



# SharkFest '18 ASIA



## 05 - Sneaking in The Backdoor

Hacking the Non-Standard Layers



Phill “Sherlock” Shade

Merlion’s Keep Consulting



# Phillip “Sherlock” Shade (Phill)

phill.shade@gmail.com



- Certified instructor and internationally recognized network security and forensics expert with more than 30 years of experience
- Retired US Navy and the founder of Merlion’s Keep Consulting, a professional services company specializing in network and forensics analysis
- A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, and the IEEE and volunteer at Cyber Warfare Forum Initiative
- Holds numerous certifications, including Certified Network Expert (CNX)-Ethernet, CCNA, Certified Wireless Network Administrator (CWNA), and WildPackets Certified Network Forensics Analysis Expert (WNAX)
- Certified Wireshark University, Sniffer University and Planet 3 Wireless instructor

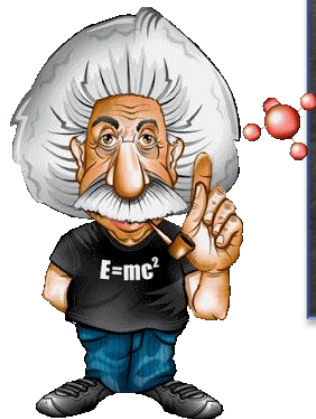




# Today's Agenda



1. Welcome to my World..... I'm not a good guy.....
2. Key Forensics Questions to Ask? and those Things You Have to Know - Overview and Terminology
3. What should I look For?
3. Exploiting the lower Layers – Cases Studies to Surprise and Impress (hopefully) you!





# Case Studies



1. *MK - Forensics Case Study #4 – Man-in-the-Middle*
2. *MK - WiFi - Attack - Denial of Silence (Extended)*
3. *Attack - MAC Flood - Capture 2 (macof) Switch*
4. *MK - Advanced Analysis Lab 8c / e / 9d*
5. *MK - Sample - IPv4 - IPv6 - Tunneled Ping*
6. *MK - Advanced Analysis Lab 8f - IPX Exploit*
7. *MK - IP Service Scan*
8. *Covert Channels-ping-example5.*





# Welcome to my World....







# Key Network Forensics Questions to Ask



1. What damage has been done?
2. Who was the intruder and how did they penetrate the existing security precautions?
3. What did they do? - (Did the intruder leave anything such as a new user account, a Trojan horse or perhaps some new type of Worm or Bot software behind?)
4. Is there sufficient data to analyze and reproduce the attack and verify the fix will work?



# For This to Work - Normal or Abnormal?



Source	Destination	Protocol	Length	Src Port	Dst Port	Info
Micro-St_70:13:b7	IPv6mcast_00:00:00:	SSDP	208	51760	1900	M-SEARCH * HTTP/1.1
Micro-St_70:13:b7	IPv6mcast_00:00:00:	SSDP	208	51760	1900	M-SEARCH * HTTP/1.1
Micro-St_70:13:b7	Netgear_52:9e:a0	DNS	71	58501	53	Standard query A www.cnn.com
Netgear_52:9e:a0	Micro-St_70:13:b7	DNS	288	53	58501	Standard query response A 157.166.255.19
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	66	65045	80	65045 > 80 [SYN] Seq=419029810 win=8192 L
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	66	80	65045	80 > 65045 [SYN, ACK] Seq=1914813027 Ack=
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	54	65045	80	65045 > 80 [ACK] Seq=419029811 Ack=191481
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	1448	65045	80	[TCP segment of a reassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e:a0	TCP	1448	65045	80	[TCP segment of a reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Micro-St_70:13:b7	Netgear_52:9e:a0	HTTP	1194	65045	80	GET / HTTP/1.1
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	60	80	65045	80 > 65045 [ACK] Seq=1914813028 Ack=41903
Netgear_52:9e:a0	Micro-St_70:13:b7	TCP	1448	80	65045	[TCP segment of a reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:13:b7					reassembled PDU]
Micro-St_70:13:b7	Netgear_52:9e:a0					Seq=419033739 Ack=191481
Netgear_52:9e:a0	Micro-St_70:13:b7					reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:13:b7					reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:13:b7					Seq=419033739 Ack=191481
Netgear_52:9e:a0	Micro-St_70:13:b7					reassembled PDU]
Netgear_52:9e:a0	Micro-St_70:13:b7					reassembled PDU]



**Forensics Analysis Tip:** Be familiar with the expected or Baseline behavior of protocols before trying to identify suspect behavior!



