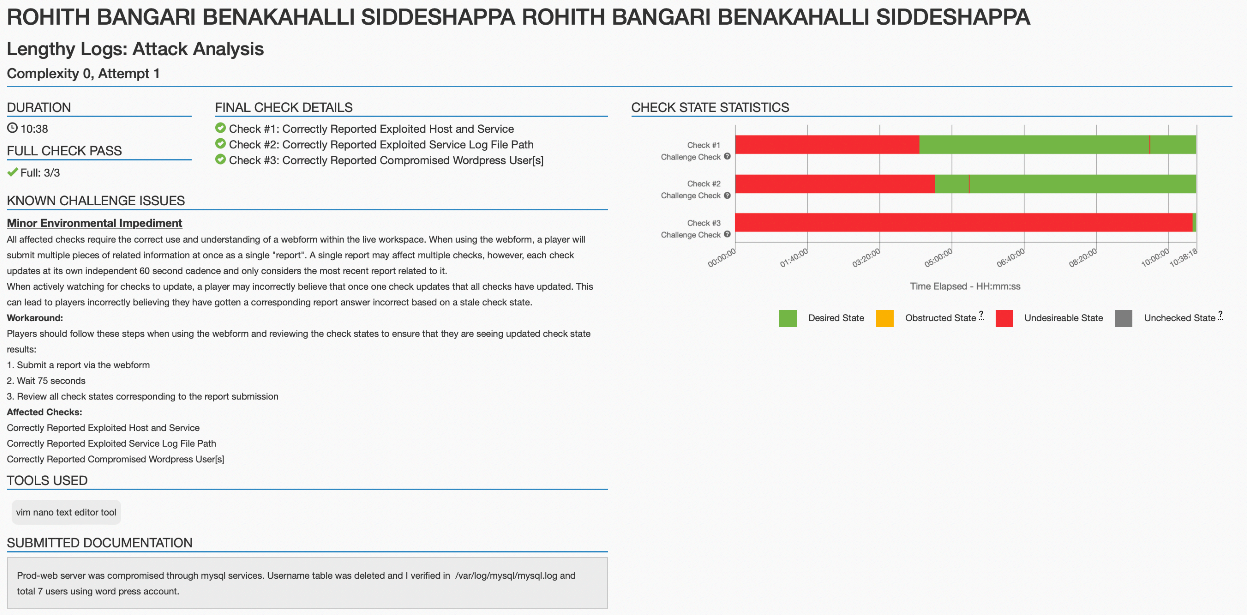
NICE Challenge Assignment 1

1)Lengthy Logs: Attack Analysis :



ROHITH BANGARI BENAKAHALLI SIDDESHAPPA ROHITH BANGARI BENAKAHALLI SIDDESHAPPA

Lengthy Logs: Attack Analysis

Complexity 0, Attempt 1

DURATION

10:38

FULL CHECK PASS

✓ Full: 3/3

FINAL CHECK DETAILS

✓ Check #1: Correctly Reported Exploited Host and Service
✓ Check #2: Correctly Reported Exploited Service Log File Path
✓ Check #3: Correctly Reported Compromised Wordpress User[s]

KNOWN CHALLENGE ISSUES

Minor Environmental Impediment

All affected checks require the correct use and understanding of a webform within the live workspace. When using the webform, a player will submit multiple pieces of related information at once as a single "report". A single report may affect multiple checks, however, each check updates at its own independent 60 second cadence and only considers the most recent report related to it.

When actively watching for checks to update, a player may incorrectly believe that once one check updates that all checks have updated. This can lead to players incorrectly believing they have gotten a corresponding report answer incorrect based on a stale check state.

Workaround:

Players should follow these steps when using the webform and reviewing the check states to ensure that they are seeing updated check state results:

1. Submit a report via the webform
2. Wait 75 seconds
3. Review all check states corresponding to the report submission

Affected Checks:

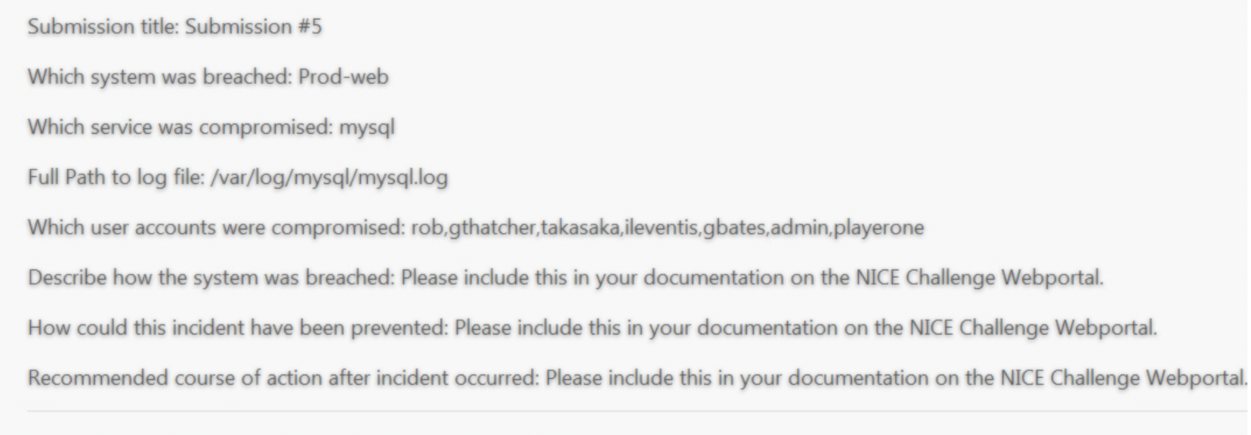
Correctly Reported Exploited Host and Service
Correctly Reported Exploited Service Log File Path
Correctly Reported Compromised Wordpress User[s]

TOOLS USED

vim nano text editor tool

SUBMITTED DOCUMENTATION

Prod-web server was compromised through mysql services. Username table was deleted and I verified in /var/log/mysql/mysql.log and total 7 users using word press account.



Submission title: Submission #5

Which system was breached: Prod-web

Which service was compromised: mysql

Full Path to log file: /var/log/mysql/mysql.log

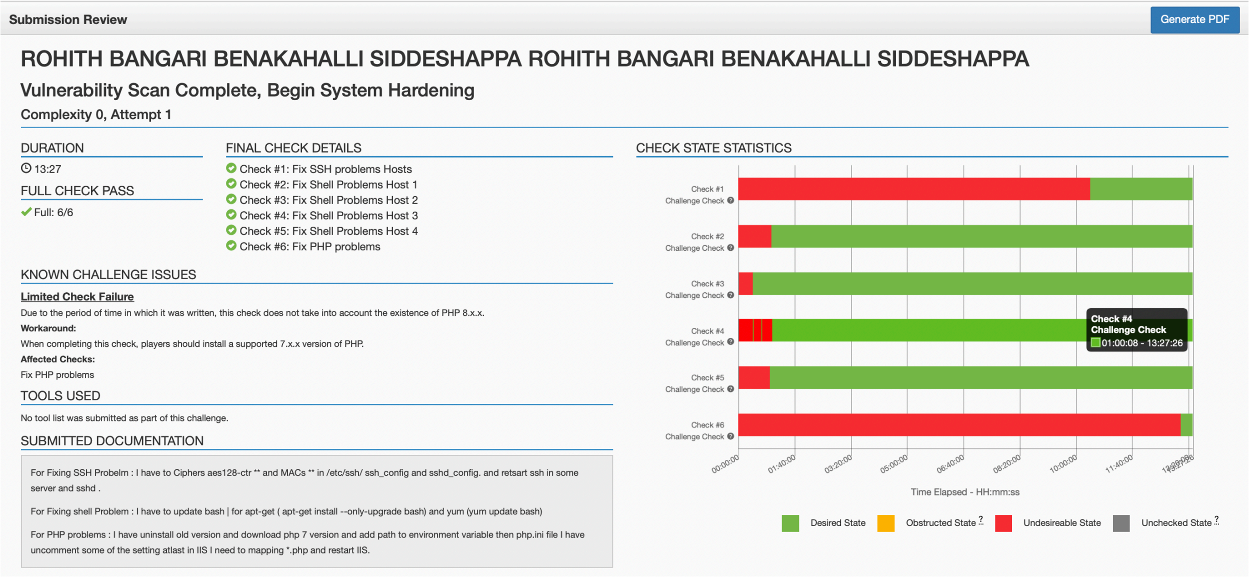
Which user accounts were compromised: rob,gthatcher,takasaka,ileventis,gbates,admin,playerone

Describe how the system was breached: Please include this in your documentation on the NICE Challenge Webportal.

How could this incident have been prevented: Please include this in your documentation on the NICE Challenge Webportal.

Recommended course of action after incident occurred: Please include this in your documentation on the NICE Challenge Webportal.

2) Vulnerability Scan Complete, Begin System Hardening:



ROHITH BANGARI BENAKAHALLI SIDDESHAPPA ROHITH BANGARI BENAKAHALLI SIDDESHAPPA

Vulnerability Scan Complete, Begin System Hardening

Complexity 0, Attempt 1

DURATION

13:27

FULL CHECK PASS

✓ Full: 6/6

FINAL CHECK DETAILS

- ✓ Check #1: Fix SSH problems Hosts
- ✓ Check #2: Fix Shell Problems Host 1
- ✓ Check #3: Fix Shell Problems Host 2
- ✓ Check #4: Fix Shell Problems Host 3
- ✓ Check #5: Fix Shell Problems Host 4
- ✓ Check #6: Fix PHP problems

CHECK STATE STATISTICS

KNOWN CHALLENGE ISSUES

Limited Check Failure

Due to the period of time in which it was written, this check does not take into account the existence of PHP 8.x.x.

Workaround:

When completing this check, players should install a supported 7.x.x version of PHP.

Affected Checks:

Fix PHP problems

TOOLS USED

No tool list was submitted as part of this challenge.

SUBMITTED DOCUMENTATION

For Fixing SSH Probelm : I have to Ciphers aes128-ctr ** and MACs ** in /etc/ssh/ ssh_config and sshd_config. and retsart ssh in some server and sshd .

For Fixing shell Problem : I have to update bash | for apt-get (apt-get install --only-upgrade bash) and yum (yum update bash)

For PHP problems : I have uninstall old version and download php 7 version and add path to environment variable then php.ini file I have uncomment some of the setting atlast in IIS I need to mapping *.php and restart IIS.