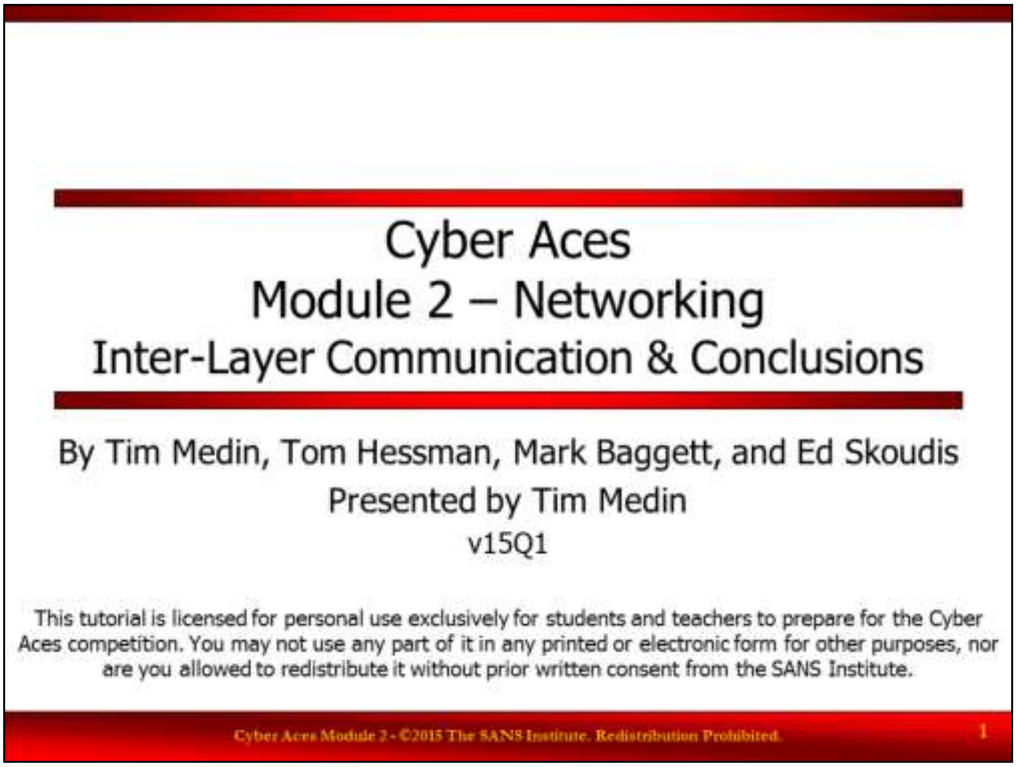


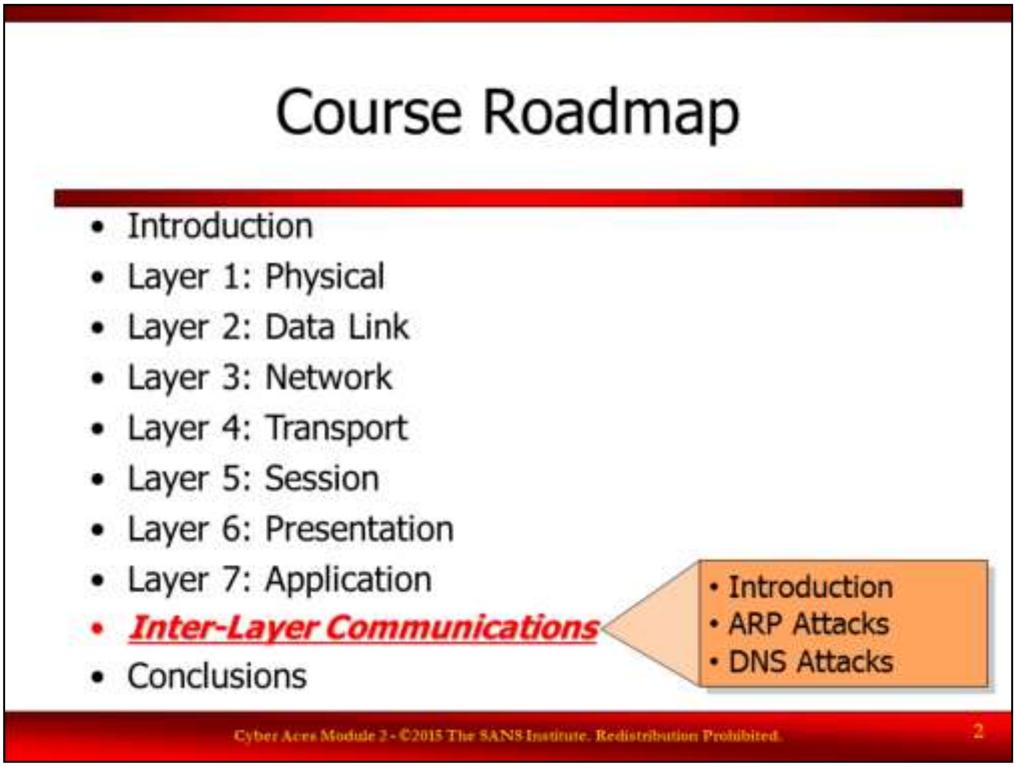
Cyber Aces
Module 2 – Networking
Inter-Layer Communication & Conclusions