# The Key – Reference / Baseline Files



- How can you recognize suspicious behavior unless you understand the expected behavior of a protocol?
- This is where the use of known-good reference or baseline files becomes important!
  - Reference files of standard network activities
  - Samples of network device behavior
  - Many devices, Scanning tools, Exploits, Hackers have specific signatures or patterns that can be used to identify a specific behavior







# So...



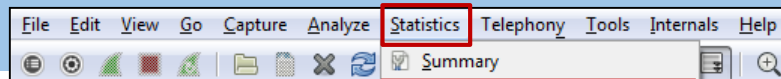
## Where do I Get Samples to Start With?

- <http://packetlife.net/captures/>
- <http://www.pcapr.net>
- <http://www.netresec.com/?page=PcapFiles>
- <https://wiki.wireshark.org/SampleCaptures>
- <http://ambitwire.com/useful-links/public-pcap-repositories/link/public-pcap-repositories-ambitwires-ultimate-collection>
- <http://contagiodump.blogspot.nl/2013/04/collection-of-pcap-files-from-malware.html>
- <https://www.evilmfingers.com/repository/pcaps.php>
- <https://www.bro.org/community/traces.html>
- <http://www.secrepo.com/>

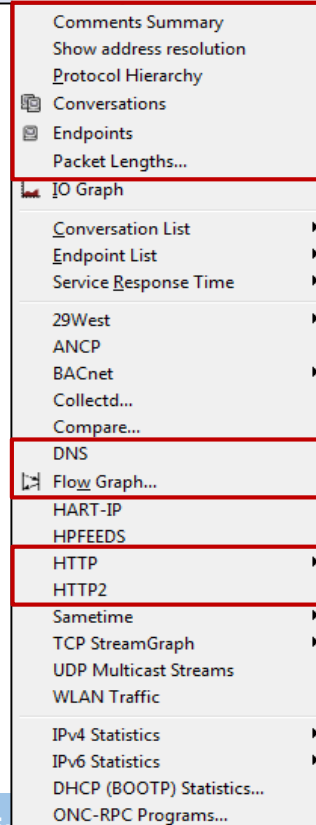
**Forensics Analysis Tip:** For specific requests, email me! [Phill.shade@gmail.com](mailto:Phill.shade@gmail.com)



# What Should I Look For?



- ⚠ Unusual communication pairs
- ⚠ Unusual protocols and ports
- ⚠ Excessive failed connections
- ⚠ Suspicious inbound connections
- ⚠ Suspicious Outbound Connections
- ⚠ Suspicious DNS Queries / Replies





# Let's Have Some Fun...



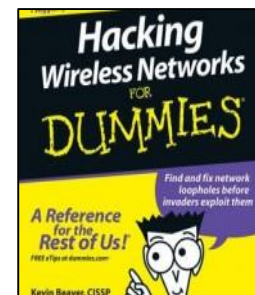
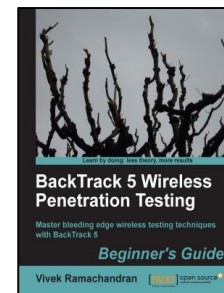
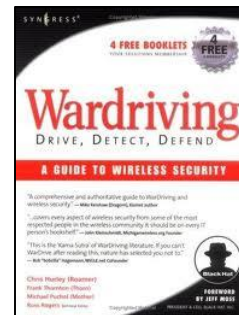
Trust me... I'm  
here to help...



# #1 - First We Need Some Tools...

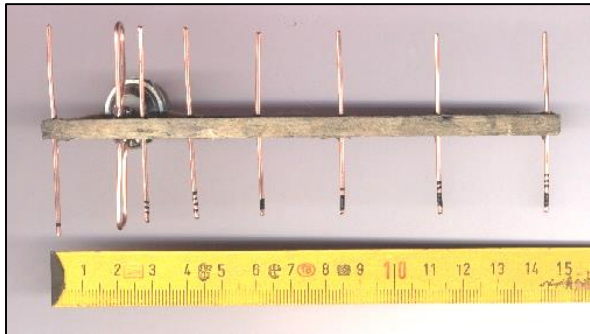
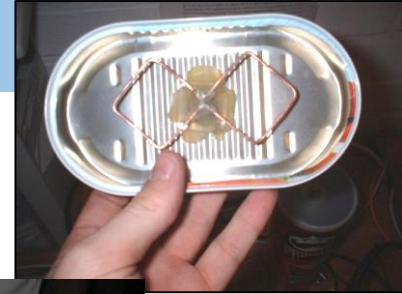


- Portable computer
  - Capture device such as AirPcap
  - Wireless card
- Software
  - Wireless Network analysis Tool
    - Wireshark
    - Aircrack-ng
    - NetStumbler
    - Kismet
    - Air-Jack (and variants)
  - Vendor-provided "discovery and configuration" tools
    - Cisco Aironet Utilities





