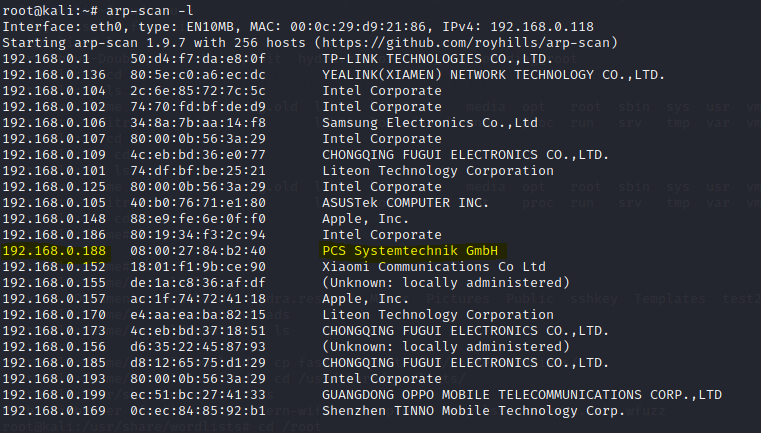
***GoldenEye-1 : Vulnhub Walkthrough***

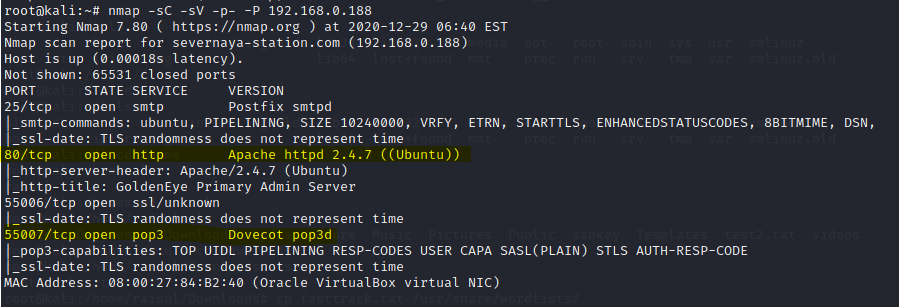
আজকে যে বক্সটি আমরা সলভ করবো তার নাম GoldenEye-1. এটি নিচের লিংক থেকে ডাউনলোড করা যাবে ।

