NAME- KHUSHEE VIPIN RANE

INTERN ID - 2049

Exploring Port Vulnerabilities in Metasploitable-2 Using Kali Linux

Port Scanning

Description:

Port scanning is the process of probing a target system to identify open network ports and the services listening on them. By analyzing the responses from these probes, one can determine whether a port is open, closed, or filtered. This activity helps in identifying exposed services, operating systems, and possible security weaknesses.

Impact:

- Service Exposure: Reveals running services and their versions.
- System Mapping: Helps attackers understand the internal structure of the target.
- Attack Preparation: Provides a foundation for selecting suitable exploits.
- Firewall Weakness Identification: Detects improperly configured network defenses.

Severity:

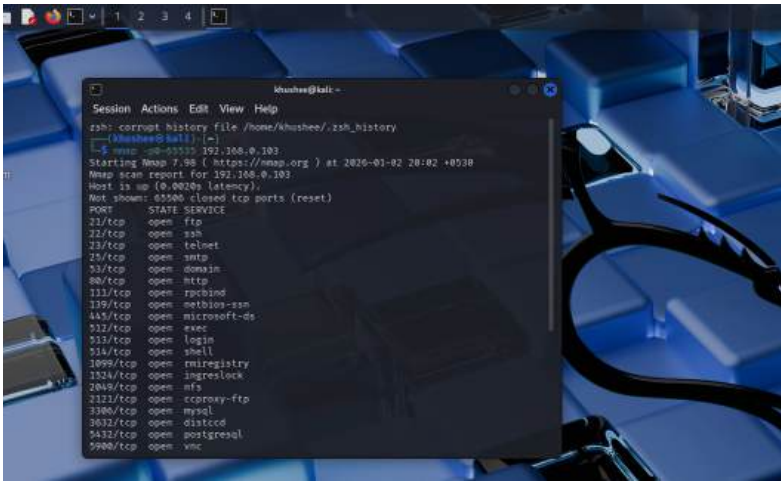
Critical

Remedial:

- Apply restrictive firewall policies
- Monitor traffic using IDS/IPS
- Disable unnecessary services
- Conduct periodic internal scans

To Scan All Ports
Command:

nmap -p0-65535 192.168.0.103



1)FTP – Port 21

Description:

Port 21 is used by the File Transfer Protocol to manage file transfer commands. FTP does not encrypt authentication details or transmitted data. In Metasploitable-2, the FTP service runs a vulnerable version of vsFTPd that contains a built-in backdoor.

Impact:

- **Unencrypted Credentials:** Usernames and passwords can be intercepted.
- **Remote Shell Access:** Exploitation leads to direct system access.
- **Automated Attacks:** Frequently targeted by brute-force tools.

Severity:

Critical

Remedial Actions:

- Replace FTP with SFTP
- Disable anonymous access
- Use strong authentication mechanisms
- Keep FTP services updated

Method 1: FTP Client Access

ftp 192.168.0.103

Connects to the FTP service to upload/download files.
Often used to check anonymous or weak authentication.

Method 2: Anonymous Login Check

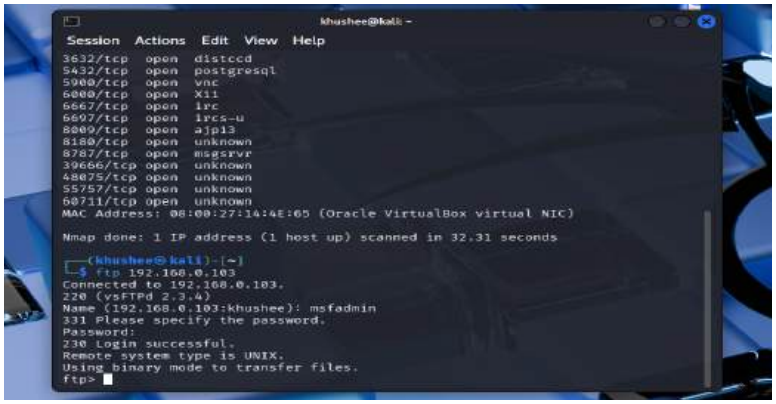
ftp
open 192.168.0.103 user: anonymous
password: anonymous

