Stephanie Vergil

OS Hardening Lab Results

Password Policy Changes (from Section 1, Activity 2)

Under **Security Configuration and Analysis** (left-side panel)	Policy (right-side panel)	Old Computer Setting	Set **Database Setting** to:
Account Policies > Password Policy	Enforce password history	24 passwords remembered	24 passwords remembered
	Maximum password age	42 days	42 days
	Minimum password age	1 days	1 day
	Minimum password length	O characters	0 characters[1]
	Password must meet complexity requirements	Disabled	Disabled[2]
	Store passwords using reversible encryption	Disabled	Disabled
Local Policies > Security Options	Network security: Do not store LAN Manager hash value on next password change	Disabled	Enabled
	Network security: LAN Manager	Send NTLM response only	Send NTLMv2 response only. Refuse LM

[1] We normally wouldn't set Minimum Password Length to 0 characters—8 characters is a common setting—but we're doing this to make comparisons with the previous lab easier.

[2] We would normally enable password complexity requirements, but we're doing this to make comparisons with the previous lab easier.

	authentication level		

password: What happened and why? (from Section 2, Activity 1)

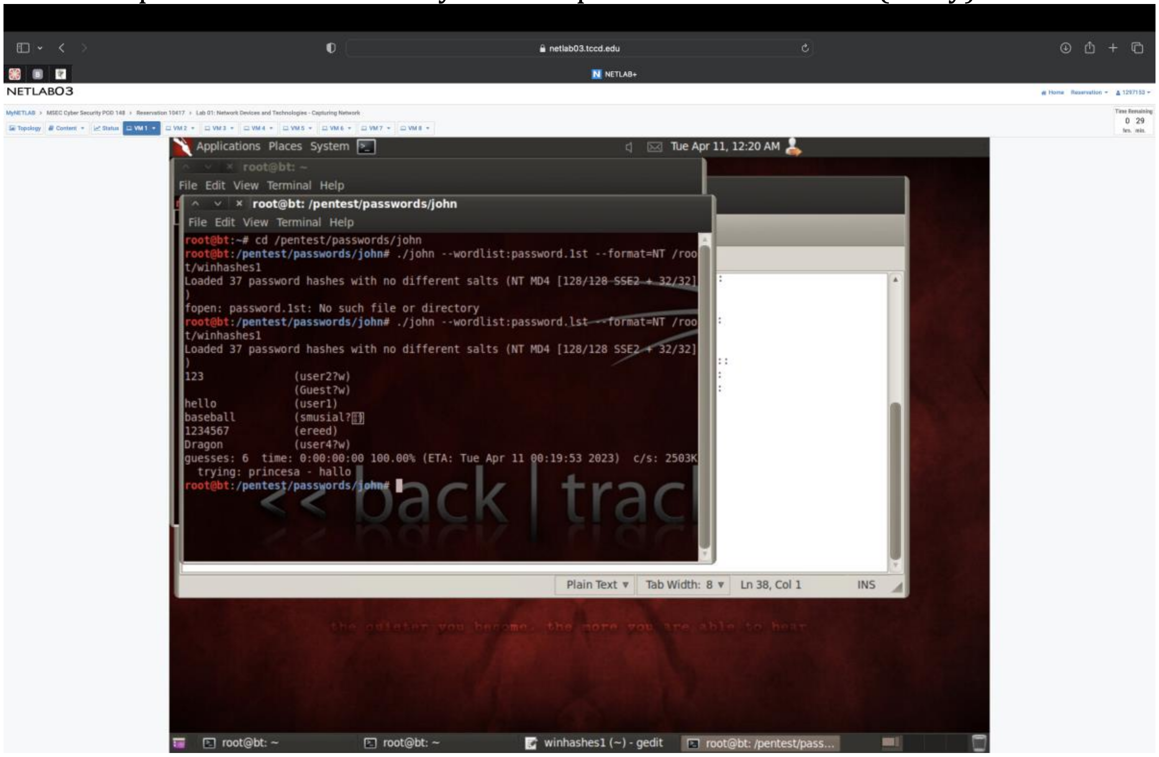
An error massage has appeared, it states "Your Password must be at least 0 characters, cannot repeat any of your previous 24 passwords and must beat least 1 day old. Please type a different password. Type a password which meets these requirements in both text boxes." In this case I tried to re-elect the same password that was already registered by the system.

ITSY1400!: What happened and why? (from Section 2, Activity 1)

A pop-up message appeared stating that " your password has been change" this time I was able to change the password due to having a different one than the on that was already registered with the system since the enforced password history setting is set to not repeat the 24 previous passwords .

Basic Password Attack (from Section 2, Activity 3)

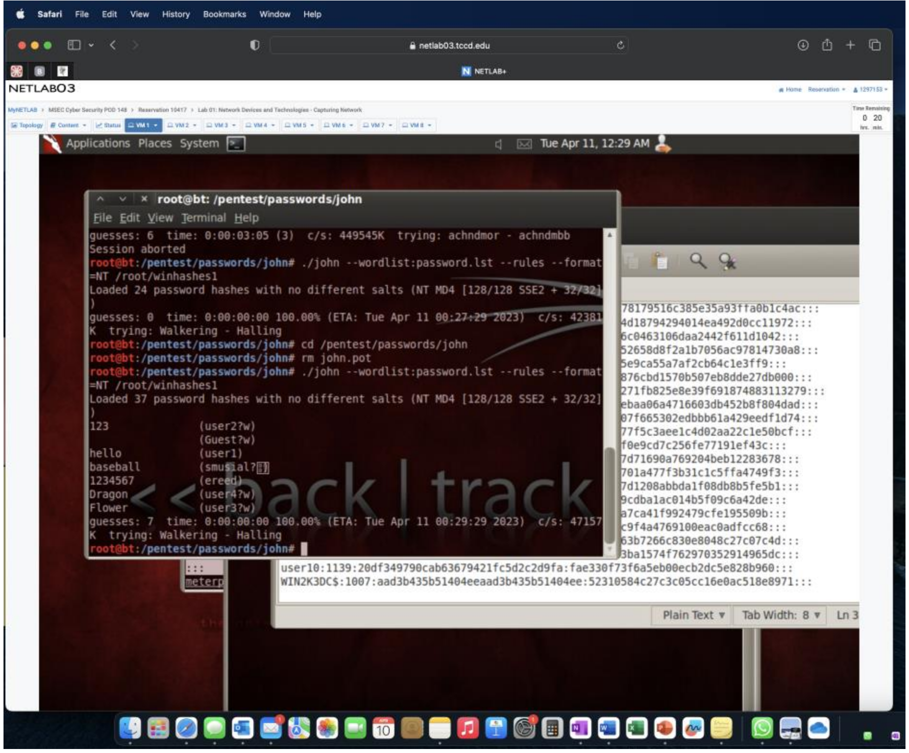
Enter the passwords returned by the first password attack here (if any):



```
root@bt:~# cd /pentest/passwords/john
root@bt:/pentest/passwords/john# ./john --wordlist:password.1st --format=NT /roo
t/winhashes1
Loaded 37 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32]
)
fopen: password.1st: No such file or directory
root@bt:/pentest/passwords/john# ./john --wordlist:password.lst --format=NT /roo
t/winhashes1
Loaded 37 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32]
)
123              (user2?w)
                 (Guest?w)
hello            (user1)
baseball         (smusial?
1234567          (ereed)
Dragon           (user4?w)
guesses: 6  time: 0:00:00:00 100.00% (ETA: Tue Apr 11 00:19:53 2023)  c/s: 2503K
  trying: princesa - hallo
root@bt:/pentest/passwords/john# 
```

Hybrid Password Attack (from Section 2, Activity 3)

Enter the passwords returned by the second password attack here:



Safari File Edit View History Bookmarks Window Help
netlab03.tccd.edu
NETLAB+
NETLAB03
Applications Places System
Tue Apr 11, 12:29 AM
root@bt: /pentest/passwords/john
File Edit View Terminal Help
Plain Text ▾
Tab Width: 8 ▾
Ln 3

```
guesses: 6  time: 0:00:03:05 (3)  c/s: 449545K  trying: achndmor - achndmbb
Session aborted
root@bt:/pentest/passwords/john# ./john --wordlist:password.lst --rules --format
=NT /root/winhashes1
Loaded 24 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32]
)
guesses: 0  time: 0:00:00:00 100.00% (ETA: Tue Apr 11 00:27:29 2023)  c/s: 42381
K  trying: Walkering - Halling
root@bt:/pentest/passwords/john# cd /pentest/passwords/john
root@bt:/pentest/passwords/john# rm john.pot
root@bt:/pentest/passwords/john# ./john --wordlist:password.lst --rules --format
=NT /root/winhashes1
Loaded 37 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32]
)
123               (user2?w)
                  (Guest?w)
hello             (user1)
baseball          (smusial?
1234567           (ereed)
Dragon            (user4?w)
Flower            (user3?w)
guesses: 7  time: 0:00:00:00 100.00% (ETA: Tue Apr 11 00:29:29 2023)  c/s: 47157
K  trying: Walkering - Halling
root@bt:/pentest/passwords/john# 
```

```
78179516c385e35a93ffa0b1c4ac:::
4d18794294014ea492d0cc11972:::
6c0463106daa2442f611d1042:::
52658d8f2a1b7056ac97814730a8:::
5e9ca55a7af2cb64c1e3ff9:::
876cbd1570b507eb8dde27db000:::
271fb825e8e39f691874883113279:::
ebaa06a4716603db452b8f804dad:::
07f665302edbbb61a429eedf1d74:::
77f5c3aee1c4d02aa22c1e50bcf:::
f0e9cd7c256fe77191ef43c:::
7d71690a769204beb12283678:::
701a477f3b31c1c5ffa4749f3:::
7d1208abbda1f08db8b5fe5b1:::
9cdba1ac014b5f09c6a42de:::
a7ca41f992479cfe195509b:::
c9f4a4769100eac0adfcc68:::
63b7266c830e8048c27c07c4d:::
3ba1574f762970352914965dc:::
user10:1139:20df349790cab63679421fc5d2c2d9fa:fae330f73f6a5eb00ecb2dc5e828b960:::
WIN2K3DC$:1007:aad3b435b51404eeaad3b435b51404ee:52310584c27c3c05cc16e0ac518e8971:::
```

Benchmark Introduction (from Section 3, Activity 2)

Page 6 from an earlier version of the CIS Windows Server 2003 benchmark stated:

One side-effect of this wealth of information available is that there are local computer security experts who want to toss the documentation aside, and apply the standards. I have one piece of advice before you go and do that:
IF YOU ONLY READ ONE PAGE IN THIS GUIDE, READ THIS PAGE!
This guide imposes changes that are best implemented in a managed environment. They are designed to limit communication between computers to positively identified and authorized personnel. This is a change from the normal way of thinking in a Windows world. Major systems should still function, but testing this benchmark in a controlled environment is essential.

Why do you think CIS included this warning against applying the standards without testing? one should carefully consider the possible impact to software applications when applying these recommended technical controls.

Page 11 lists the two security levels defined within this benchmark: **Enterprise**, and **Specialized Security – Limited Functionality (SSLF)**. SSLF has the tightest security settings, so an administrator might be tempted to assume that "tightest security" = "best option." Why might that be a bad assumption?

the expense of functionality, performance, and interoperability.

Benchmark Recommendations (From Section 3, Activity 2)

Read "1.1.2 Maximum password age" on page 13. Why do limits on password ages improve security? Enforcing a reasonably short password age will increase the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

Read "1.1.3 Minimum password age" on pages 13-14. Why is a **minimum** password age important? Enforcing a minimum password age prevents a user from quickly cycling through passwords in an attempt to reuse a familiar password. Preventing this increases the efficacy of password-based authentication systems by reducing the opportunity for an attacker to leverage a known credential.

Read "1.2 Audit Policy" on page 21 and "1.3 Detailed Security Auditing" on page 29. Why is it important to consider what events should be logged? Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents.

When complex passwords are enabled, what are the requirements for passwords? (See section 1.1.5.) longer than six characters, are not comprised or the principal's username or real name, and contain characters from at least three distinct character classes (uppercase, lowercase, integer, non-alphanumeric). For all profiles, the recommended state for this setting is `Enabled`.

If complexity requirements had been enabled, would you have been able to create these accounts? If not, why not?

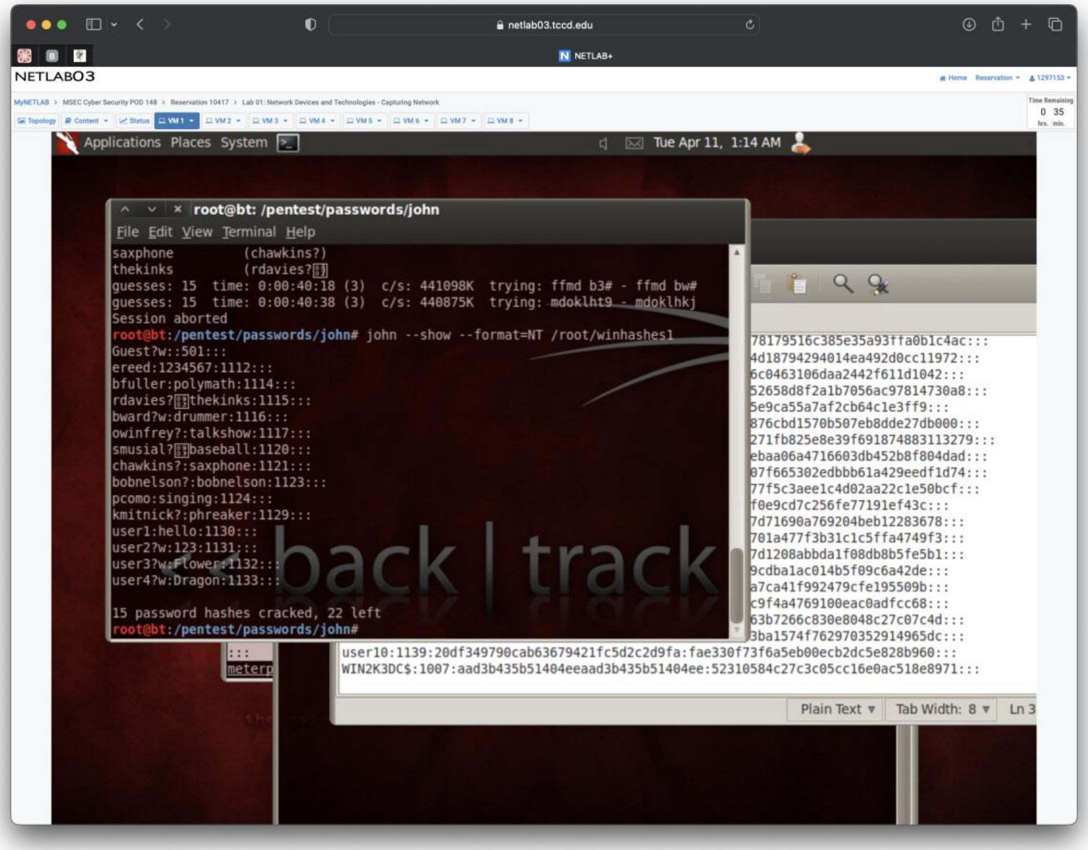
- User1: No, doesn't meet length requirement, Nor at least three distinct character classes
- User2: No, doesn't meet length requirement. Nor at least three distinct character classes
- User3 No, only has 1 distinct character upper case (it's also a name)
- User4: No, doesn't have at least three distinct character classes.
- User5: : No, doesn't have at least three distinct character classes.
- User6: No, doesn't have at least three distinct character classes.
- User7: Yes