<https://www.vulnhub.com/entry/goldeneye-1,240/>

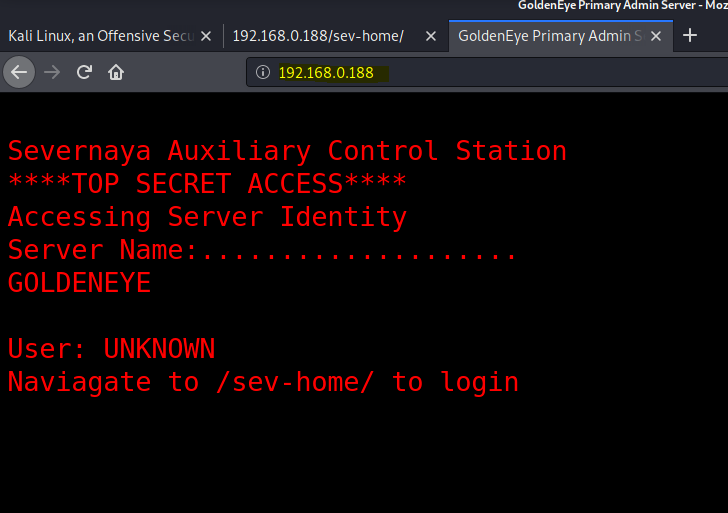
১। প্রথমেই আমরা arp-scan করি ।



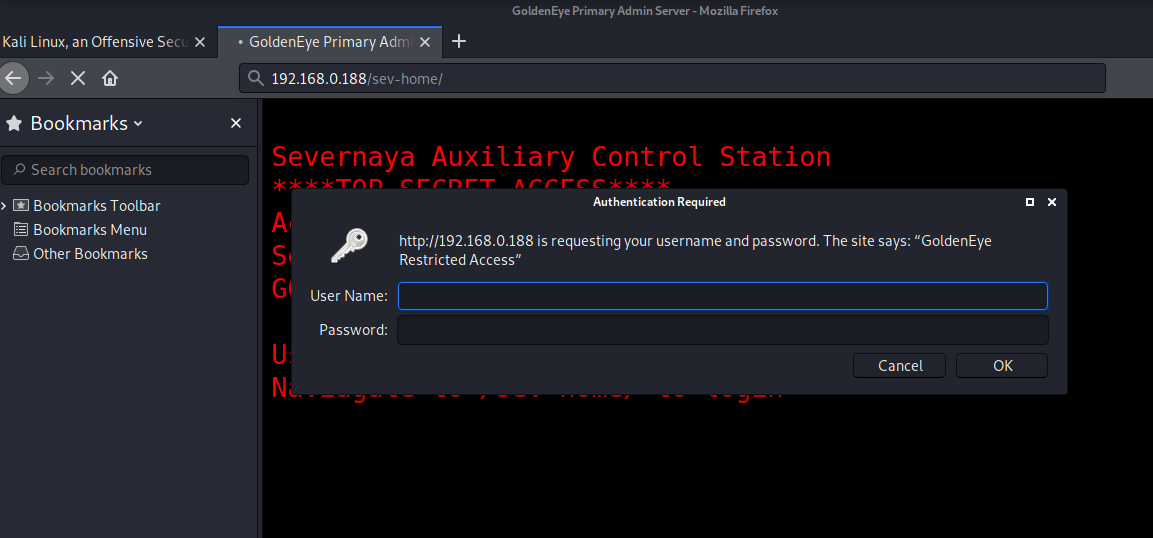
২। এবার প্রাপ্ত আইপিটিকে আমরা nmap-scan করবো ।



৩। Nmap-scan থেকে আমরা দেখতে পাচ্ছি যে চারটি open পোর্ট রয়েছে। আমি ব্রাউজারে ৮০ পোর্ট এ ip address টি রান করলাম এবং এটি একটি আকর্ষণীয় ওয়েব পেজ দেখিয়েছে।

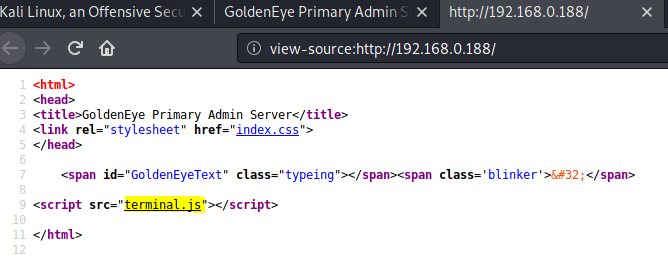


৪। উপরের স্ক্রিনশটটিতে প্রদর্শিত লেখায় একটি clue উল্লেখ করা হয়েছে। সুতরাং ব্রাউজারে "/sev-home/” এই url টি সন্ধান করি।

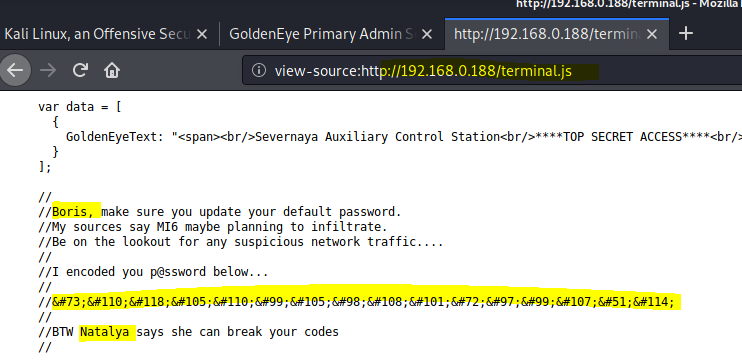


আপনি দেখতে পাচ্ছেন যে উপরের পৃষ্ঠাটিতে ব্যবহারকারীর নাম এবং পাসওয়ার্ড প্রবেশ করানোর জন্য অনুরোধ করা হয়েছে।