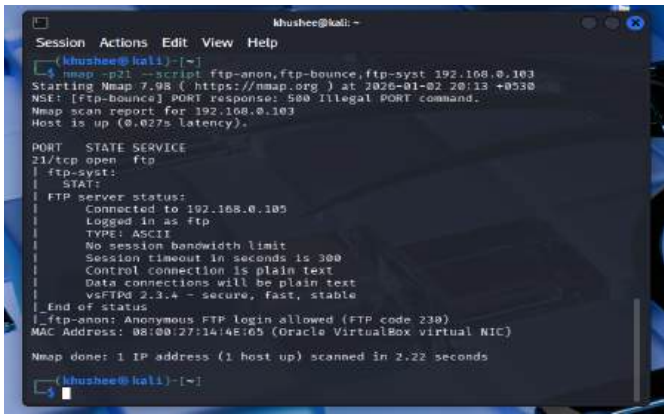
Check if the FTP server allows anonymous access without credentials.

Method 3: Nmap Enumeration

nmap -p21 --script ftp-anon,ftp-bounce,ftp-syst
192.168.0.103

Enumerates FTP configuration, system info, and anonymous access.





2) SSH – Port 22

Description:

SSH provides encrypted remote login. In Metasploitable-2, SSH is misconfigured with weak credentials, making it vulnerable to brute-force attacks.

Impact:

- **Unauthorized Access:** Attackers can gain shell access.
- **Privilege Escalation:** Can lead to root compromise.

Severity:

High

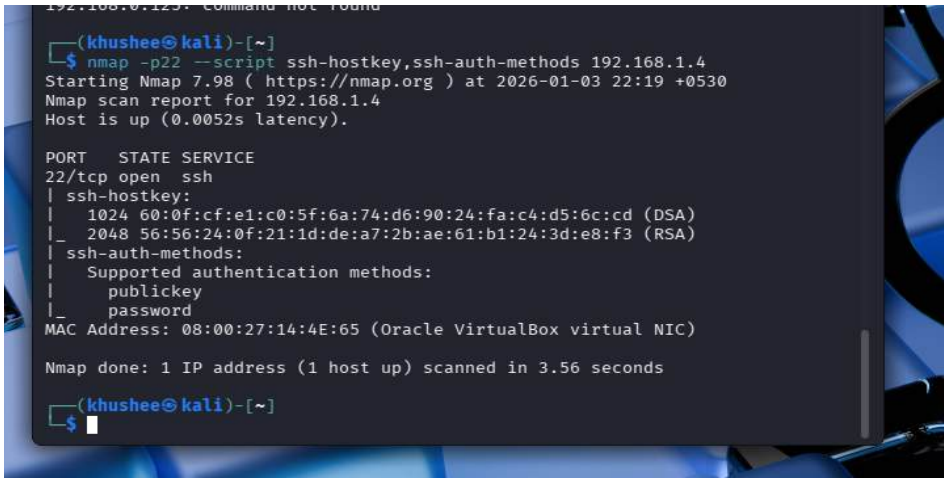
Remedial Actions:

- Disable password authentication
- Use key-based login
- Limit login attempts
- Change default credentials

Method 1: Nmap Enumeration

nmap -p22 --script ssh-hostkey,ssh-auth-methods 192.168.0.125

➡ Extracts SSH version and encryption keys.



3) Telnet – Port 23

Description:

Telnet allows remote login but transmits data in plaintext. Metasploitable-2 allows login using default credentials, making it extremely insecure.

Impact:

- **Credential Sniffing**
- **Unauthorized Access**
- **Session Hijacking**

Severity:

Critical

Remedial Actions:

- Disable Telnet
- Replace with SSH
- Enforce encrypted communication

Method 1: Telnet Access

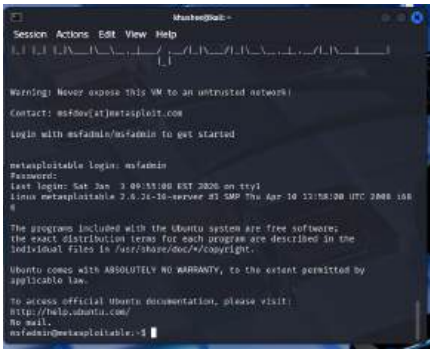
telnet 192.168.0.125

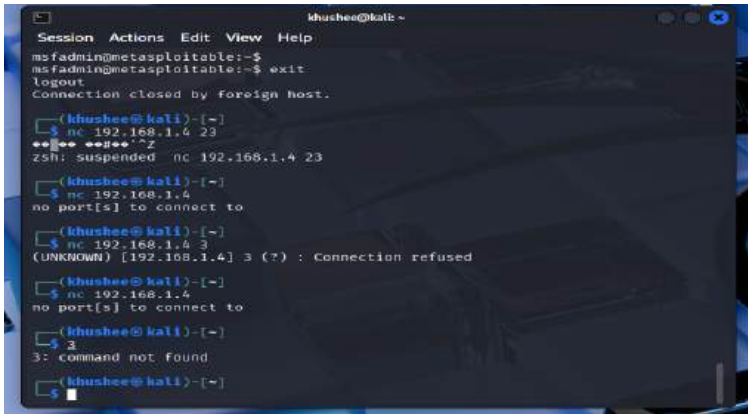
➡ Attempts plaintext remote login to the system.

Method 2: Netcat

nc 192.168.0.125 23

➡ Check if the Telnet service responds and accepts input.





4) SMTP – Port 25

Description:

SMTP (Simple Mail Transfer Protocol) is responsible for sending emails between servers. In Metasploitable-2, the SMTP service is misconfigured and vulnerable to user enumeration and information disclosure. These weaknesses allow attackers to identify valid system accounts, which can later be used for brute-force or privilege-escalation attacks.

Impact:

- **User Enumeration:** Valid usernames can be discovered.
- **Information Disclosure:** Reveals internal user accounts.
- **Attack Chaining:** Enumerated users can be used in SSH/FTP brute-force attacks.
- **Email Abuse:** Server can be misused for spam or phishing.

Severity:

High

Remedial Actions:

- Disable SMTP VRFY and EXPN commands
- Restrict SMTP access using firewall rules
- Enable authentication for mail services
- Regularly update and harden mail server configuration

Method 1: SMTP User Enumeration Using Nmap

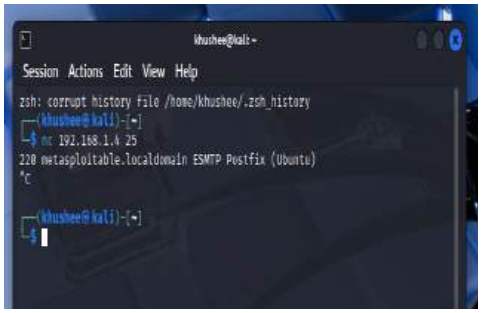
Command:

```
nmap --script smtp-enum-users -p 25 192.168.1.4
```

Method 2: Banner Grabbing (Information Disclosure)

Command:

```
nc 192.168.1.4 25
```



5) DNS – Port 53

Description:

Domain Name System (DNS) operates on port 53 and is responsible for translating domain names into IP addresses. A DNS server may also store records related to hosts, mail servers, and name servers. In Metasploitable-2, DNS is intentionally misconfigured, allowing attackers to gather sensitive domain information through enumeration techniques.

Impact:

- Network Mapping: Reveals internal hostnames and IP addresses.
- Information Disclosure: Exposes DNS records such as A, MX, and NS.
- Attack Planning: Helps attackers identify potential targets within the network.
- Facilitates Further Attacks: Discovered hosts can be used for service exploitation.

Severity:

High

Remedial Actions:

- Disable DNS zone transfers for unauthorized hosts
- Restrict DNS queries using access control lists
- Monitor DNS logs for suspicious requests
- Keep DNS software updated and hardened

Method 1: DNS Enumeration

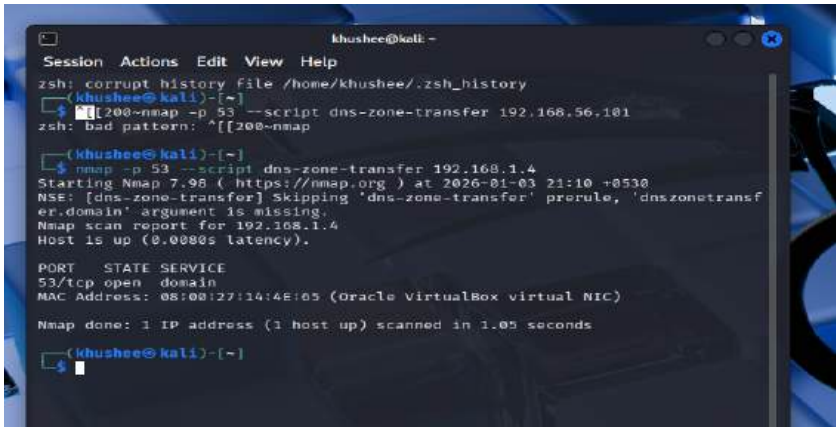
nmap -p53 --script dns-recursion 192.168.1.4