By Tim Medin, Tom Hessman, Mark Baggett, and Ed Skoudis

Presented by Tim Medin

v15Q1

Welcome to Cyber Aces, Module 2! A firm understanding of network fundamentals is essential to being able to secure a network or attack one. This section provides a broad overview of networking, covering the fundamental concepts needed to understand computer attacks and defenses from a network perspective.



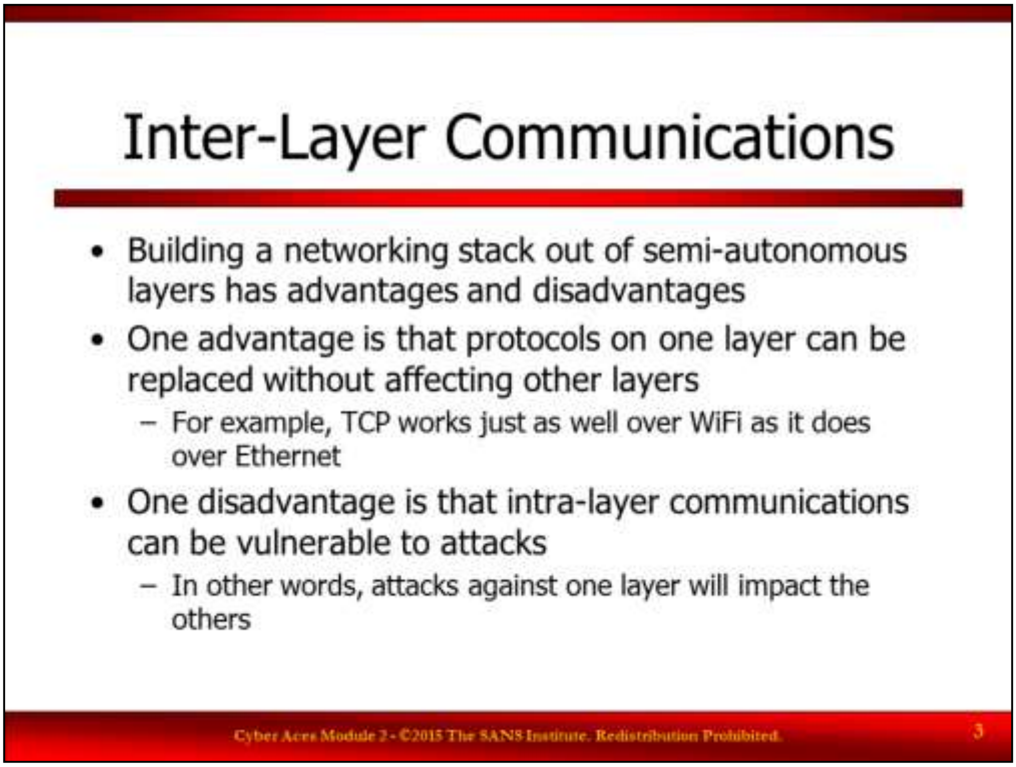
Course Roadmap

- Introduction
- Layer 1: Physical
- Layer 2: Data Link
- Layer 3: Network
- Layer 4: Transport
- Layer 5: Session
- Layer 6: Presentation
- Layer 7: Application
- ***Inter-Layer Communications***
- Conclusions