৫। আমি কোনও দরকারী ইঙ্গিতের জন্য হোমপেজে HTML চেক করা শুরু করেছি। এটি নীচে দেওয়া স্ক্রিনশটে দেখা যাবে।



৬। উপরের স্ক্রিনশটটিতে আপনি হাইলাইটেড এরিয়ায় দেখতে পাবেন যে "terminal-js" নামে একটি javascript ফাইল রয়েছে যা আকর্ষণীয় দেখায়। আসুন এই javascript ফাইলটি অন্য একটি ব্রাউজার উইন্ডোতে খুলি। এটি নীচের স্ক্রিনশটে দেখা যাবে।



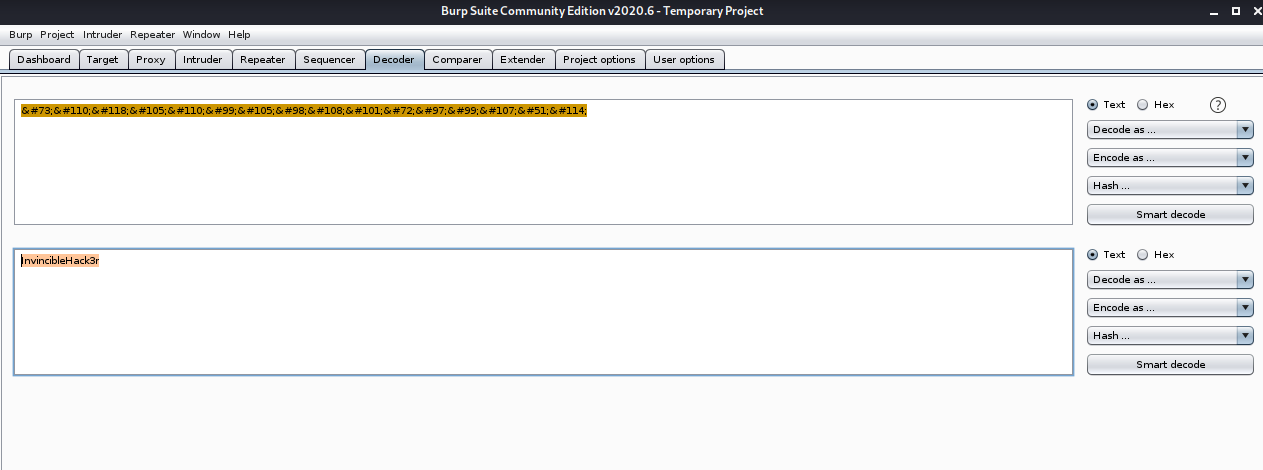
আমরা দুটি ব্যবহারকারীর নাম পেয়েছি। তারা নীচে তালিকাভুক্ত করা হয়েছে:

1. Boris 2. Natalya

আমরা একটি এনকোডযুক্ত string পেয়েছি যা উপরের স্ক্রিনশটটিতে হাইলাইট করা জায়গায় দেখা যায়। নীচে এনকোডেড string দেওয়া আছেঃ

