Module 17:Attacking What We Do

CyberOps Associates v1.0

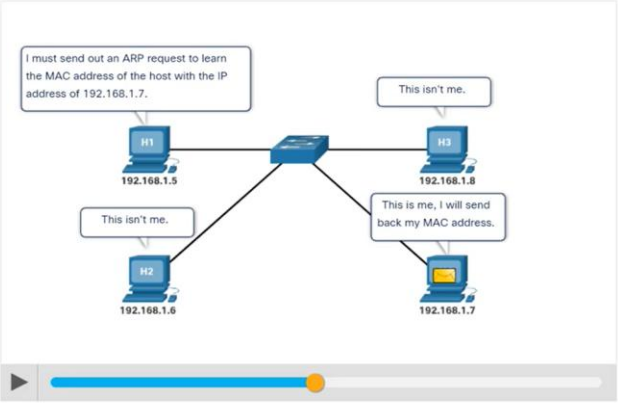
17.1 IP Services

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 3

ARP Vulnerabilities

- Hosts broadcast an ARP Request to other hosts on the network segment to determine the MAC address of a host with a particular IP address.
- The host with the matching IP address in the ARP Request sends an ARP Reply called “gratuitous ARP.”
- A threat actor can poison the ARP cache of devices on the local network
- The goal is to associate the threat actor’s MAC address with the IP address of the default gateway in the ARP caches of hosts on the LAN segment.

Play the animation to see the ARP process at work.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 4

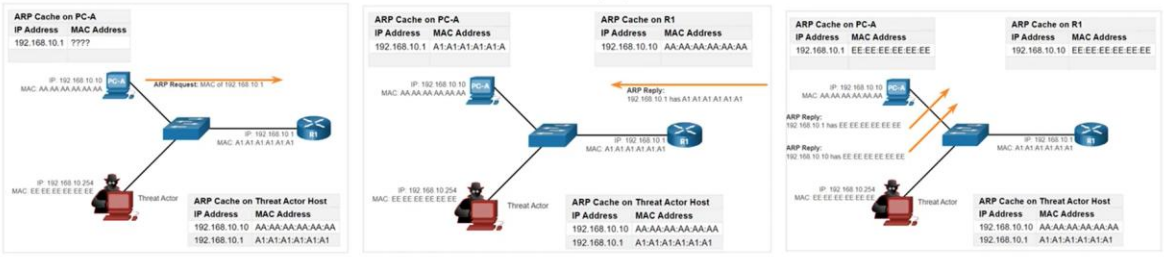
Attacking What We Do

ARP Cache Poisoning

- ARP cache poisoning can be used to launch various man-in-the-middle attacks.

ARP cache poisoning process

ARP Request | ARP Reply | Spoofed Gratuitous ARP replies



***Note**: There are many tools available on the internet to create ARP MITM attacks including dsniff, Cain & Abel, ettercap, Yersinia, and others.*

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 5

Attacking What We Do

DNS Attacks

DNS attacks include the following:

DNS open resolver attacks:

- A DNS open resolver is a publicly open DNS server such as Google DNS (8.8.8.8) that answers client's queries outside its administrative domain. DNS open resolvers are vulnerable to multiple malicious activities described in the table.

DNS Resolver Vulnerabilities	Description
DNS cache poisoning attacks	Threat actors send spoofed, falsified Record Resource (RR) information to a DNS resolver to redirect users from legitimate sites to malicious sites.
DNS amplification and reflection attacks	Threat actors send DNS messages to the open resolvers using the IP address of a target host.
DNS resource utilization attacks	This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 13

Attacking What We Do

DNS Attacks (Contd.)

DNS Stealth Attacks

- To hide their identity, threat actors also use the DNS stealth techniques described in the table to carry out their attacks.

DNS Stealth Techniques	Description
Fast Flux	Threat actors use this technique to hide their phishing and malware delivery sites. The DNS IP addresses are continuously changed within minutes.
Double IP Flux	Threat actors use this technique to rapidly change the hostname to IP address mappings and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack.
Domain Generation Algorithms	Threat actors use this technique in malware to randomly generate domain names that can then be used as rendezvous points to their command and control (C&C) servers.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 14

Attacking What We Do

DNS Attacks (Contd.)