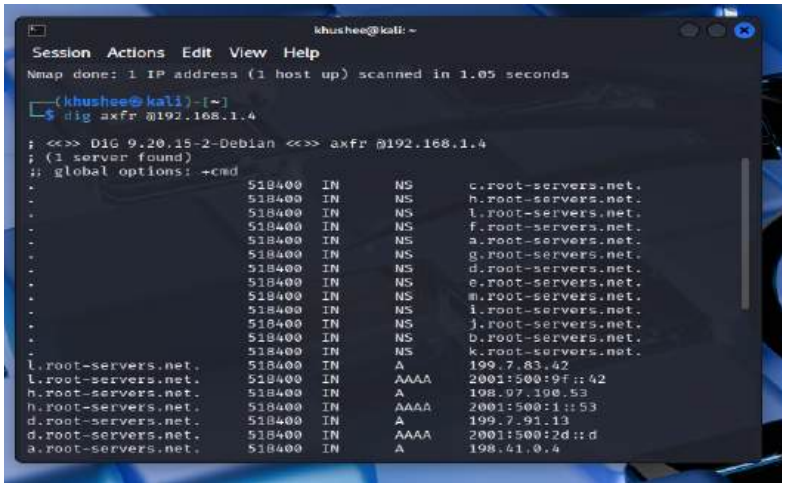
➡ Checks if recursive queries are allowed.

Method 2: Zone Transfer Attempt

dig axfr @192.168.1.4

➡ Attempts to dump DNS records.





6) HTTP – Port 80

Description:

Port 80 hosts web applications such as DVWA and Mutillidae, which are intentionally vulnerable. These applications allow exploitation through common web attacks like SQL injection and command execution.

Impact:

- **Database Exposure:** Sensitive information can be extracted.
- **Web Shell Deployment:** Attackers can upload malicious scripts.
- **Remote Command Execution:** Full control of the server.

Severity:

Critical

Remedial Actions:

- Validate and sanitize user input
- Apply security patches
- Use web application firewalls
- Remove vulnerable test applications

Method 1: Web Browser

dirb http://192.168.56.101

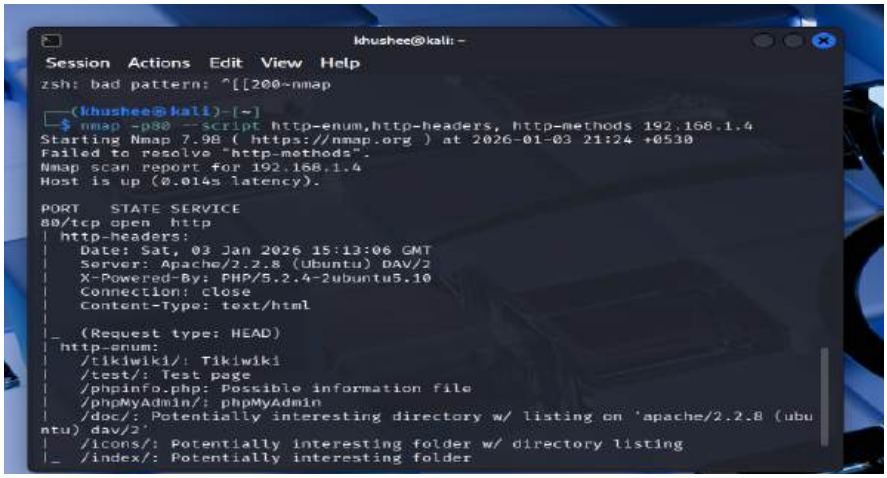
sqlmap -u "http://192.168.56.101/..." --dbs

