CIT 270: SYSTEMS SECURITY I

CHAPTER 5: NETWORKING AND SERVER ATTACKS

BYU
IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note 📎

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

NETWORKING-BASED ATTACKS

Threat Actors place high priority on targeting networks in their attacks because exploiting a single vulnerability could expose hundreds or thousands of devices.

Interception

- Man-in-the-Middle (MITM)
- Man-in-the-browser (MITB)
- Replay

Poisoning

- ARP Poisoning
- DNS Poisoning
- Privilege Escalation

NETWORKING-BASED ATTACKS: INTERCEPTION

Man-in-the-Middle (MITM): an attack intercepting legitimate communication and forging a fictitious response to the sender; external.

Man-in-the-Browser (MITB): an attack intercepting communication between parties to steal or manipulate data; internal.

Replay: variation of a MITM attack where the intercepted data is copied and then sent (replayed) later; faking a logon or getting valuable network information.

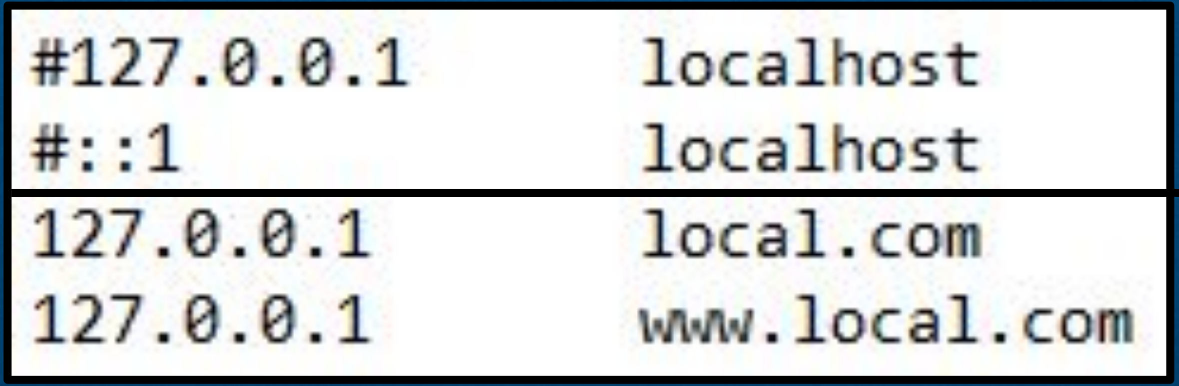
NETWORKING-BASED ATTACKS: POISONING

Address Resolution Protocol (ARP) is the protocol used to assign an IP address to a computer based off the computer's MAC address; broadcast. ARP poisoning is when a threat actor alters the ARP cache changing a valid MAC address to their own effectively taking over the valid IP address; MAC spoofing.

Attack	**Description**
Steal data	Attacker substitutes their MAC address and steals data meant for another device.
Prevent internet access	Attacker substitutes an invalid MAC address for the network gateway.
Man-in-the-middle	MITM device is set to receive all communications by substituting the MAC.
Denial of Service	An invalid IP address is substituted for the valid IP causing all traffic to fail.

NETWORKING-BASED ATTACKS: POISONING

Domain name resolution (DNS) is the process by which domain names are looked up and matched to their IP address. These lookups (matches) are then stored locally in your host table. DNS poisoning substitutes a DNS address to that of another computer or server inside your host table.



```
#127.0.0.1          localhost
#::1                localhost
127.0.0.1           local.com
127.0.0.1           www.local.com
```

Original

Altered

NETWORKING-BASED ATTACKS: POISONING

Privilege escalation is when a threat actor exploits a vulnerability to gain access to resources that a user normally would be restricted from.

Type	Description
vertical escalation	using privilege escalation to grant themselves access to functions reserved for higher privileged users.
horizontal escalation	using privilege escalation to access an account with the level of access the threat actor is after; an employee in payroll for example.
relationship escalation	using privilege escalation to exploit an unintentional relationship between multiple systems; computer 1 accessing computer 2 which can access computer 3.

SERVER ATTACKS: DENIAL OF SERVICE

Denial of Service (DoS) attacks are a deliberate attempts to prevent authorized users from accessing a system by sending so many bogus requests the server can not reply to legitimate requests.

Most DoS attacks today are Distributed Denial of Service (DDoS) attacks. These attacks involve more than one device making request and often includes hundreds to thousands of devices; *botnet*.

Botnet: a network of computers infected with malicious software and controlled as a group without the owners' knowledge.

SERVER ATTACKS: DENIAL OF SERVICE

There are several types of Denial of Service (DoS) attacks:

Type	**Description**
Smurfing attack	a broadcasted network message sent to multiple computers but with the sender altered to the victim computer; IP spoofing. Each computer then responds to the message overwhelming the victim computer.
DNS amplification attack	floods an unsuspecting victim by redirecting valid responses to it. Threat actors send a DNS request with the victim as the sender. DNS servers then respond overwhelming the victim computer.
SYN flood attack	altering the synchronization (SYN) message by changing the sender IP to a non-existent IP when connecting with a server. The server replies with its acknowledgment (ACK) and keeps the line open waiting for a response.