DNS Domain Shadowing Attacks

- In Domain Shadowing, threat actor gather domain account credentials in order to create multiple sub-domains which will be used during the attacks.
- These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 15

Attacking What We Do

DNS Tunneling

- It is necessary for the cybersecurity analyst to be able to detect when an attacker is using DNS tunneling to steal data, and prevent and contain the attack.
- To accomplish this, the security analyst must implement a solution that can block the outbound communications from the infected hosts.
- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions.
- For the threat actor to use DNS tunneling, the different types of DNS records such as TXT, MX, SRV, NULL, A, or CNAME are altered. For example, a TXT record can store the commands that are sent to the infected host bots as DNS replies.
- To stop DNS tunneling, a filter that inspects DNS traffic must be used.

A → IPv4
AAAA → IPv6
MX → server mail indirizz

Tutte le tecniche che permettono di far viaggiare con DNS
tutto ciò che non è DNS

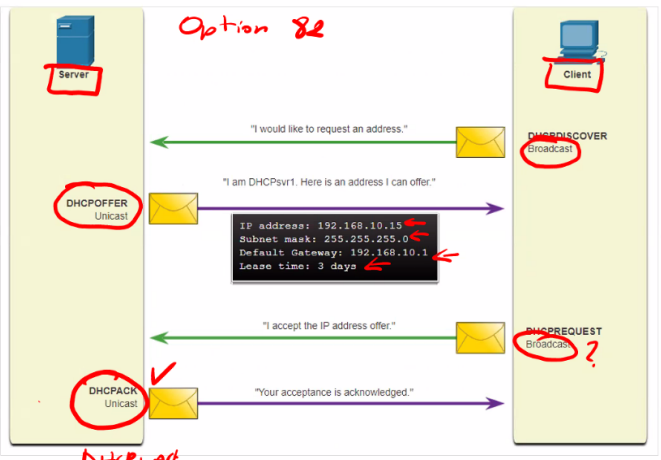
Clic destro

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 16

Attacking What We Do

DHCP

- DHCP servers dynamically provide IP configuration information to clients.
- In the figure, a client broadcasts a DHCP discover message.
- The DHCP server responds with a unicast offer that includes addressing information the client can use.
- The client broadcasts a DHCP request to tell the server that the client accepts the offer.
- The server responds with a unicast acknowledgment accepting the request.



Normal DHCP Operation

per ritrovare l'ind. il client manda un REQUEST in unicast prima della seconda

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 17

Attacking What We Do

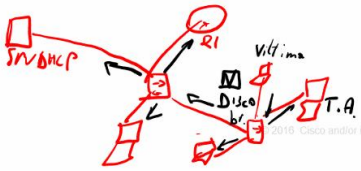
DHCP Attacks

DHCP Spoofing Attack

- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.

A rogue server can provide a variety of misleading information such as:

- **Wrong default gateway** - Threat actor provides an invalid gateway, or the IP address of its host to create a MITM (Man In The Middle) attack.
- **Wrong DNS server** - Threat actor provides an incorrect DNS server address pointing the user to a malicious website.
- **Wrong IP address** - Threat actor provides an invalid IP address, invalid default gateway IP address, or both. The threat actor then creates a DoS attack on the DHCP client.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 13

17.2 Enterprise Services

Enterprise Services

HTTP and HTTPS

- To investigate web-based attacks, security analysts must have a good understanding of how a standard web-based attack works.

Common stages of a typical web attack:

- The victim unknowingly visits a web page that has been compromised by malware.
- The compromised web page redirects the user to a site containing malicious code.
- The user visits this site with malicious code and their computer becomes infected.
- After identifying a vulnerable software package running on the victim's computer, the exploit kit contacts the exploit kit server to download the malicious code.
- After the victim's computer has been compromised, it connects to the malware server and downloads a payload.
- The final malware package is run on the victim's computer.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential 14

Enterprise Services

HTTP and HTTPS (Contd.)

- Server connection logs can often reveal information about the type of scan or attack.
- The different types of connection status codes are: HTTP
  - **Informational 1xx**
  - **Successful 2xx**
  - **Redirection 3xx**
  - **Client Error 4xx**
- To defend against web-based attacks:
  - Always update the OS and browsers with current patches and updates.
  - Use a web proxy to block malicious sites.
  - Use the best security practices from the Open Web Application Security Project (OWASP) when developing web applications.
  - Educate end users by showing them how to avoid web-based attacks.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enterprise Services

Common HTTP Exploits

Malicious iFrames

- An iFrame is an HTML element that allows the browser to load another web page from another source.
- In iFrame attacks, the threat actors insert advertisements from other sources into the page.
- Threat actors compromise a webserver and modify web pages by adding HTML for the malicious iFrame.
- As the iFrame is running in the page, it can be used to deliver a malicious exploit. such as spam advertising, exploit kits, and other malware.