- Introduction
- ARP Attacks
- DNS Attacks

Course Roadmap

In this short section, you'll be introduced to a few attacks that are possible due to the interaction between layers of the OSI model, such as ARP and DNS attacks.



Inter-Layer Communications

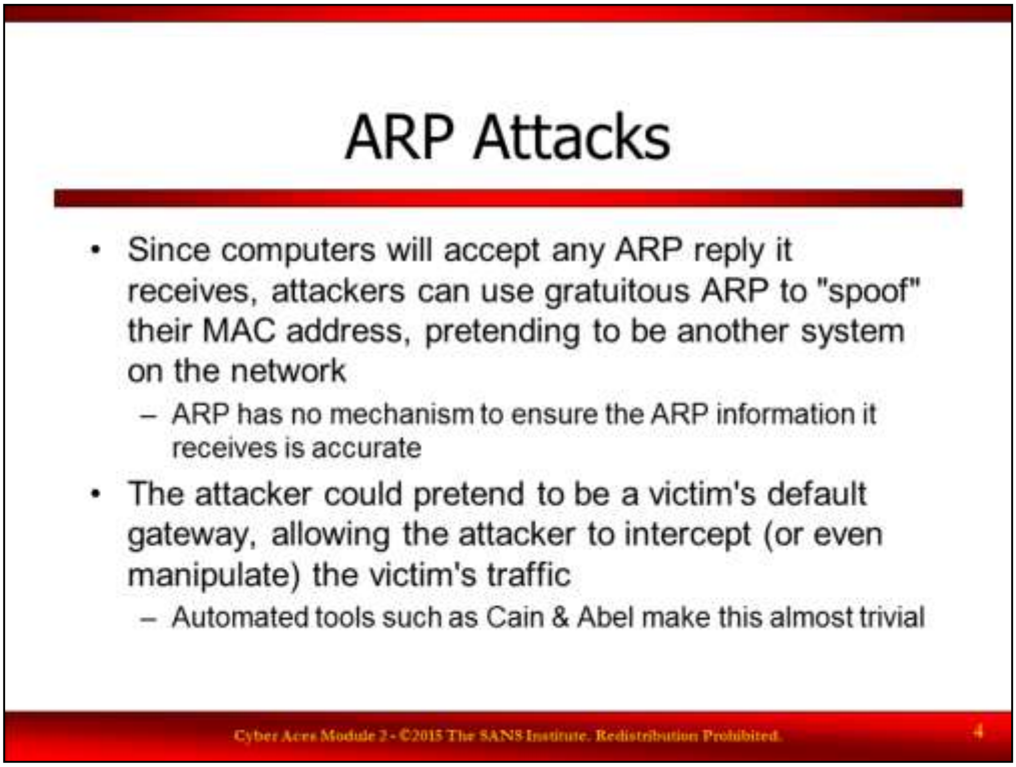
- Building a networking stack out of semi-autonomous layers has advantages and disadvantages
- One advantage is that protocols on one layer can be replaced without affecting other layers
  - For example, TCP works just as well over WiFi as it does over Ethernet
- One disadvantage is that intra-layer communications can be vulnerable to attacks
  - In other words, attacks against one layer will impact the others

3

Inter-Layer Communications

Building our networking stack out of semi-autonomous layers has its advantages and disadvantages. One advantage is that we can easily replace layers with other protocols without affecting the operations of the rest of the stack. For example, TCP/ IP can operate over a wireless network exactly the same way it operates over Ethernet without any knowledge of the underlying protocol. The downside is that the intra-layer communications can be vulnerable to attacks.

