GIT- HAPPENS -THM

A simple room that explores a poorly configured git repository that can be accessed publicly. The room description mentions Version Control which for purposes of proper understanding this room, is the practice of tracking and managing changes to software code. For developers, version control systems are beneficial as they allow coordinated tracking of changes over time in a special database. Any mistakes that are made, can be reversed by comparing earlier versions of the code in order to sort out the issue.

More Information: <https://www.atlassian.com/git/tutorials/what-is-version-control>

Diving into the room ...

--------------------------------------------------------------------

There is not much to do with an unscanned IP address so let’s get nmap running.

***nmap -Pn -v -n --reason --disable-arp-ping -A -oA GitHappens -g 53 $IP\_address***

|\_\_ -Pn : disable host discovery, assume the host is up.

|\_\_ -v : verbose

|\_\_ -n : disable host name resolution (makes scan faster)

|\_\_ --reason : show the reason why a port state is shown

|\_\_ --disable-arp-ping : part of the host discovery disabling process

|\_\_ -A : perform an aggressive scan. Consists of Default Scripts, service detection, OS detection

|\_\_ -oA : save the output in all forms - xml, nmap and grep into GitHappens

|\_\_ -g 53 : make the traffic look like DNS traffic (usually used to evade firewalls or IDS/IPS)

|\_\_ $IP\_address : address from THM

After the scan we have our results. (Something I like to do while waiting for the scan to complete is just run the $IP\_address in the browser just to see if there is any web application running on default ports)

*PORT STATE SERVICE REASON VERSION*

*80/tcp open http syn-ack ttl 63 nginx 1.14.0 (Ubuntu)*

*|\_http-title: Super Awesome Site!*

*| http-git:*

*| 10.10.200.123:80/.git/*

*| Git repository found!*

*|\_ Repository description: Unnamed repository; edit this file 'description' to name the...*

*| http-methods:*

*|\_ Supported Methods: GET HEAD*

*|\_http-server-header: nginx/1.14.0 (Ubuntu)*

*No exact OS matches for host*

Following our above point, when browsing to $IP\_address directly, we get a login page. The room summary mentioned git so most likely we don’t need to attack the login page directly.

Our Nmap scan found a .git repository. Browsing directly to it we find directory listing is enabled (bad security practice).

*branches/ 23-Jul-2020 22:39 -*

*hooks/ 23-Jul-2020 22:39 -*

*info/ 23-Jul-2020 22:39 -*

*logs/ 23-Jul-2020 22:39 -*

*objects/ 23-Jul-2020 22:39 -*

*refs/ 23-Jul-2020 22:39 -*

*HEAD 23-Jul-2020 22:39 23*

*config 24-Jul-2020 06:25 110*

*description 23-Jul-2020 22:39 73*

*index 23-Jul-2020 22:39 645*

*packed-refs 24-Jul-2020 06:25 102*

As we are dealing with a Git repository, we need a tool to be download the repository, namely git-dumper. It is installed by pip install git-dumper

***git-dumper http://$ip\_address/.git/ .***

|\_\_ go to the specified URL

|\_\_ "." : save in the current directory

Running the above command, will dump the git repository onto our machine. We run the

***git log***

|\_\_ will show the logs of the development; ie the progression of events

One log file catches our attention.

*commit 395e087334d613d5e423cdf8f7be27196a360459 (HEAD)*

*Author: Hydragyrum <hydragyrum@gmail.com>*

*Date: Thu Jul 23 23:17:43 2020 +0200*

*Made the login page, boss!*

It references the login page. Run

git checkout 395e087334d613d5e423cdf8f7be27196a360459

|\_\_ switches to detached head state

In order to understand what is happening, we are "turning back time" and going to view how things where before changes were made at the particular time of the commit. As the display message explains More information : <https://www.cloudbees.com/blog/git-detached-head>

If we run

***ls -la***

And we look at the login page, which we remember is at index.html we see the user admin along with the password. Verifying it works we can log in. As we have a 'PoC' (Proof of Concept) the password is the flag and room completed.