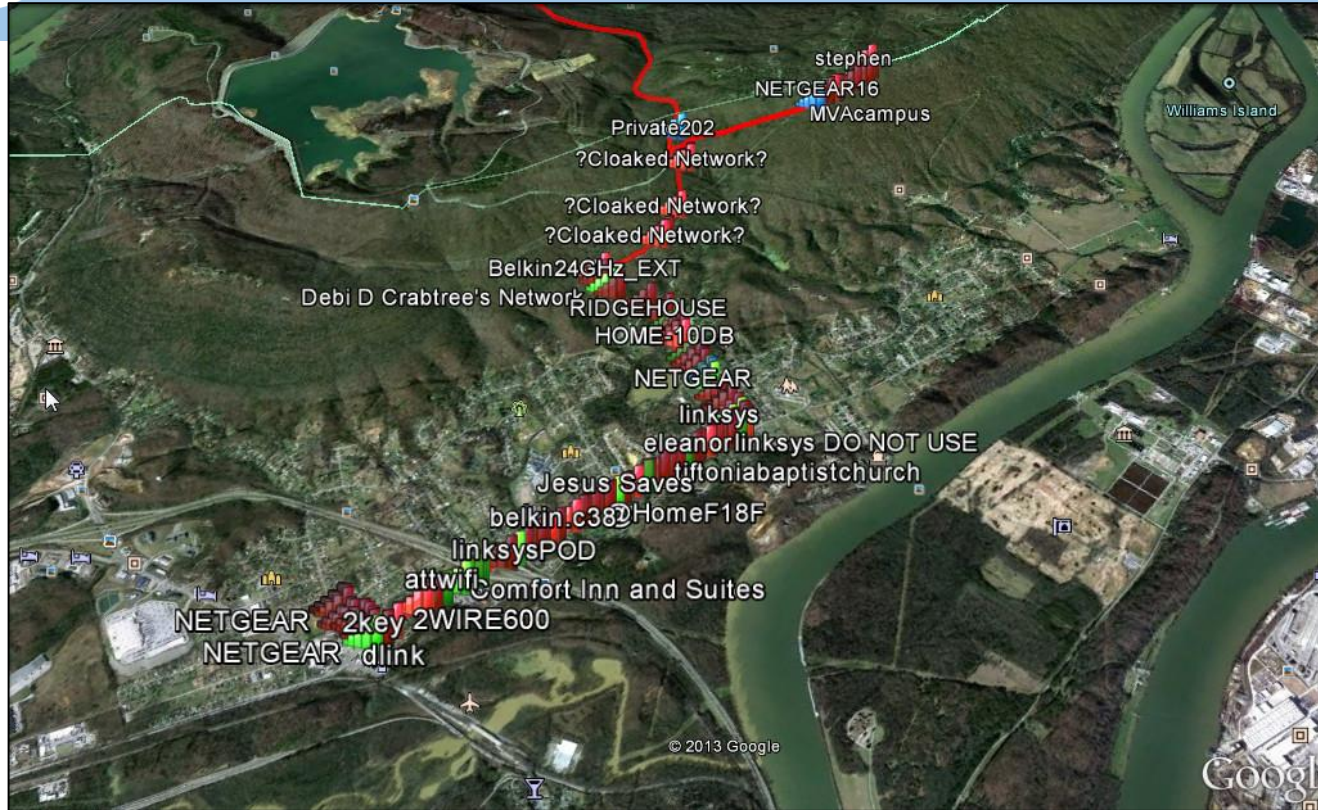
# #2 - Now We Need an Antenna...







# #3 - Now We Need a Target...







# Follow Along in the Pcap: *MK - Forensics Case Study #4*



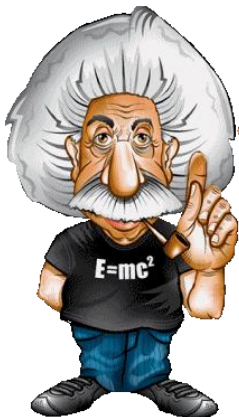


# Layer 2 - Case Study: Man-in-the-Middle Attack



## Setting the Stage...

1. A major network analysis vendor had been working on a key project for two years
2. One week prior to product launch, a competitor trademarked the primary and secondary names for the product
3. Company was forced to research, develop, and produce an entirely new marketing campaign, literature, and product documentation
4. A forensics investigation aided by the company's data recorders revealed that the software company had been "Man-in-the-Middle" victimized
5. Cost to company was in excess of \$4,000,000 USD





# Scene of the Crime...





# Forensic Reconstruction of the Crime...



Before Intrusion



No Encryption



No Encryption



After  
Intrusion



Dual-Radio Access Point





# ARP Poison in Progress



No.	Source	Destination	Time	Length	Protocol	Info
990	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
991	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
992	IntelCor_ac:b1:5e	IntelCor_ac:b1:3e	137.161139	60	ARP	Who has 192.168.60.3? Tell 192.168.60.1
993	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
994	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
995	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
996	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
997	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
998	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
999	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1000	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1001	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1002	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1003	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1004	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1005	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1006	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1007	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl
1008	IntelCor_ac:b1:3e	CiscoInc_cd:fe:d0	137.161157	42	ARP	192.168.60.3 is at 00:02:b3:ac:b1:3e (dupl

The device **IntelCor\_ac:b1:5e** is attempting to trick the Projector (CiscoInc\_cd-fe-do) into thinking it is the client while making the client (**IntelCor\_ac:b1:3e**) think it is the Projector.