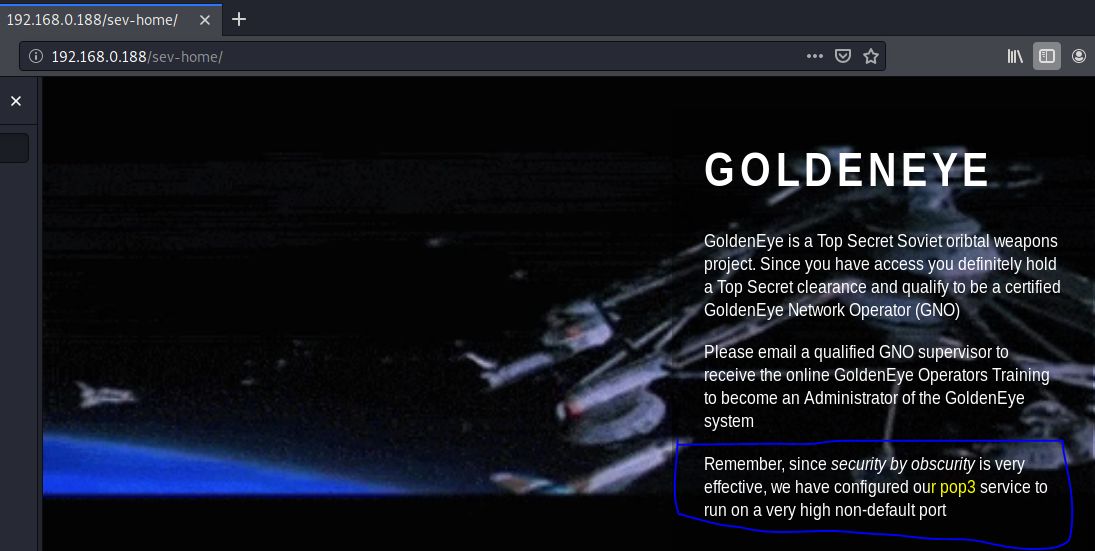
&#73;&#110;&#118;&#105;&#110;&#99;&#105;&#98;&#108;&#101;&#72;&#97;&#99;&#107;&#51;&#114;

৭। String ডিকোড করার জন্য আমি এইচটিএমএল ডিকোডার Burp Suite ব্যবহার করেছি।



৮। আপনি দেখতে পাচ্ছেন, আমরা পাসওয়ার্ডটি ডিকোড করেছি। আমাদের কাছে ইতিমধ্যে উপরে দুটি বৈধ ব্যবহারকারীর নাম পাওয়া গেছে, আসুন অ্যাপ্লিকেশনটিতে লগ ইন করার চেষ্টা করি।

**Decoded Password: InvincibleHack3r**

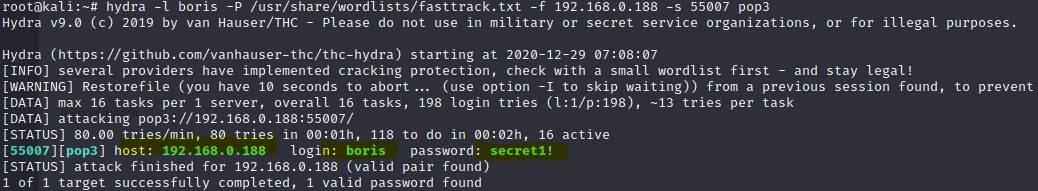


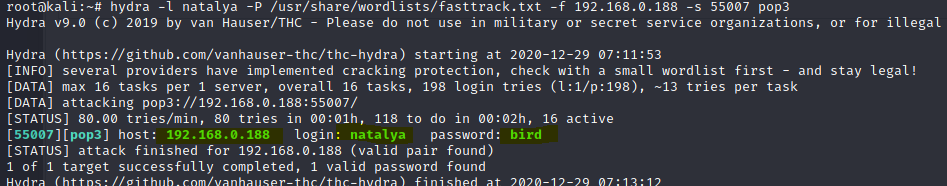
উপরের স্ক্রিনশটে এটি দেখা যাবে যে আমরা "GoldenEye" অ্যাপ্লিকেশনটিতে সফলভাবে লগ ইন করেছি। এটি উপরের স্ক্রিনশটটিতে হাইলাইট করা বার্তাটি নিম্নরূপ:

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

উপরের বার্তাটি থেকে আমরা বুঝতে পারি যে কিছু non-default পোর্টে একটি সক্রিয় pop3 service চলছে। আমরা প্রথম ধাপে ইতিমধ্যে টার্গেট আইপিতে একটি সম্পূর্ণ nmap স্ক্যান পরিচালনা করে জানি যে পোর্ট pop3 সার্ভারটি চলছে।

৯। এছাড়াও, "terminal.js" এর html বিশ্লেষণ করার সময় আমরা পেয়েছি যে, টার্গেট সিস্টেমটি default password ব্যবহার করছে। সুতরাং আসুন hydra এর সাথে pop3 service বরাবর "boris" ও “Natalya” ব্যবহারকারীর নামটি ব্যবহার করে password খুজে বের করার চেষ্টা করি ।

