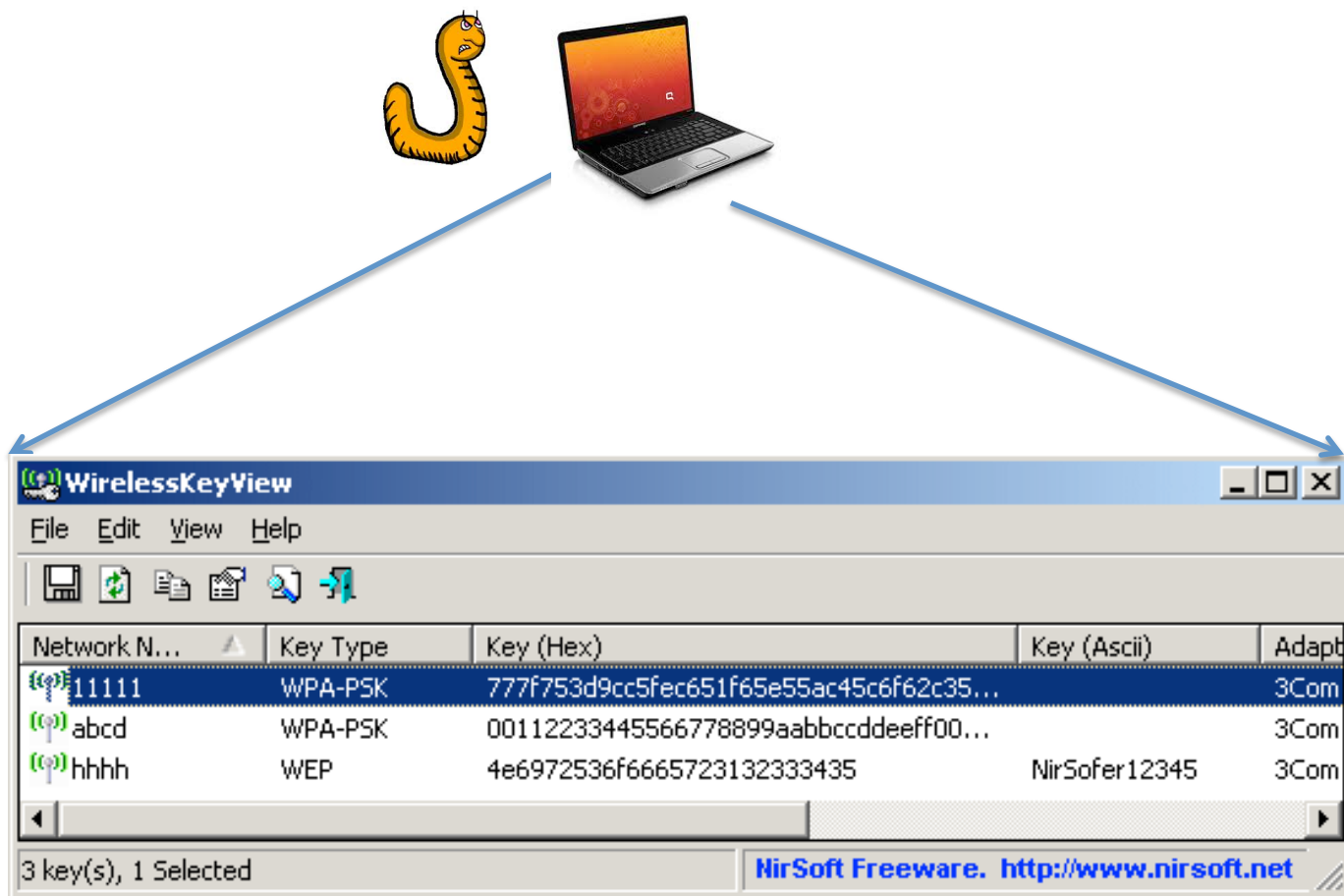
Worm -----



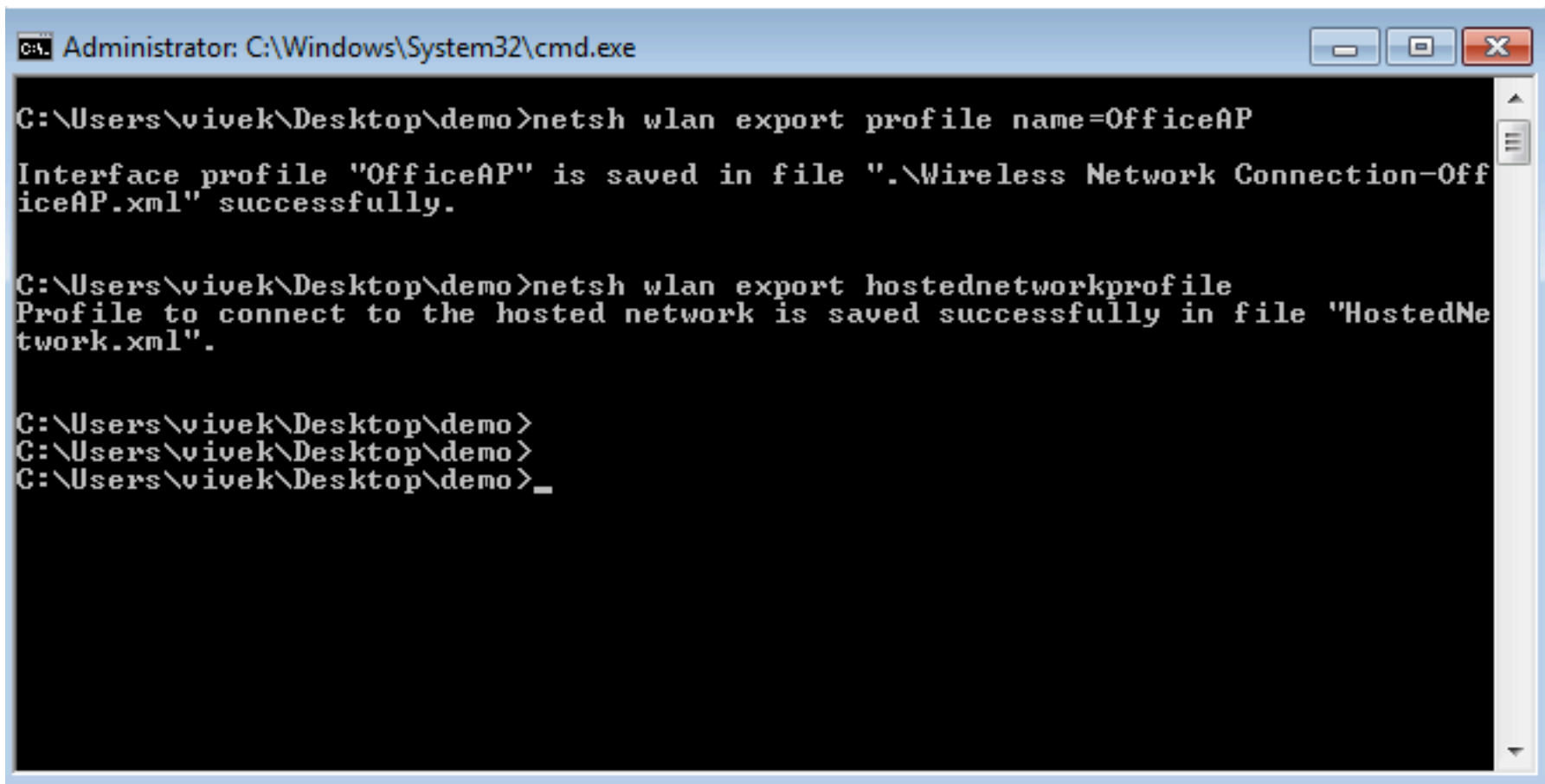
Hosted Network Encryption

- Uses WPA2-PSK for encryption
 - Key is encrypted in configuration file
 - Can be decrypted 😊
-
- What if there is an office network configured on the same machine with WPA2-PSK?