Imagine a soldier who is sitting in a fully armored Abrams Tank. While he is in the tank he is safe from most small arms fire attacks. At night he sleeps in a fully armored bunker where he is also safe from small arms fire. However, the soldier is still highly vulnerable to attack as he moves from the tank to the bunker. Likewise, the connection points between secure systems and layers in computer networks are often vulnerable to attacks. This is also true for the OSI model. Let's look at a connection between Layers 2 and 3 (ARP) and a connection between Layer 7 and 3 (DNS) and how these mappings between the layers create weakness in the communications stack.



ARP Attacks

- Since computers will accept any ARP reply it receives, attackers can use gratuitous ARP to "spoof" their MAC address, pretending to be another system on the network
  - ARP has no mechanism to ensure the ARP information it receives is accurate
- The attacker could pretend to be a victim's default gateway, allowing the attacker to intercept (or even manipulate) the victim's traffic
  - Automated tools such as Cain & Abel make this almost trivial

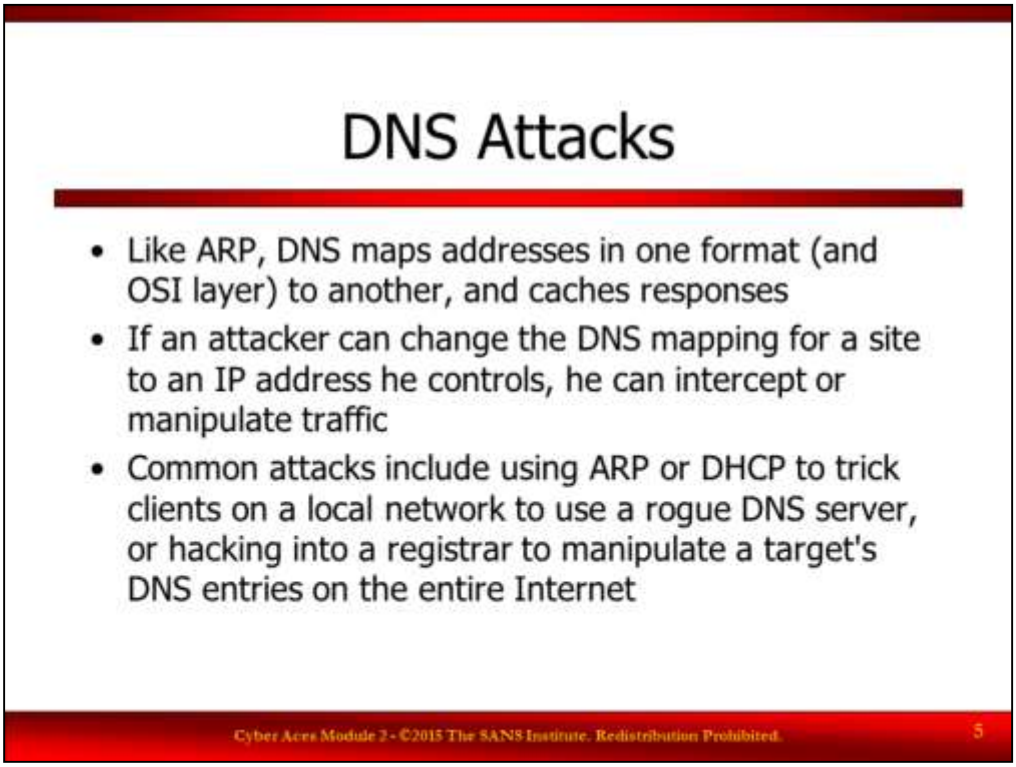
ARP Attacks

Since the host that receives the response to their ARP broadcast has no way to verify the information it received was accurate, attackers can lie about their MAC addresses. To make matters worse, computers will accept "Gratuitous ARP Responses" meaning that they will learn from ARP answers even when they didn't ask the question. This enables attacker to initiate a lie to a victim. Using ARP spoofing, an attacker can use a tool like Wireshark to sniff (or even manipulate) traffic between two hosts that it would not normally see in a switched environment. ARP spoofing can also be used to pretend to be another system on the network. There are automated tools that make this almost trivial for an attacker to execute, such as Cain and Abel.