# Results of the Investigation...



The results of the internal Forensic Investigation revealed several findings:

1. The original Wired Projector in the executive conference room had been replaced with an unauthorized WiFi model (that did not support any type of NAC or encryption)
2. Encryption was switched off on the presenters laptop to enable connecting to the WiFi projector
3. Rogue Access point was located outside conference room in a tree!





# Follow Along in the Pcap: *MK - WiFi - Attack - Denial of Silence (Extended)*





# WiFi Layer 1 - Denial of Silence Attack



MK - WLAN Attack - Denial of Silence (Extended)1.pcap [Phill's Magical Mystery Machine - Wireless Configuration]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + 802.11 Beacons 802.11 Data 802.11

No.	Source	Destination	BSS Id	ESSID	Time	Delta Time	Size	Protocol
1	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		0.000000	0.000000	59	802.11
2	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	0.000000	0.000000	67	802.11
3	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		28.761356	28.761356	59	802.11
4	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	28.761356	0.000000	67	802.11
5	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		57.522711	28.761355	59	802.11
6	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	57.532726	0.010015	67	802.11
7	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		86.294082	28.761356	59	802.11
8	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	86.294082	0.000000	67	802.11
9	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		115.065454	28.771372	59	802.11
10	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	115.065454	0.000000	67	802.11
11	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		143.826813	28.761359	59	802.11
12	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	143.826813	0.000000	67	802.11
13	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		172.598182	28.771369	59	802.11
14	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	172.598182	0.000000	67	802.11
15	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		201.359539	28.761357	59	802.11
16	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	201.359539	0.000000	67	802.11
17	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		230.130911	28.771372	59	802.11
18	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	230.130911	0.000000	67	802.11
19	DeltaNet_20:c7:9a	HewlettP_6e:6a:6d	00:30:ab:20:c7:9a		258.892267	28.761356	59	802.11
20	PlanetTe_2f:cd:41	HewlettP_57:42:1b	00:30:4f:2f:cd:41	TS-Public	258.892267	0.000000	67	802.11



# WiFi Attack – Denial of Silence Details



```
1 DeltaNet_20:c7:9a HewlettP_6e:6a:6d 0.000000 0.000000 IEEE 802.11 59 Association Request, SN=3047, FN=0, Flags...
+ Frame 1: 59 bytes on wire (472 bits), 59 bytes captured (472 bits)
- IEEE 802.11 Association Request, Flags: .....
  Type/Subtype: Association Request (0x00)
  Frame Control: 0x0000 (Normal)
  Version: 0
  Type: Management frame (0)
  Subtype: 0
  Flags: 0x0
  .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To
  .... ..0.. = More Fragments: This is the last fragment
  .... 0... = Retry: Frame is not being retransmitted
  ...0 .... = PWR MGT: STA will stay up
  ..0. .... = More Data: No data buffered
  .0.. .... = Protected flag: Data is not protected
  0.... .... = Order flag: Not strictly ordered
  Duration: 8189
  Destination address: HewlettP_6e:6a:6d (00:02:a5:6e:6a:6d)
  Source address: DeltaNet_20:c7:9a (00:30:ab:20:c7:9a)
  BSS id: DeltaNet_20:c7:9a (00:30:ab:20:c7:9a)
  Fragment number: 0
  Sequence number: 3047
- IEEE 802.11 wireless LAN management frame
  Fixed parameters (4 bytes)
  Capability Information: 0xE2D2
  .... ..0 = ESS capabilities: Transmitter is a STA
  .... ..1. = IBSS status: Transmitter belongs to an IBSS
  .... ..1. .... 00.. = CFP participation capabilities: Unknown (0x0080)
  .... ..1 .... = Privacy: AP/STA can support WEP
  .... ..0. .... = Short Preamble: Short preamble not allowed
  .... ..1. .... = PBCC: PBCC modulation allowed
  .... ..1... .... = Channel Agility: Channel agility in use
  .... ..0 .... .... = Spectrum Management: dot11SpectrumManagementRequired FALSE
  .... ..0.. .... .... = Short Slot Time: Short slot time not in use
  .... 0... .... .... = Automatic Power Save Delivery: apsd not implemented
  ..1. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation allowed
  .1.. .... .... .... = Delayed Block Ack: delayed block ack implemented
  1... .... .... .... = Immediate Block Ack: immediate block ack implemented
  Listen Interval: 0xc70e
```