Steps to prevent or reduce malicious iFrames:

- Use a web proxy like to block malicious sites.
- Ensure web developers do not use iFrames.
- Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.
- Ensure the end user understands what an Iframe is.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enterprise Services

Common HTTP Exploits (Contd.)

HTTP 302 Cushioning

- Threat actors use the 302 Found HTTP response status code to direct the user's web browser to a new location.
- The browser believes that the new location is the URL provided in the header. The browser is invited to request this new URL. This redirect function can be used multiple times until the browser finally lands on the page that contains the exploit.

Steps to prevent or reduce HTTP 302 cushioning attacks:

- Use a web proxy to block malicious sites.
- Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.
- Ensure the end user understands how the browser is redirected through a series of HTTP 302 redirections.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enterprise Services

Common HTTP Exploits (Contd.)

Domain Shadowing

- When a threat actor create a domain shadowing attack, first they compromise a domain. Then they must create multiple subdomains of that domain to be used for the attacks using Hijacked domain registration logins.
- After these subdomains have been created, attackers can use them even if they are found out to be malicious domains. They can simply make more from the parent domain.

Steps to prevent or reduce Domain shadowing attacks:

- Secure all domain owner accounts.
- Use a web proxy to block malicious sites.
- Use a service such as Cisco Umbrella to prevent users from navigating to web sites that are known to be malicious.
- Make sure that domain owners validate their registration accounts and look for any subdomains that they have not authorized.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enterprise Services

Email

- As the level of use of email rises, security becomes a greater priority.
- The way users access email today also increases the opportunity for the threat of malware to be introduced.

Examples of email threats:

- **Attachment-based attacks** - Threat actors embed malicious content in business files such as an email from the IT department.
- **Email spoofing** - Threat actors create email messages with a forged sender address that is meant to fool the recipient into providing money or sensitive information.
- **Spam email** - Threat actors send unsolicited email containing advertisements or malicious files.
- **Open mail relay server -** This is an SMTP server that allows anybody on the internet to send mail.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enterprise Services

Web-Exposed Databases

- Web applications commonly connect to a relational database to access data.
- As relational databases often contain sensitive data, databases are a frequent target for attacks.

Code Injection

- The attacker's commands are executed through the web application and has the same permissions as the web application.
- This type of attack is used because often there is insufficient validation of input.

SQL Injection

- Threat actors use SQL injections to breach the relational database, create malicious SQL queries, and obtain sensitive data from the relational database.
- A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and sometimes, issue commands to the operating system.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Enterprise Services

Client-side Scripting

Cross-Site Scripting

- Cross-Site Scripting (XSS) is where web pages that are executed on the client-side, within their own web browser, are injected with malicious scripts.
- These scripts can be used by Visual Basic, JavaScript, and others to access a computer, collect sensitive information, or deploy more attacks and spread malware.
- The two main types of XSS are **Stored (persistent)** and **Reflected (non-persistent).**
- **Ways to prevent or reduce XSS attacks**:
  - Ensure that web application developers are aware of XSS vulnerabilities and how to avoid them.
  - Use an IPS implementation to detect and prevent malicious scripts.
  - Use a web proxy to block malicious sites.
  - Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

17.3 Attacking What We Do Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Attacking What We Do Summary

What Did I Learn in this Module?

- Any client can send an unsolicited ARP Reply called a “gratuitous ARP.”
- A threat actor can poison the ARP cache of devices on the local network, creating an MiTM attack to redirect traffic.
- The Domain Name Service (DNS) protocol uses Resource Records (RR) to identify the type of DNS response.
- DNS open resolvers are vulnerable to multiple malicious activities, including DNS cache poisoning, in which falsified records are provided to the open resolver.
- In DNS amplification and reflection attacks, the benign nature of the DNS protocol is exploited to cause DoS/ DDoS attacks.
- In DNS resource utilization attacks, a DoS attack is launched against the DNS server itself.
- Threat actors use Fast Flux, in which malicious servers will rapidly change their IP address.
- To stop DNS tunneling, a filter that inspects DNS traffic must be used.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Attacking What We do Summary

What Did I Learn in this Module?

- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.
- The compromised web page redirects the user to a site that hosts malicious code which is known as a drive-by download.
- Cross-Site Scripting (XSS) attacks occur when browsers execute malicious scripts on the client and provide threat actors with access to sensitive information on the local host.
- The OWASP Top 10 Web Application Security Risks is designed to help organizations create secure web applications.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential