

System Hardening Lab Form

Name: | |

Date: | |

1. What was the administrator's password originally set to on the HMI system? Why was this so password so easy to crack?

The administrator's original password was "password123".

The original password was easy to crack because it was a common password found in a password dictionary.

```
(student@kali)-[~]  
$ hydra -l administrator -P rockyou.txt smb://10.0.255.101  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in  
military or secret service organizations, or for illegal purposes (this is n  
on-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-14 11:  
12:11  
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)  
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:1  
4344399), ~14344399 tries per task  
[DATA] attacking smb://10.0.255.101:445/  
[445][smb] host: 10.0.255.101 login: administrator password: password123  
1 of 1 target successfully completed, 1 valid password found
```

2. Hydra can use brute force (try every combination of characters) to crack passwords. Given that a four-character password consisting of only lower-case alpha characters can have up to 4503599627370496 combinations which do you think is more secure, a shorter password made up of randomly selected characters or a long password which uses a word found in rockyou.txt dictionary? (HINT: If you would like to see the number of entries in the dictionary file type the command "wc -l rockyou.txt" at the terminal on the Kali system)

The shorter password will probably be more secure because there are more combinations that will need to be tried to crack the password than with a dictionary file.

3. Post the screen shot taken in the "Demonstrate the Importance of Software Patches" section of the lab here.



The system should not be vulnerable.

```
(student@kali)-[~]
$ sudo nmap --script smb-vuln-ms08-067 10.0.255.101
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-07 15:22 EDT
Nmap scan report for 10.0.255.101
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1038/tcp  open  mtqp
MAC Address: 08:00:27:7B:38:4C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
```

4. Post the screen shot taken in the “Remove or Disable Unnecessary System Services” section of the lab here.

The system should not be vulnerable and port 445 should not be open.

```
(student@kali)-[/usr/share/nmap/scripts]
$ sudo nmap --script smb-vuln-ms17-010 10.0.255.101
[sudo] password for student:
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-07 10:38 EDT
Nmap scan report for 10.0.255.101
Host is up (0.00016s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
1041/tcp  open  danf-ak2
MAC Address: 08:00:27:79:57:23 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds

(student@kali)-[/usr/share/nmap/scripts]
$
```

5. Post the first screen shot taken in the “Enable a Host Firewall” section of the lab here.

The system should have cracked the passwords.



```
(student@kali)-[~]  
$ john --show --format=NT secrets.sam  
Administrator:Password01:500:e52cac67419a9a22c295285c92cd06b4:7100a909c7ff05b266af3c42ec058c33:::  
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
student:Password01:1003:e52cac67419a9a22c295285c92cd06b4:7100a909c7ff05b266af3c42ec058c33:::  
sammy:RockYou:1005:2dec0e2359e75259aad3b435b51404ee:bab5c642d936244755554a435e7b8059:::  
  
4 password hashes cracked, 3 left
```

6. Post the second screen shot taken in the “Enable a Host Firewall” section of the lab here.

Port 445 should not be open.

```
(student@kali)-[~]  
$ nmap -p 445 10.0.255.101  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-07 15:54 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.07 seconds
```