Management Frame Type

Network Allocation Vector (NAV) – Duration ID in seconds

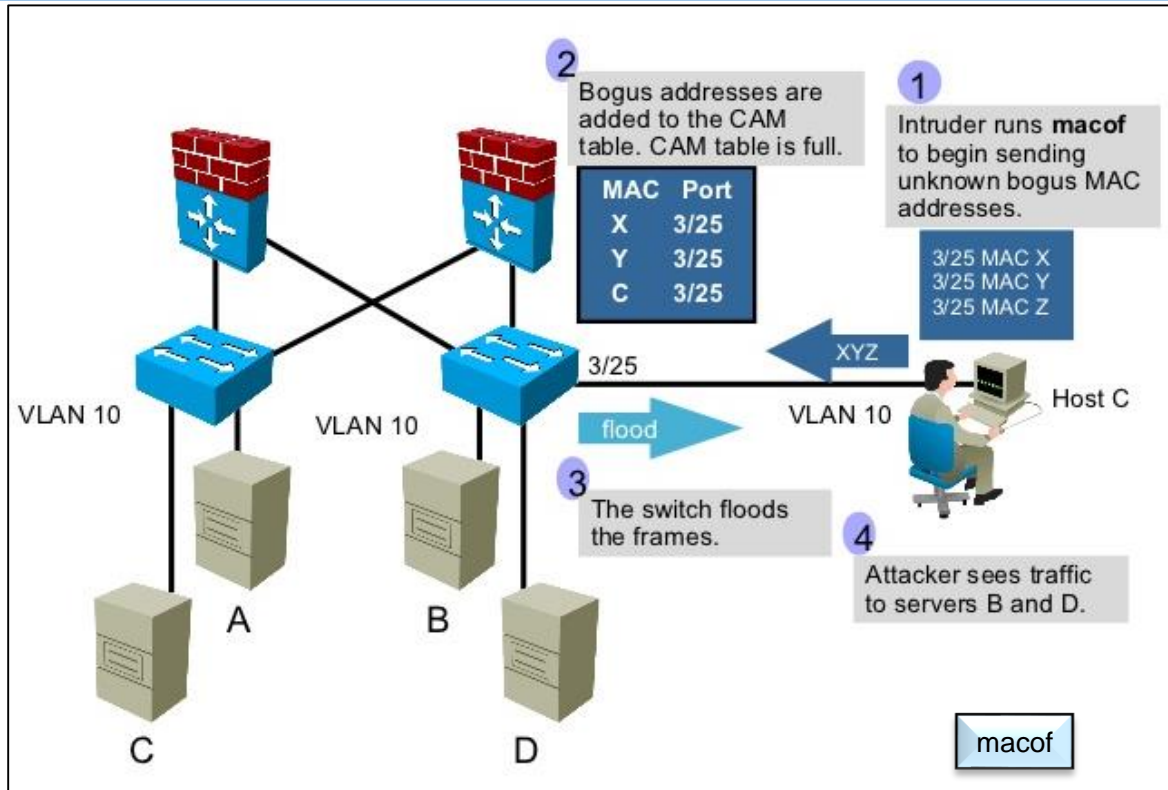


# Follow Along in the Pcap: *Attack - MAC Flood - Capture 2 (macof) Switch*





# Layer 2 - MAC / CAM Table Overflow Attacks









# Follow Along in the Pcap: *MK - Advanced Analysis Lab 8c / e / 9d*





# Layer 3 - IPv4 Options



- Default length of the IP header is 20 bytes (Greater than 20 bytes indicates the presence of IP options)
  - Many options have been present since the early days of IP and continue to be added.
    - Most are rare and few protocols take advantage of them— one of the few protocols that does is IGMP
    - Many of these options can be generated via the DOS ping command – Type ‘ping -?’ for a list of options
  - Some of the options lend themselves to exploit potential

```
C:\>ping -?
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v IOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] target_name

Options:
  -t             Ping the specified host until stopped.
                To see statistics and continue - type Control-Break;
                To stop - type Control-C.
  -a             Resolve addresses to hostnames.
  -n count      Number of echo requests to send.
  -l size        Send buffer size.
  -f             Set Don't Fragment flag in packet.
  -i TTL        Time To Live.
  -v IOS        Type Of Service.
  -r count      Record route for count hops.
  -s count      Timestamp for count hops.
  -j host-list  Loose source route along host-list.
  -k host-list  Strict source route along host-list.
  -w timeout    Timeout in milliseconds to wait for each reply.
```