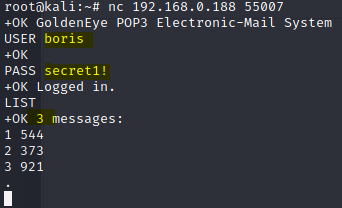




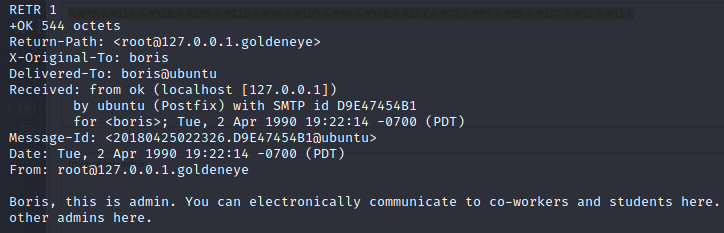
সুতরাং এখন আমাদের দুটি ব্যবহারকারীর নাম এবং পাসওয়ার্ড সংমিশ্রণ রয়েছে যা নীচের সারণীতে দেখা যাবে।

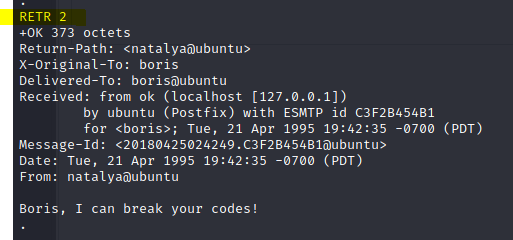
|  |  |
| --- | --- |
| **User Name** | **Password** |
| boris | secret1! |
| natalya | bird |

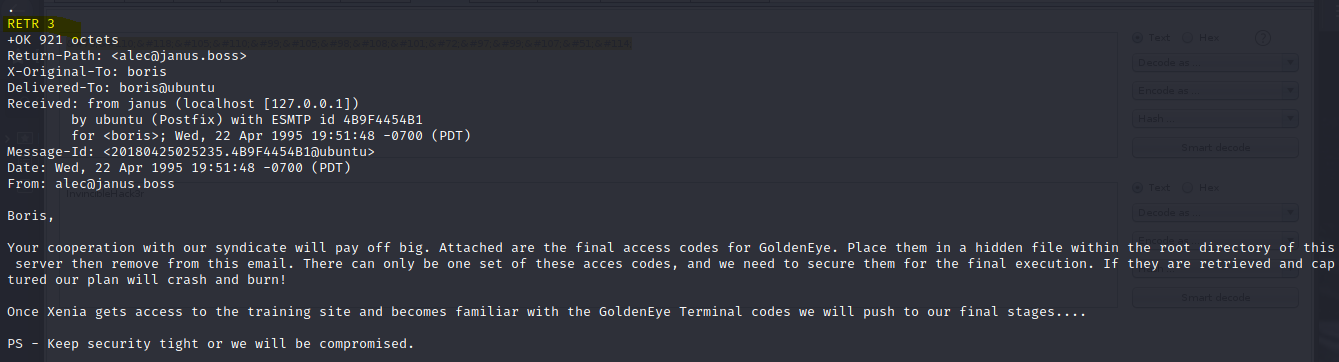
১০। আসুন এই অ্যাপ্লিকেশনটিতে লগ ইন করার চেষ্টা করি। আমি netcat দিয়ে pop3 পোর্টের মাধ্যমে টার্গেট সার্ভারে লগ ইন করতে "Boris" ও “secret1!” ব্যবহার করেছি। এটি নীচে দেওয়া স্ক্রিনশটে দেখা যাবে



১১। সুতরাং উপরের কমান্ড দ্বারা, আমরা খুঁজে পেয়েছি যে লক্ষ্য সিস্টেমে তিনটি ইমেল আছে। আমরা লক্ষ্য মেশিন সম্পর্কে কোনও দরকারী ইঙ্গিত পাই কিনা তা দেখতে এই ইমেলগুলি পড়ুন ।