For further learning:

Watch this excellent Tutorial on how ARP Spoofing works: http://www.oxid.it/downloads/apr-intro.swf

Watch this video to see IronGeek put the attack in action: http://www.irongeek.com/i.php?page=videos/cain1



DNS Attacks

- Like ARP, DNS maps addresses in one format (and OSI layer) to another, and caches responses
- If an attacker can change the DNS mapping for a site to an IP address he controls, he can intercept or manipulate traffic
- Common attacks include using ARP or DHCP to trick clients on a local network to use a rogue DNS server, or hacking into a registrar to manipulate a target's DNS entries on the entire Internet

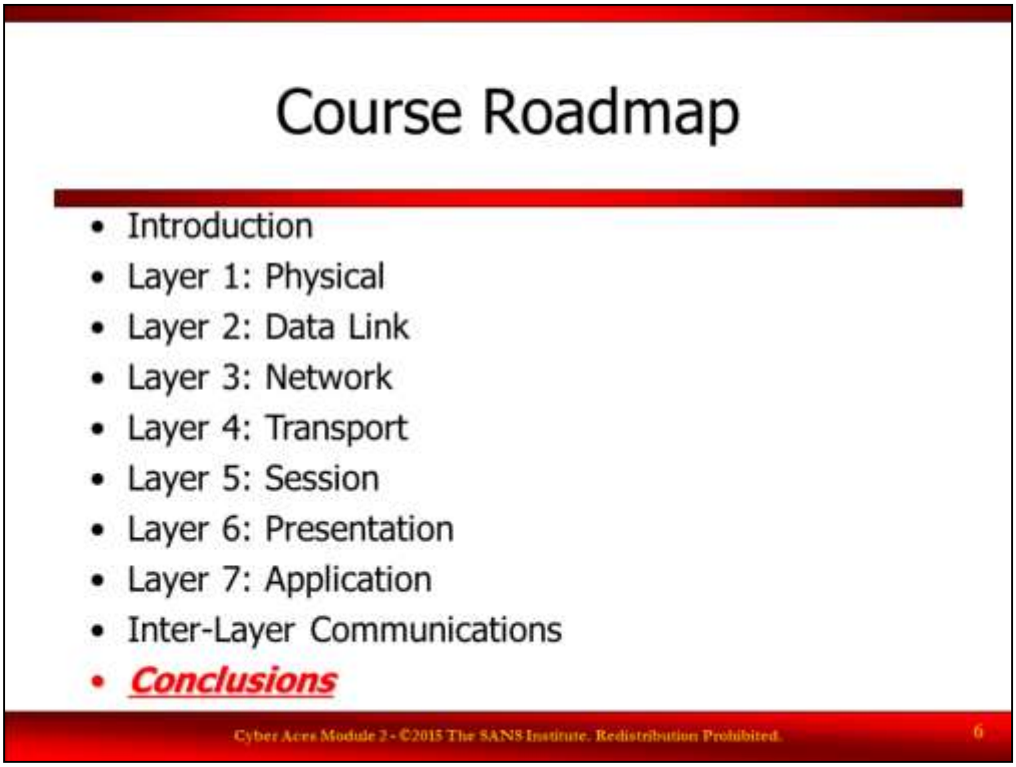
DNS Attacks

Like ARP, DNS is used to map addresses in one form to a format that lower OSI layers can understand. As mentioned earlier, DNS maps human-readable host names to machine-readable IP addresses. DNS operates at Layer 7, and its job is to map Layer 7 host names into Layer 3 addresses. It serves a function very similar to ARP. Also similar to ARP, DNS clients and servers maintain a cache of answers it has learned so that it doesn't ask redundant questions. As you can probably guess, just like ARP, DNS is vulnerable to similar attacks.

If an attacker changes the DNS mapping of www.bigbank.com so that it now points to his IP address, then he can easily capture logins and passwords to the bank as victims enter them into his fake Big Bank site. Creating a bogus DNS mapping is more difficult than creating bogus ARP entries. DNS queries contain "Transaction ID" numbers and will only accept a response if the Transaction ID in the response matches the one in the request. DNS is also more selective about from whom it will accept gratuitous responses. An attacker cannot simply send a DNS response saying "I am big bank" to any DNS client who didn't ask that question and have them accept it. However, many attacks are possible. An attacker could use an ARP attack to pretend to be the DNS server, use a rogue DHCP server to get clients to use his DNS server, or even hack into a registrar and change the DNS records for a target.

For further learning, watch this video on DNS Cache Poisoning attacks:

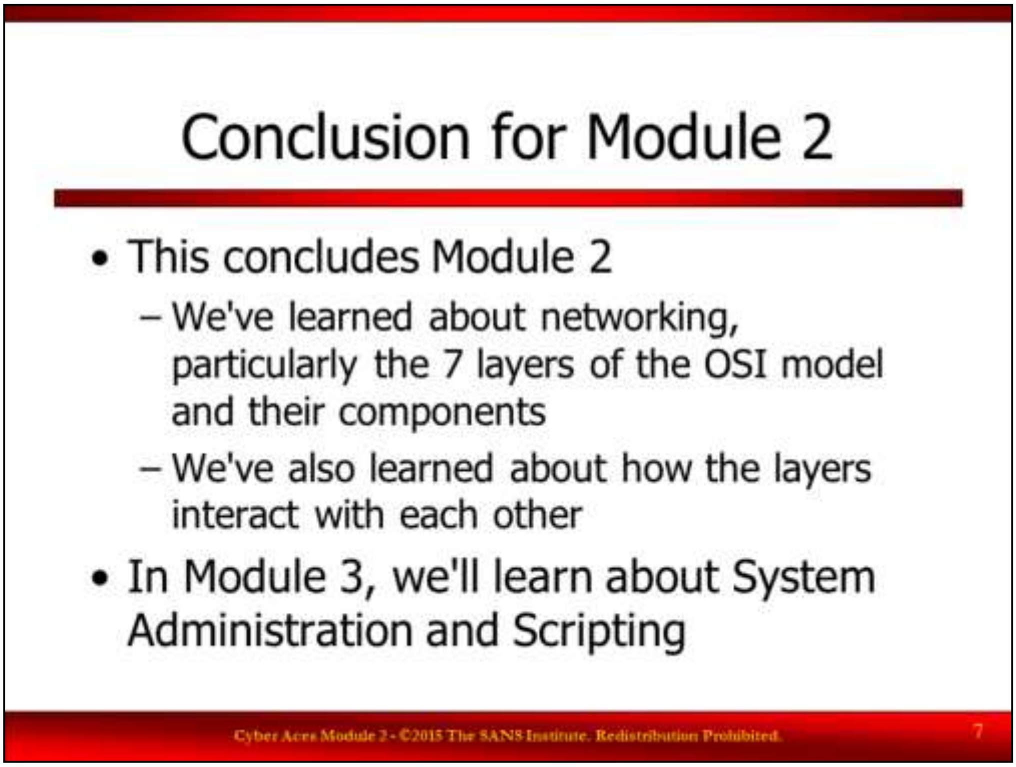
http://www.youtube.com/watch?v=1d1tUefYn4U



Course Roadmap

- Introduction
- Layer 1: Physical
- Layer 2: Data Link
- Layer 3: Network
- Layer 4: Transport
- Layer 5: Session
- Layer 6: Presentation
- Layer 7: Application
- Inter-Layer Communications
- ***Conclusions***

This concludes Module 2.



Conclusion for Module 2

- This concluses Module 2
  - We've learned about networking, particularly the 7 layers of the OSI model and their components
  - We've also learned about how the layers interact with each other
- In Module 3, we'll learn about System Administration and Scripting

This concludes Module 2. Throughout the module, we've learned about computer networking, focusing on the 7 layers of the OSI model and their components. We've also learned about how the layers interact with each other. You should now have a firm understand of network fundamentals, which will help you to understand computer attacks and defenses from a network perspective.

In Module 3, we'll learn about System Administration and Scripting.