# IPv4 Options Details



```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.1 (192.168.1.1)
  Version: 4
  Header length: 56 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..0. = ECN-Capable Transport (ECT): 0
    .... ...0 = ECN-CE: 0
  Total Length: 96
  Identification: 0x3516 (13590)
  Flags: 0x00
    0... = Reserved bit: Not set
    .0.. = Don't fragment: Not set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 128
  Protocol: ICMP (0x01)
  Header checksum: 0x2fa6 [correct]
    [Good: True]
    [Bad : False]
  source: 192.168.1.106 (192.168.1.106)
  Destination: 192.168.1.1 (192.168.1.1)
  Options: (36 bytes)
    Time stamp:
      Pointer: 5
      Overflow: 0
      Flag: Time stamp and address
      Address = -, time stamp = 0
      Address = -, time stamp = 0
      Address = -, time stamp = 0
      Address = -, time stamp = 0
```

***Forensics Analysis Tip:*** IP options are very often used in exploits – although some exceptions include IGMP and other routing protocols



# Layer 3 Exploit - Record Route - Ping (-r)



```
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 192.168.1.1 (192.168.1.1)
  Version: 4
  Header length: 60 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 100
    Identification: 0x369a (13978)
  Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
  Header checksum: 0x6b1c [correct]
    Source: 192.168.1.106 (192.168.1.106)
    Destination: 192.168.1.1 (192.168.1.1)
  Options: (40 bytes)
    Record route (39 bytes)
      Pointer: 4
      - <- (current)
      -
      Reply from 4.2.2.1: bytes=32 time=50ms TTL=245
      Route: 65.1.11.102 ->
             68.152.252.190 ->
             205.152.146.42 ->
             65.83.237.93 ->
             172.25.69.230 ->
             172.25.69.228 ->
             4.68.1.140 ->
             209.247.11.243 ->
             209.247.11.245
    EOL
```

```
C:\>ping -n 15 -r 9 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
```

The Route Data field contains the list of routers from source to destination

**Forensics Analysis Tip:** Presence of IP Option: Record Route is a probable indication of a network under reconnaissance by an intruder with the goal of identifying routers to attack



# Layer 3 Router Exploit – Loose / Strict Source Routing (-J)



```
D:\WP>ping -j 10.1.1.254 10.1.1.33

Pinging 10.1.1.33 with 32 bytes of data:

Reply from 10.1.1.33: bytes=32 time=5ms TTL=127
Route: 10.1.1.254
```

No. -	Source	Destination	Protocol	Info	
1	NxpSemic_00:	Broadcast	ARP	who has 10.1.1.254?	
2	Cisco_cb:50:	NxpSemic_00:	ARP	10.1.1.254 is at 00:e	
3	10.1.1.33	10.1.1.254	ICMP	Echo (ping) reply	
4	10.1.1.33	10.1.1.5	ICMP	Echo (ping) reply	
5	10.1.1.5	10.1.1.254	ICMP	Echo (ping) request	
6	10.1.1.5	10.1.1.33	ICMP	Echo (ping) request	
7	10.1.1.33	10.1.1.254	ICMP	Echo (ping) reply	
8	10.1.1.33	10.1.1.5	ICMP	Echo (ping) reply	
9	10.1.1.5	10.1.1.254	ICMP	Echo (ping) request	
10	10.1.1.5	10.1.1.33	ICMP	Echo (ping) request	
11	10.1.1.33	10.1.1.254	ICMP	Echo (ping) reply	
12	10.1.1.33	10.1.1.5	ICMP	Echo (ping) reply	
13	10.1.1.5	10.1.1.254	ICMP	Echo (ping) request	82
14	10.1.1.5	10.1.1.33	ICMP	Echo (ping) request	82
15	10.1.1.33	10.1.1.254	ICMP	Echo (ping) reply	82

```
Internet Protocol, Src: 10.1.1.33 (10.1.1.33), Dst: 10.1.1.254 (10.1.1.254)
Version: 4
Header length: 28 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... ..0. = ECN-Capable Transport (ECT): 0
.... ...0 = ECN-CE: 0
Total Length: 68
Identification: 0x8d57 (36183)
Flags: 0x00
0... = Reserved bit: Not set
..0. = Don't fragment: Not set
...0. = More fragments: Not set
Fragment offset: 0
Time to live: 128
Protocol: ICMP (0x01)
Header checksum: 0x072f [correct]
Source: 10.1.1.33 (10.1.1.33)
Destination: 10.1.1.254 (10.1.1.254)
Options: (8 bytes)
Loose source route (7 bytes)
Pointer: 4
10.1.1.5 <- (current)
EOL
```

***Forensics Analysis Tip:*** This option allows a packet sender to override a router's normal forwarding process and potentially sneak packets past firewalls



