



INTERNATIONAL COLLEGIATE
CYBER DEFENSE
INVITATIONAL

Team 01 — NUST

Inject Scoring Sheets

Inject 1

ZOOM AND SLACK

Team #: 01

Scored By: James & LAHJA

Due by: 0:30

On Time? (Circle) ☒ Y N 5:08 pm

What Blue Team Receives

Set up your Slack account and connect to Zoom Conference. You should be connected to both of these at all times during the competition. Instructions can be found in your email. Please complete this by 0:30

Scoring Instructions:

Check to verify that the team is connected to both Zoom and Slack by viewing one of the computers for access to the Slack group and voice communication through Zoom service.

Scoring Rubric:

Connected to Zoom and Slack account is setup

[1]

NOTE: If the team is unable to connect to Zoom and setup Slack for communication by the deadline. It will be important to inform White team to assist with this step.

WHITE TEAM

Inject 2

WEBSITE

Team #: Region 01
Scored By: J. Kadamika

Due by: 1:30

On Time? (Circle)

Y

N

DNF

What Blue Team Receives

Rebrand the website to reflect the Aware merger. Complete the following changes:

- Change the header image from the Snak to the Aware branded image attached.
- Edit the About Us page to include the AWARE acquisition statement provided below.
- Post an announcement using the AWARE acquisition statement below on the front page of SNAK website.

Aware Acquisition Statement:

"We are excited to announce the merging of AWAR3 and SNAK. We believe this will further our efforts to integrate AI into more of what you do and to make our technology more widely available."

Have this completed by 1:30.

Scoring Instructions:

Verify that the website has AWARE branding with images and content. It should include the following graphics found below on the website.

Scoring Rubric:

AWARE graphics present on blue team website	[]
The "About Us" page is updated	[]
Announcement with the provided statement is on SNAK front page	[]

WHITE TEAM

Inject 3

JOIN AWARE DOMAIN

Team #: *Region 01*Scored By: *J. Kadamika*

Due by: 2:00

On Time? (Circle)

Y

(N)

*DNF***What Blue Team Received:**

In order to expand the Awar3.net domain across all regions, we need a domain controller that is joined to the awar3.net domain. Make ED209 a domain controller on the aware.net domain. Make sure to rename the machine to ED209RegionXX first so that there are not duplicate server names on the domain.

Join server "Bender" to the Aware domain.

Have this completed by 2:00

Scoring Instructions:

Verify that the ED209 machine is both renamed and a dc on the awar3.net domain. Check hostname and verify AD users and computers is available on the Awar3.net domain

Hostname Changed

[]

DC on Aware domain

[]

WHITE TEAM

Inject 4

DATABASE ADDITION

Team #: Region 01
Scored By: J. Kadamika

Due by: 2:30

On Time? (Circle)

Y



DNF

What Blue Team Received:

Hi Team,

Our database administrator was working on adding some new customers to the "CustomerDB" database. He received an emergency phone call and had to leave without completing the job. Your task is to find the file that contains the customer's information and add those customers to the "CustomerDB" database in the corporate server. He left you a sticky note saying, "look for a file called 'NewCustomers'".

Have this completed by 2:30.

Scoring Instructions:

Have blue team show the "Customer_table" in the "CustomerDB" database. Verify 70 records in the table..

Scoring Rubric:

All new customers are added to the customer database.

[]

WHITE TEAM

Inject 7

HASH VALUES

Team #: 01

Scored By: J. Kadamika.

Due by: 4:30

On Time? (Circle)

Y

N 20:50pm

8:30p m

What Blue Team Receives

Attached to this email, you will find a list of files which contain the usernames and personal information of our company employees. We have a feeling of that someone might made some changes to our files and made a copy of our records. I need you to look for the files that match these hash values to ensure that no changes have been made.

If you can get this filled out and get back to me by 4:30 that would be much appreciated.

Scoring Instructions:

Compare the hashes to the files by matching the key provided.

Scoring Rubric:

All Hashes Match

[M]

WHITE TEAM

ROOM JUDGE VERSION

Filename	MD5	SHA1	Matched?
securefiles2.zip	2e243f27e07ef17ffa36ef1c37efbcc5	86755771fa21b16d2b187160203ab4a67bc6bd77	[]
securefiles3.7z	b2c70c8d85da561956c9a28d770f4518	3a75f025a0b0f2aceee7a2426583a17ab0c41cbc	[]
SecurityX_Datafiles.zip	bde77dd588b3b4c6a1f72eb32ad6685e	a3ca181b24728dfd71cc2ca68bf8a79ddb6ec765	[]
System-Datasets-584-6ade9-dfa6ed.7z	b2c70c8d85da561956c9a28d770f4518	3a75f025a0b0f2aceee7a2426583a17ab0c41cbc	[]
AWARE CUSTOMER CACHE DATASET 63524-8567-74216.7z	af7e0d558e1d8a98325c5e0719154ed5	e982f7b05e3d1f1d77fee8195c4c10982c9b3ef6	[]
AWARE Security Updates 213586542.5535.zip	ad2479da90b78ab581a85f52ffa3ccae	92165644426b4dbf9c2f0e5ced93199a0e22da91	[]
AWARE Security Updates.7z	9c8e510dd3b6a9de804943c2fe17bcd3	b486baede6dd0e460da238f7d112e61aebfdd278	[]
Securefiles1.7z	7bdba364a9350a8b24c8c22250ed1af3	474ec6d07b54778a2a0022e07288dbc7eb11881b	[]
securefiles2.7z	f3432df897a5e4b38ed1c90b8f59f502	652a2f9c5dd652f126b6b1a71c37ab516cd16f57	[]

Inject 9

MAP NETWORK DRIVE

Team #:

01

Scored By:

Nakasole

7/7/2018
15:30

Due by: 6:00

On Time? (Circle)

(Y)

N

What Blue Team Received:

Hello Team,

Map a network drive on the machines that are joined to the Aware domain to the file share:

\\self.awar3.net\\snakfiles

We need this completed by 6:00.

10:00pm
- Team did on complete
- Had issues with VM
- ~~Team~~ Reported to help desk

- no response from help desk

Scoring Instructions:

Verify from blue team that they have access to the fileshare:

[fileshare path]

Scoring Rubric:

Access to the fileshare

[Y]

4pm

WHITE TEAM

Inject 11

GPO PUSH

Team #: 01 Nast

Scored By: Nakasole

Due by: 7:30 2:00

On Time? (Circle) ☒ Y N**What Blue Team Receives**

We have had some issues on our network, we believe our domain policy can be improved and should be better aligned with Aware's domain policy. If you could take a look at the following GPO's and make sure they are set correctly, it would be appreciated!

Password Policies

Account Lockout Policies

Set event log auditing for logon attempts

Scoring Instructions:

Let the Blue Team show Group Policies that were applied. Confirm for all the items in the rubric. They should show the Default Group Policy and ask to see the above listed. Mark off from list below:

Scoring Rubric:

- | | |
|---|-----|
| 1a) Password Length Policy (At least 12 characters) | [Y] |
| 1b) Complexity Requirements Policy (upper, lower, numeric, special) | [Y] |
| 2) Account Lockout Threshold Policy (3 maximum) | [Y] |
| 4. (Advanced Audit Policy Configuration) | |
| 4a) Audit Other Logon/Logoff (Failures set) | [Y] |
| 4b) Audit Logon (Failures set) | [Y] |
| 4c) Audit Credential Validation (Failures set) | [Y] |
| 4d. (Local Policy > Audit Policy) | |
| 4d) Audit Account Logon Events (Failures set) | [Y] |

WHITE TEAM