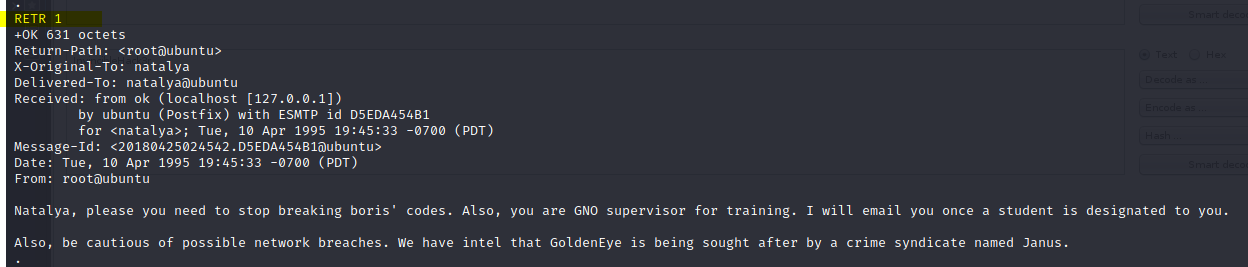


উপরের স্ক্রিনশটে আমরা দেখতে পাচ্ছি যে একটি ইমেল রয়েছে যাতে গোল্ডেনইয়ের অ্যাক্সেস কোডগুলি সংযুক্তি হিসাবে প্রেরণ করা হয় যা মূল ডিরেক্টরিতে রাখা হয়। তবে আমরা এখান থেকে সংযুক্তিগুলি পড়তে পারি না।

১২। আমি netcat দিয়ে pop3 পোর্টের মাধ্যমে টার্গেট সার্ভারে লগ ইন করতে "Natalya" ও “bird” ব্যবহার করেছি। এটি নীচে দেওয়া স্ক্রিনশটে দেখা যাবে



১৩। সুতরাং উপরের কমান্ড দ্বারা, আমরা খুঁজে পেয়েছি যে লক্ষ্য সিস্টেমে দুইটি ইমেল আছে। আমরা লক্ষ্য মেশিন সম্পর্কে কোনও দরকারী ইঙ্গিত পাই কিনা তা দেখতে এই ইমেলগুলি পড়ুন ।





উপরের স্ক্রিনশটটিতে, আমরা হাইলাইটেড এরিয়াতে দেখতে পাচ্ছি যে আমরা কিছু দরকারী তথ্য পেয়েছি যা নীচে দেওয়া হয়েছে।