# Follow Along in the Pcap: *MK - Sample - IPv4 - IPv6 - Tunneled Ping*







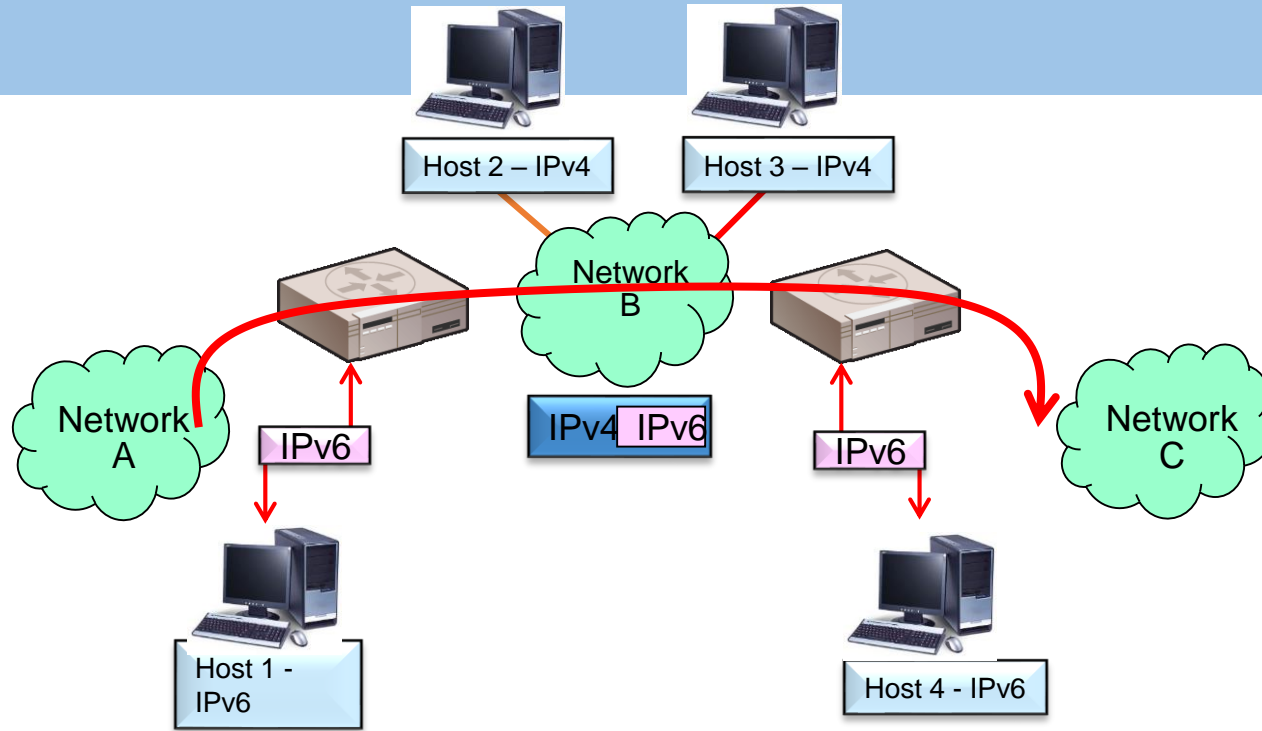
# Layer 3 - Emerging IPv6 Trends



- Exhaustion of available IPv4 addresses in February 2011 forced many IP Address changes:
  - Significant increase in the use of Network Address Translation (NAT) and related use of "Private" IPv4 addressing
  - Most applications and devices have migrated to IPv6
  - Most Operating Systems now enable IPv6 compatibility as a default (dual stack)
    - Windows XP pro + / Linux Redhat 2.4+ / etc...
- Criminals / Hackers elements of the Internet have embraced IPv6 in a large part due to the perceived unfamiliarity of Law Enforcement community as well as the shortcomings of many of the current generation of LE tools
  - New Attacks and Exploits are emerging to take advantage of this



# Layer 3 - Interfacing IPv4 with IPv6: Tunneling



Note: IPv6 packets must be encapsulated before traversing the IPv4 network



# Layer 3 Exploit – IPv6 Tunnel Attack



```
▣ Frame 12: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
▣ Ethernet II, Src: CiscoInc_18:a6:71 (00:19:06:18:a6:71), Dst: CiscoInc_7c:77:a0 (00:0c:29:7c:77:a0)
▣ Internet Protocol Version 4, Src: 10.0.4.2, Dst: 10.0.4.1
▣ Internet Protocol Version 6, Src: 2006:0:b::1, Dst: 2006:0:2::1
    0110 .... = Version: 6
    ▣ .... 0000 0000 .... .. = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .. 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 60
    Next header: ICMPv6 (58)
    Hop limit: 64
    Source: 2006:0:b::1
    Destination: 2006:0:2::1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▣ Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x27fd [correct]
    Identifier: 0x215e
    Sequence: 4
    \[Response To: 11\]
    [Response Time: 0.475 ms]
    ▣ Data (52 bytes)
```