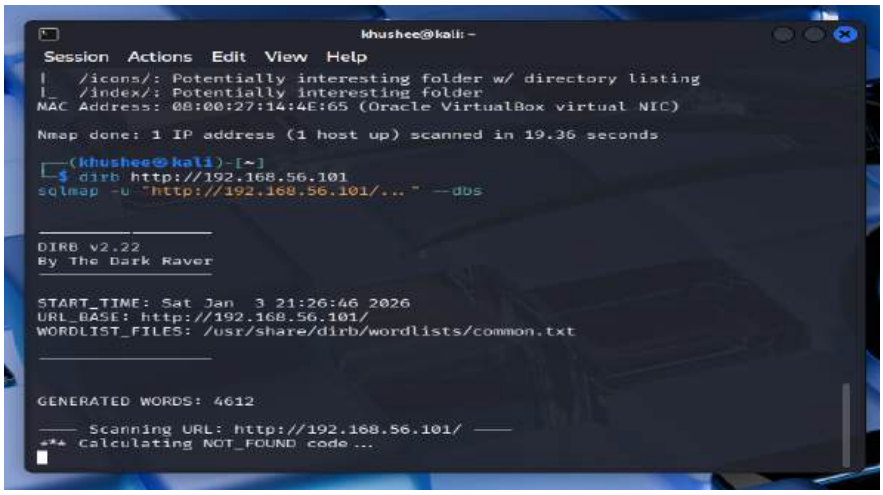
➡ Directly accesses the web application hosted on the server.

Method 2: Nmap Web Scripts **nmap -p80 --script http-enum,http-headers,http-methods**

192.168.1.4

➡ Discovers directories, server headers, and web technologies.





7) Port 111 – RPCBind

Description:

RPCBind (Remote Procedure Call Binder) operates on port 111 and acts as a directory service for RPC-based applications. It maps RPC program numbers to their corresponding network port numbers, allowing clients to locate services such as NFS, mountd, and statd. In Metasploitable-2, RPCBind is openly accessible and exposes detailed information about running RPC services.

Impact:

- **Service Enumeration:** Reveals active RPC services and their ports.
- **Information Leakage:** Discloses internal service architecture.
- **Attack Chaining:** Enables attackers to identify exploitable services like NFS.
- **Network Reconnaissance:** Assists in mapping backend services.

Severity:

High

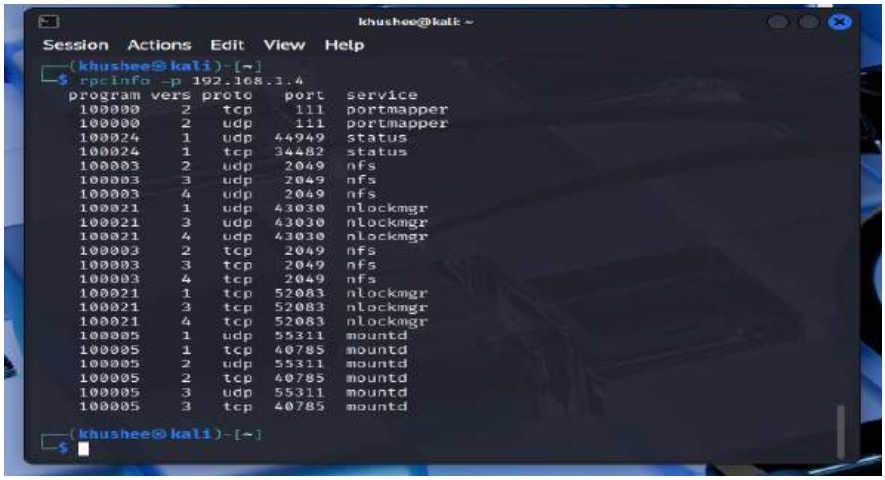
Remedial Actions:

- Restrict RPCBind access using firewall rules
- Disable unnecessary RPC services
- Allow RPC traffic only from trusted hosts
- Monitor RPC-related activity in system logs

Method 1: RPC Enumeration

rpcinfo -p 192.168.1.4

➡ Lists all RPC services.



8)rexec-Port 512

Description:

Port 512 is used by the **rexec (Remote Execution)** service, which allows users to execute commands on a remote system after authentication. The rexec protocol is considered insecure because it transmits usernames and passwords in plaintext. In Metasploitable-2, the rexec service is enabled and configured with weak credentials, making it vulnerable to unauthorized access.