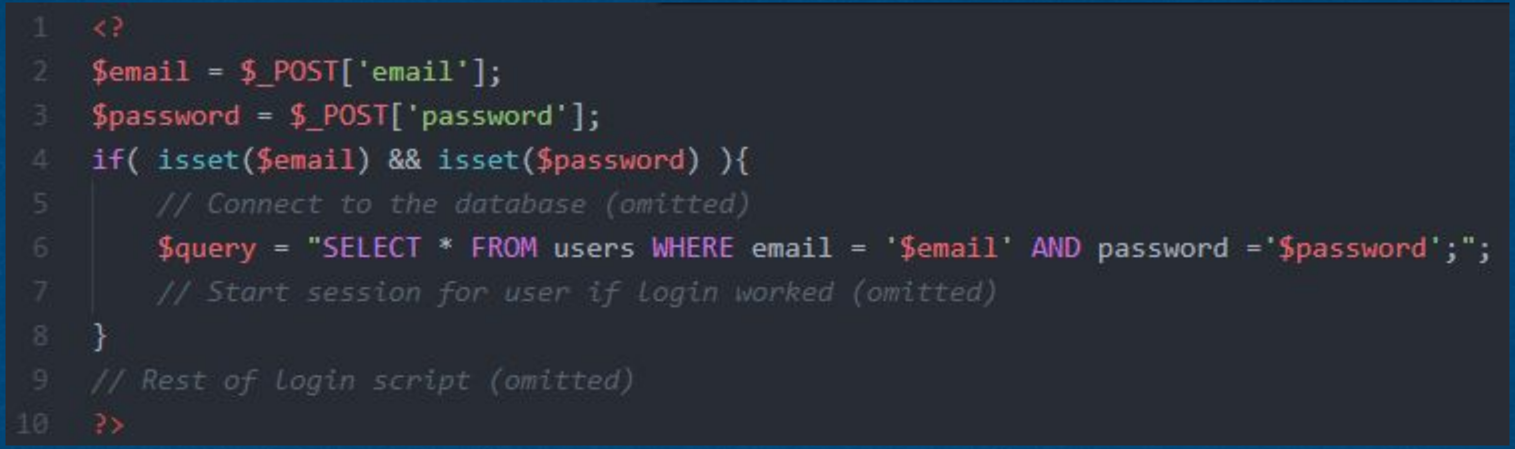
SERVER ATTACKS: CROSS-SITE SCRIPTING

Cross-Site Scripting (XSS) attacks refer to when a threat actor takes advantage of web applications that accept user input without validating the input before using it to present something back to the user.

Cross-Site Request Forgery (XSRF) attacks refer to when a threat actor tricks a victim into making a request the victim did not intend to make.

SERVER ATTACKS: INJECTION

Injection Attacks: new input is introduced to exploit a vulnerability; SQL injection.



```
<?
$email = $_POST['email'];
$password = $_POST['password'];
if( isset($email) && isset($password) ){
    // Connect to the database (omitted)
    $query = "SELECT * FROM users WHERE email = '$email' AND password ='$password';";
    // Start session for user if login worked (omitted)
}
// Rest of login script (omitted)
?>
```

ORIGINAL

```
SELECT * FROM users WHERE email = ‘a@a.com’ AND password = ‘1234’;
```

INJECTED

```
SELECT * FROM users WHERE email = ‘a@a.com’ AND password = ‘1234’ OR ‘a’ = ‘a’;
```

SERVER ATTACKS: HIJACKING

Session Hijacking: an attack where attackers attempt to impersonate a user by using their session token; XSS and session cookies.

URL Hijacking / Typosquatting: attackers purchase domain names spelled similar to popularly used sites; ad revenue or malicious fake clones.

Domain Hijacking: attackers change the web server a domain name points to and redirects it to their own server.

Clickjacking: an attack where users are tricked into clicking a link that is other than what it appears; hidden buy button.

SERVER ATTACKS: OVERFLOW

Buffer Overflow: attackers attempt to store data in RAM beyond the boundaries of the storage buffer tricking the computer into running the attackers code.

Integer Overflow: attackers change the value of a variable to something outside the range the programmer intended. This could be used for several purposes:

- buffer overflow
- altering programs to give refunds or change available balances

COMPUTER / BROWSER ATTACKS: ADVERTISING

Malvertising: using online advertising to spread malware; 3rd party networks.

Ad Fraud: fake impressions, clicks, conversion, or data events that generate revenue for attackers from advertisers.

COMPUTER / BROWSER ATTACKS: SCRIPTING CODE

Defense	**Explanation**
Limit Capabilities	JavaScript does not support certain capabilities such as read, write, create, delete, or list files on the system *
Sandboxing	Only permitting JavaScript to run in a restricted environment can limit what a computer resources it can access or actions it can take *
Same Origin	This defence restricts a JavaScript download from Site A from accessing data that came from Site B *

* With new applications and JavaScript libraries like Node.js this is only true when JavaScript is used in the web browser. JavaScript used on the desktop or in the backend (server side) has far greater access to everything.

COMPUTER / BROWSER ATTACKS: ADD-ONS

Name	**Description**	**Location**	**Browser Support**	**Examples**
Extension	Written in JavaScript and has wider access to privileges	Part of the web browser	Only works with a specific browser	Download selective links on webpage, display specific fonts
Plug-in	Links to external programs	Outside of web browser	Compatible with many different browsers	Audio, video, PDF file display
Add-on	Adds functionality to browser itself	Parts of web browser	Only works with a specific browser	Directory and language packs

REFERENCES

Attacks from ARP poisoning [Table 5-2]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 198. Boston, MA: Cengage.

Browser Additions [Table 5-6]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 219. Boston, MA: Cengage.

Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.). Boston, MA: Cengage.

DNS poisoning Windows host table [JPG]. Rexburg: Caboodle Tech Inc. Public domain image.

JavaScript Defenses [Table 5-5]. Ciampa, Mark (2018). Security+ Guide To Network Security Fundamentals (6th ed.), 219. Boston, MA: Cengage.

Vulnerable PHP code: SQL injection [JPG]. Rexburg: Caboodle Tech Inc. Public domain image.