***Forensics Analysis Tip:*** Since IPv6 tunnels over IPv4 are transparent, the best way to identify their use within a network is by setting a series of capture filters on a network analyzer located within the firewall or DMZ



# Follow Along in the Pcap: *MK - Advanced Analysis Lab 8f*





- Service Advertising Protocol (SAP) is included in the IPX protocol
- Used to make the process of adding and removing services dynamic in IPX enabled network
  - As devices join or leave the network, they may advertise their services as joining or leaving the network using SAP





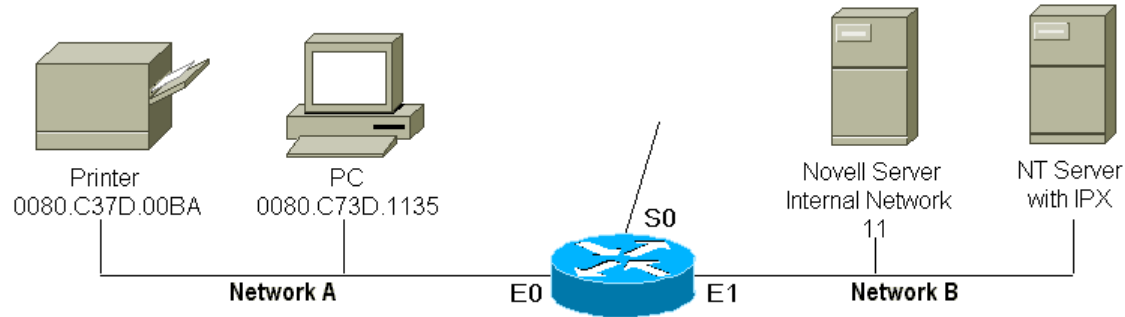
# Layer 3 - IPX SAP Header - Details



```
⊕ Internetwork Packet eXchange
  ⊖ Service Advertisement Protocol
    SAP packet type: General Response (2)
      ⊖ Server Name: 080009AC14FF03CT!ORTHO_PRINT
        Server Type: Intel Netport 2 or HP JetDirect or HP Quicksilver (0x030c)
        Network: 00 (0x00000004)
        Node: HP_ac:14:ff (08:00:09:ac:14:ff)
        Socket: HP LaserJet/QuickSilver (0x400c)
        Intermediate Networks: 1

0000 ff ff ff ff ff ff 08 00 09 ac 14 ff 00 60 ff ff ..... ..
0010 00 60 00 00 00 00 00 04 ff ff ff ff ff ff 04 52 `.....R
0020 00 00 00 04 08 00 09 ac 14 ff 04 52 00 02 03 0c .....R....
0030 30 38 30 30 30 39 41 43 31 34 46 46 30 33 43 54 080009AC 14FF03CT
0040 21 4f 52 54 48 4f 5f 50 52 49 4e 54 00 00 00 00 !ORTHO_P RINT....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 04 08 00 09 ac 14 ff 40 0c 00 01 .....@...
```

# Layer 3 - IPX SAP in Operation



```
IPX Routing 0000.0C34.E923

interface ethernet 0
 ipx network A

interface ethernet 1
 ipx network B
```

<u>Device</u>	<u>Network</u>	<u>Node</u>
Printer	A	0080.C73D.00BA
PC	A	0080.C73D.1135
RTR-E0	A	0000.0C34.C923
RTR-E1	B	0000.0C29.DCFA
Novell Server (Int)	11	0000.0000.0001
Novell Server (Ext)	B	0000.1B3D.5678



# Layer 3 - IPX SAP Exploits



- Compromise IPX SAP enabled devices (such as Printers and Servers) to inject malware from inside the network
- Spoof IPX / SAP enabled printers to steal network or printer traffic
  - Man-in-the-Middle
- Use IPX SAP enabled devices as basis for a Escalation of Privileges attack





# Follow Along in the Challenge Pcap: *MK - IP Service Scan*





# Follow Along in the Challenge Pcap: *Covert Channels-ping-example*







# Questions and Answers / Discussion

7



# Instructor Contact Information



Phill Shade: [phill.shade@gmail.com](mailto:phill.shade@gmail.com)

LinkedIn: Phill “Sherlock” Shade

Merlion’s Keep Consulting: [merlions.keep@gmail.com](mailto:merlions.keep@gmail.com)

International: [info@cybersecurityinstitute.eu](mailto:info@cybersecurityinstitute.eu)



Merlion’s Keep Consulting & Training

---

*Packets Never Lie*