Impact:

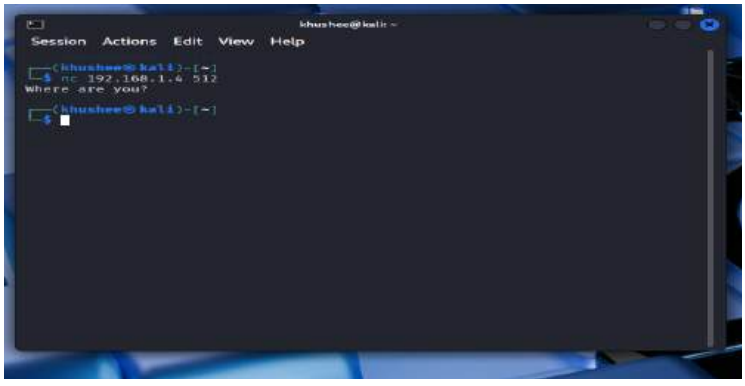
- **Plaintext Credential Exposure:** Login details can be intercepted.
- **Remote Command Execution:** Attackers can run system commands remotely.
- **Unauthorized Access:** Weak credentials allow easy compromise.
- **Privilege Escalation:** May lead to higher-level access on the system.

Severity:

High

Remedial Actions:

- Disable rexec service if not required
- Replace rexec with secure alternatives like SSH
- Enforce strong authentication mechanisms
- Block port 512 at the firewall



9) rlogin-Port 513

Description:

Port 513 is used by the **rlogin (Remote Login)** service, which allows users to log into a remote system over a network. The rlogin protocol relies on host-based authentication and transmits data, including credentials, in plaintext. In Metasploitable-2, rlogin is enabled with weak trust relationships, making it vulnerable to unauthorized access.

Impact:

- **Plaintext Authentication:** User credentials can be intercepted.
- **Trust Exploitation:** Misconfigured `.rhosts` files allow passwordless access.
- **Unauthorized Login:** Attackers can gain shell access remotely.
- **System Compromise:** Can lead to further privilege escalation.

Severity:

High

Remedial Actions:

- Disable rlogin service entirely
- Remove trust-based authentication files
- Replace rlogin with SSH
- Block port 513 at the firewall

Method 1: rlogin Access

```
rlogin 192.168.1.4 -l root
```

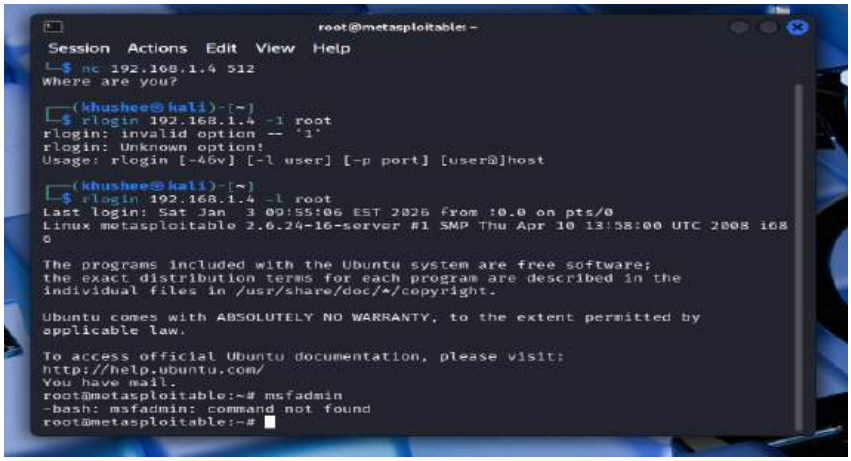
➡ Attempts remote login.

Method 2: Banner Verification Using Netcat

Command:

```
nc 192.168.1.4 513
```

➡Netcat is used to confirm that the rlogin service is accessible on the specified port.



10) rsh-Port 514

Description:

Port 514 is used by the **rsh (Remote Shell)** service, which enables users to execute commands on a remote system without establishing a full login session. The rsh protocol relies on host-based trust relationships and transmits data without encryption. In Metasploitable-2, rsh is enabled with insecure configurations, allowing attackers to execute commands remotely.

Impact:

- **Unauthenticated Command Execution:** Commands may run without proper authentication.
- **Plaintext Communication:** Data and commands can be intercepted.
- **Trust Abuse:** Misconfigured trust files allow attackers to bypass passwords.
- **System Takeover:** Remote execution can lead to full compromise.

Severity:

High

Remedial Actions:

- Disable rsh service completely
- Remove `.rhosts` and host-based trust configurations
- Use SSH instead of rsh
- Block port 514 using firewall rules

Method 1: rsh Command Execution

rsh 192.168.0.125 ls

➡ Executes commands remotely