1. Infect Authorized Computer and Decrypt Passphrase



Alternate – Dump and Copy



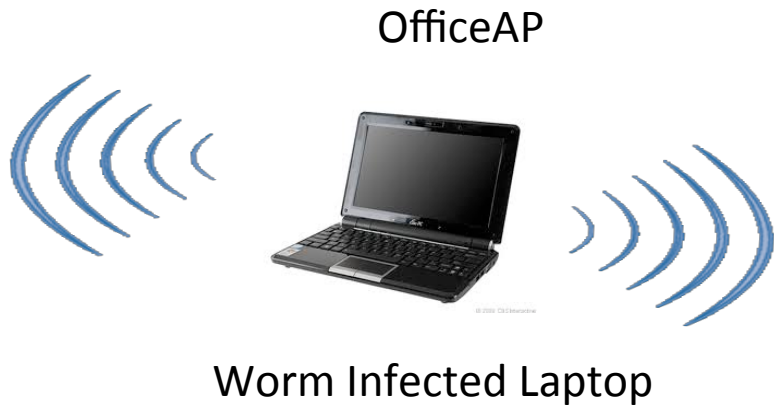
```
Administrator: C:\Windows\System32\cmd.exe

C:\Users\vivek\Desktop\demo>netsh wlan export profile name=OfficeAP
Interface profile "OfficeAP" is saved in file ".\Wireless Network Connection-OfficeAP.xml" successfully.

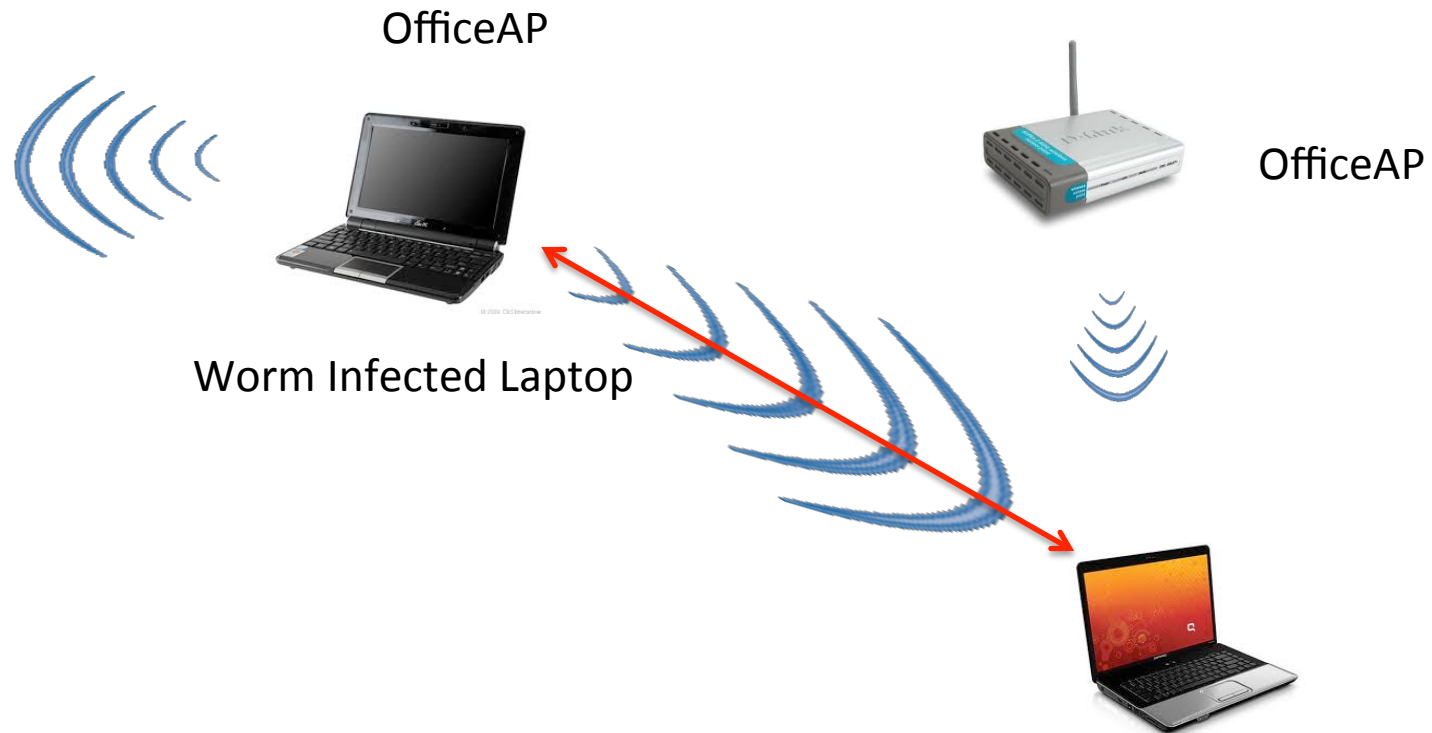
C:\Users\vivek\Desktop\demo>netsh wlan export hostednetworkprofile
Profile to connect to the hosted network is saved successfully in file "HostedNetwork.xml".

C:\Users\vivek\Desktop\demo>
C:\Users\vivek\Desktop\demo>
C:\Users\vivek\Desktop\demo>_
```

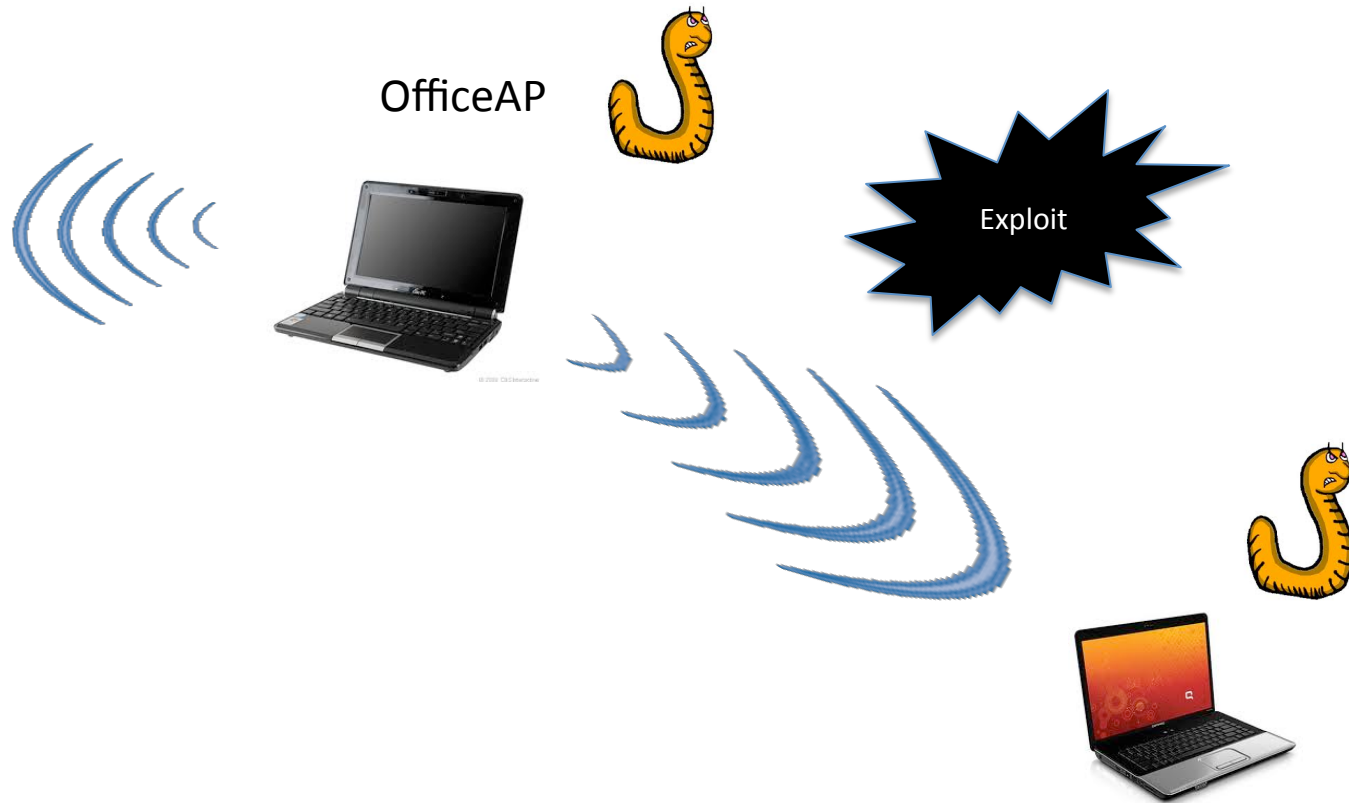
2. Create a Soft Access Point with the same Credentials



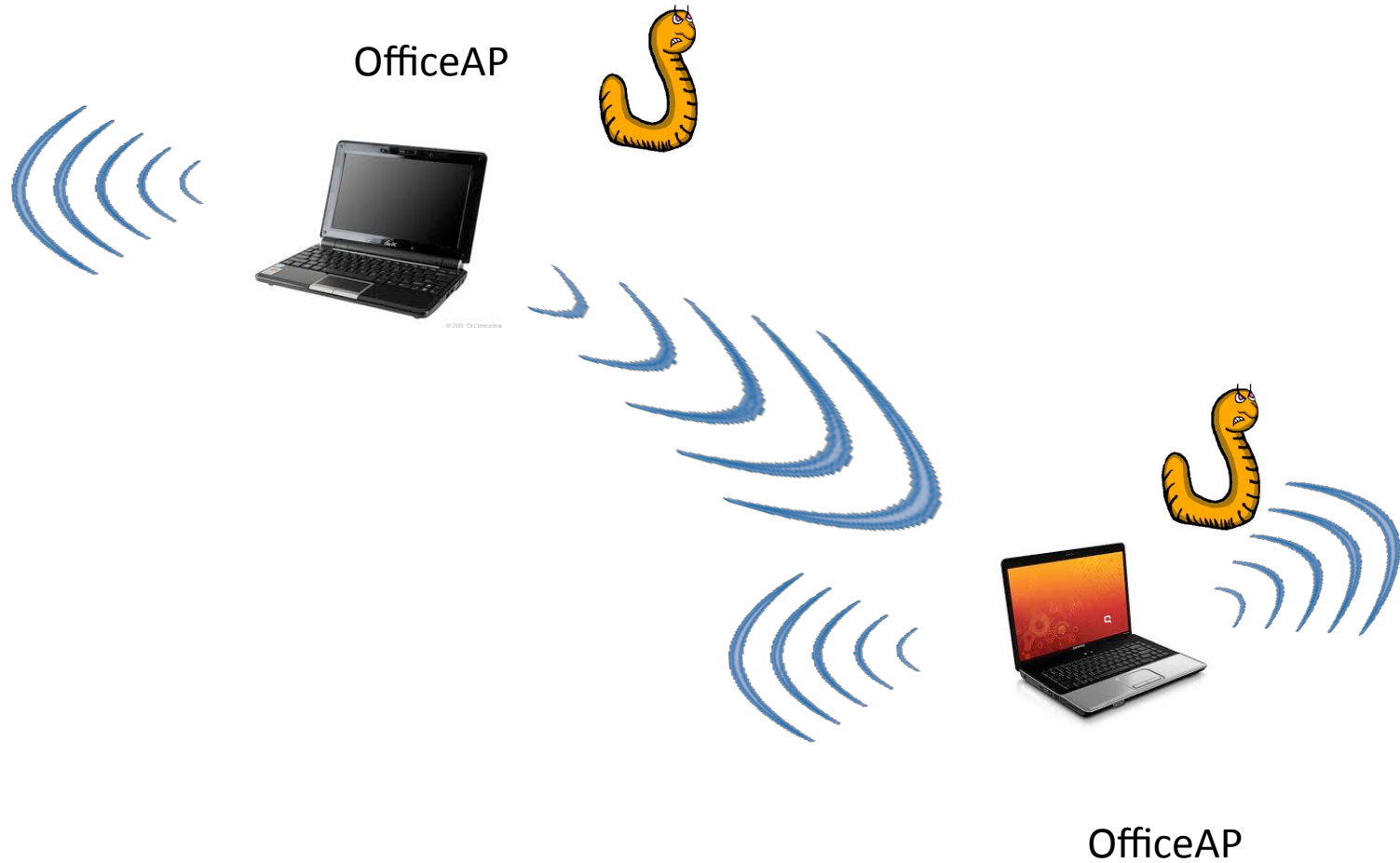
3. Signal Strength Game



4. Hop and Exploit



5. Replicate and Spread



Worms Wi-Fi Network Signal Strength > AP



Wi-Fi Worm

- Retrieve the network key for the network
- Create a hosted network with the same name
- When the victim is in the vicinity of his office, worm can be activated
- At some point the signal strength may be higher than real AP
- Other colleagues laptops may hop and connect
 - Conference rooms, Coffee and Break areas

Why is this interesting?

- Worm uses its own private Wi-Fi network to propagate
- Does not use the Wired LAN at all
- Difficult for network defenses to detect and mitigate 😊
- Targeted APT against an Enterprise

APIs for the Hosted Network Feature

Functions used	Description
WlanHostedNetworkForceStart , WlanHostedNetworkStartUsing	Start the wireless Hosted Network.
WlanHostedNetworkForceStop , WlanHostedNetworkStopUsing	Stop the wireless Hosted Network.
WlanHostedNetworkInitSettings , WlanHostedNetworkSetSecondaryKey , WlanHostedNetworkRefreshSecuritySettings	Configure wireless Hosted Network settings (change the SSID, change the secondary key, or request that the primary key is regenerated).
WlanHostedNetworkQueryStatus , WlanHostedNetworkQuerySecondaryKey , WlanHostedNetworkQueryProperty	Query the wireless Hosted Network settings and information (status, SSID, secondary key, primary key, or a list the devices currently connected).

DVD Contents

WLAN Megaprimer Video List

- ✂ Megaprimer Home
- ✂ Part 1: Getting Started
- ✂ Part 2: Bands, Channels And Sniffing
- ✂ Part 3: Pwning Beacon Frames
- ✂ Part 4: Dissecting Ap-Client Connections
- ✂ Part 5: Dissecting Wlan Headers
- ✂ Part 6: Pwning Beacon Frames
- ✂ Part 7: Laughing Off Mac Filters
- ✂ Part 8: Hacking Wlan Authentication
- ✂ Part 9: Hotspot Attacks
- ✂ Part 10: Hacking Isolated Clients
- ✂ Part 11: Alfa Card Kung-Fu
- ✂ Part 12: Man-In-The-Middle Attack
- ✂ Part 13 : SSL Man-In-The-Middle Attacks
- ✂ Part 14: Wep In-Depth
- ✂ Part 15: Wep Cracking
- ✂ Part 16: Caffe Latte Attack Basics
- ✂ Part 17: Caffe Latte Attack Demo
- ✂ Part 18: Koreks Chopchop Attack
- ✂ Part 19: Fragmentation And Hirte Attack
- ✂ Part 20: Understanding WPA/WPA2
- ✂ Challenge 1: There Is No Patch For Stupidity
- ✂ Challenge 1 Solution
- ✂ Challenge 2: Know Thy Packets
- ✂ Challenge 2 Solution : Know Thy Packets
- ✂ Challenge 3: Never Underestimate Your Enemy
- ✂ Challenge 3 Solution: Never Underestimate Your Enemy
- ✂ Part 21: WPA-PSK
- ✂ Part 22: WPA-PSK Cracking
- ✂ Part 23: WPA2-PSK Cracking
- ✂ Part 24: Speeding Up WPA/WPA2 PSK Cracking
- ✂ Part 25: Mood Swings Of A Wandering Client
- ✂ Part 26: Cracking WPA/WPA2-PSK With Just The Client
- ✂ Part 27: Questions And Answers
- ✂ Part 28: WPA_Supplicant
- ✂ Part 29: Setting Up Freeradius-WPE On Backtrack
- ✂ Part 30: EAP-MD5 Basics And Demo
- ✂ Part 31: Cracking EAP-MD5 With EAPMD5Pass And EAPMD5Crack
- ✂ Part 32: EAP Types And PEAP Demo
- ✂ Part 33: Cracking PEAP
- ✂ Part 34: Cracking PEAP In A Windows Network
- ✂ Part 35: Cracking EAP-TTLS
- ✂ Part 36: Insecurity In 3rd Party Wi-Fi Utilities
- ✂ Conclusion And The Road Ahead

<http://www.securitytube.net/downloads>

Questions

Questions?