Read "1.9.46 Network security: Do not store LAN Manager hash value on next password change" (page 126) and "1.9.47 Network security: LAN Manager authentication level" (page 127). No questions about these sections…yet!

Full Password Attack (from Section 4, Activity 1)

Enter the passwords returned by the third password attack here:

Stephanie Vergil



```
saxphone         (chawkins?)
thekinks         (rdavies?▯
guesses: 15  time: 0:00:40:18 (3)  c/s: 441098K  trying: ffmd b3# - ffmd bw#
guesses: 15  time: 0:00:40:38 (3)  c/s: 440875K  trying: mdoklht9 - mdoklhkj
Session aborted
root@bt:/pentest/passwords/john# john --show --format=NT /root/winhashes1
Guest?w::501:::
ereed:1234567:1112:::
bfuller:polymath:1114:::
rdavies?▯thekinks:1115:::
bward?w:drummer:1116:::
owinfrey?:talkshow:1117:::
smusial?▯baseball:1120:::
chawkins?:saxphone:1121:::
bobnelson?:bobnelson:1123:::
pcomo:singing:1124:::
kmitnick?:phreaker:1129:::
user1:hello:1130:::
user2?w:123:1131:::
user3?w:Flower:1132:::
user4?w:Dragon:1133:::

15 password hashes cracked, 22 left
root@bt:/pentest/passwords/john#
```

```
78179516c385e35a93ffa0b1c4ac:::
4d18794294014ea492d0cc11972:::
6c0463106daa2442f611d1042:::
52658d8f2a1b7056ac97814730a8:::
5e9ca55a7af2cb64c1e3ff9:::
876cbd1570b507eb8dde27db000:::
271fb825e8e39f691874883113279:::
ebaa06a4716603db452b8f804dad:::
07f665302edbbb61a429eedf1d74:::
77f5c3aee1c4d02aa22c1e50bcf:::
f0e9cd7c256fe77191ef43c:::
7d71690a769204beb12283678:::
701a477f3b31c1c5ffa4749f3:::
7d1208abbda1f08db8b5fe5b1:::
9cdba1ac014b5f09c6a42de:::
a7ca41f992479cfe195509b:::
c9f4a4769100eac0adfcc68:::
63b7266c830e8048c27c07c4d:::
3ba1574f762970352914965dc:::
user10:1139:20df349790cab63679421fc5d2c2d9fa:fae330f73f6a5eb00ecb2dc5e828b960:::
WIN2K3DC$:1007:aad3b435b51404eeaad3b435b51404ee:52310584c27c3c05cc16e0ac518e8971:::
```

```
:::
meterp
```

Why are the results different from the password lab? (Remember what you read for settings 1.9.46 and 1.9.47.)

> “1.9.46 Network security: Do not store LAN Manager hash value on next password change” because Enabling this setting will increase the difficulty for an attacker to successfully derive credentials by attacking the SAM file. Additionally ‘1.9.47 Network security: LAN Manager authentication level” by Configuring this setting as recommended will reduce the probability of an attacker being able to derive credentials from authentication responses.