**Username:  xenia**

**Password:  RCP90rulez!**

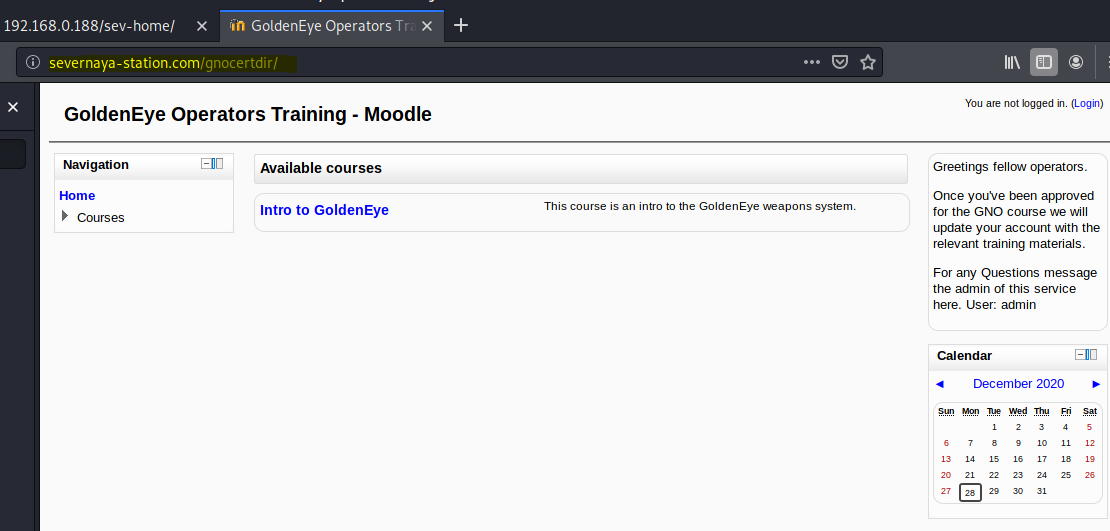
**Domain: severnaya-station.com**

**URL: severnaya-station.com/gnocertdir**

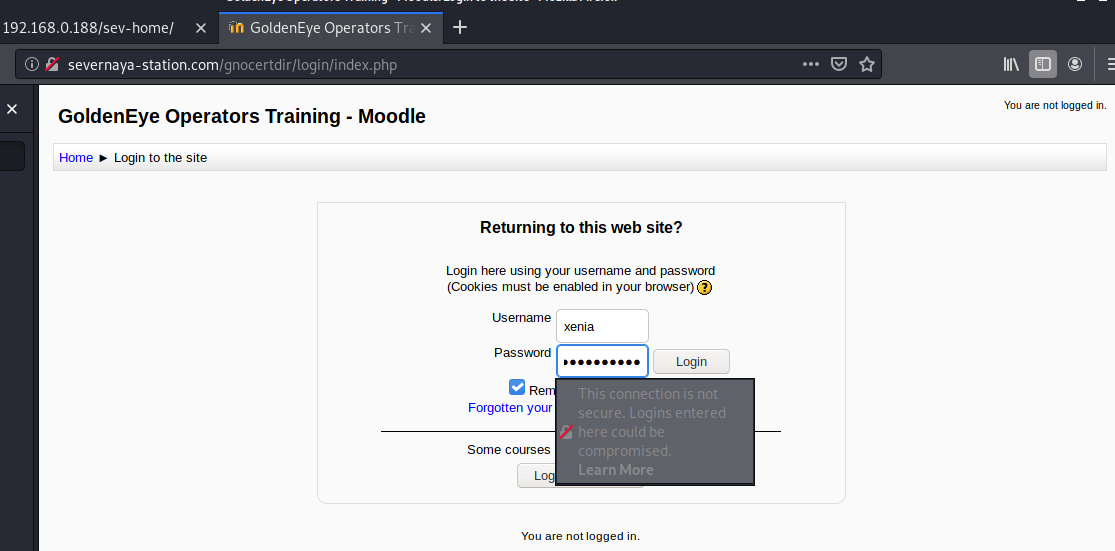
১৪। উপরোক্ত বার্তায় এটি উল্লেখ করা আছে যে আমাদের লক্ষ্য মেশিনের আইপি /etc/hosts URL বরাবর নির্দেশ করতে হবে। এখন এটি করা যাক।



১৫। উপরের স্ক্রিনশটে আমরা দেখতে পাচ্ছি যে URL সফলভাবে টার্গেট মেশিনে যুক্ত করা হয়েছে। সুতরাং ব্রাউজারে এই URL টি খুলুন।



১৬। এত চেষ্টার পরে, অবশেষে আমাদের কাছে টার্গেট মেশিনে ওয়েব অ্যাপ্লিকেশন চলছে। সুতরাং আসুন অ্যাপ্লিকেশনটিতে লগ ইন করার চেষ্টা করি।

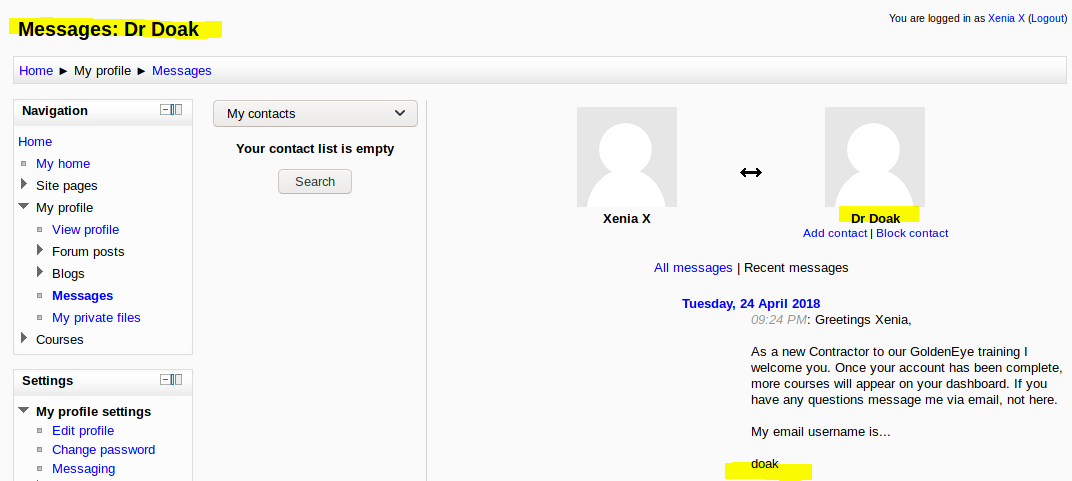


Credentials:

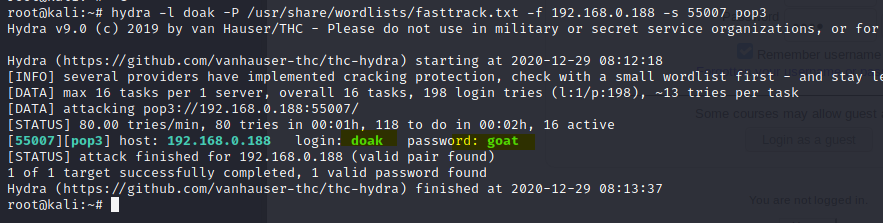
Username: xenia

Password: RCP90rulez!

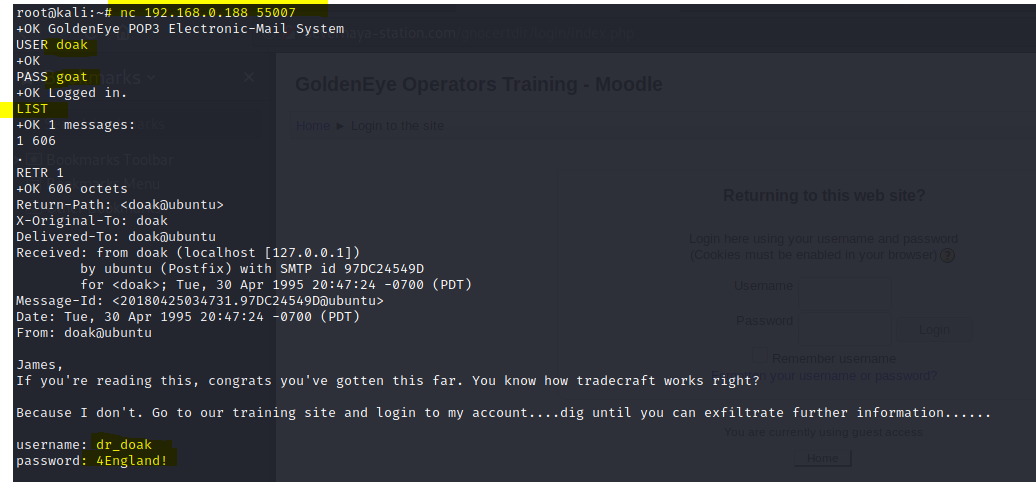
১৭। আমরা এখন অ্যাপ্লিকেশনটিতে লগইন করেছি। অ্যাপ্লিকেশনটি অন্বেষণ করার সময়, আমি বার্তা বিভাগে অন্য ব্যবহারকারীর চ্যাটটি পেয়েছি যেখানে একটি "ব্যবহারকারীর নাম" উল্লেখ করা হয়েছিল। এটি নিম্নলিখিত স্ক্রিনশটে দেখা যাবে।



১৮। অ্যাপ্লিকেশনটির পূর্ববর্তী পাসওয়ার্ড এবং ইঙ্গিতগুলি থেকে আমরা জানি যে সমস্ত ব্যবহারকারী দুর্বল পাসওয়ার্ড ব্যবহার করছেন। সুতরাং আমি নতুন পরিচয় ব্যবহারকারীর জন্য পাসওয়ার্ড গণনা করতে আবার hydra ব্যবহার করেছি।



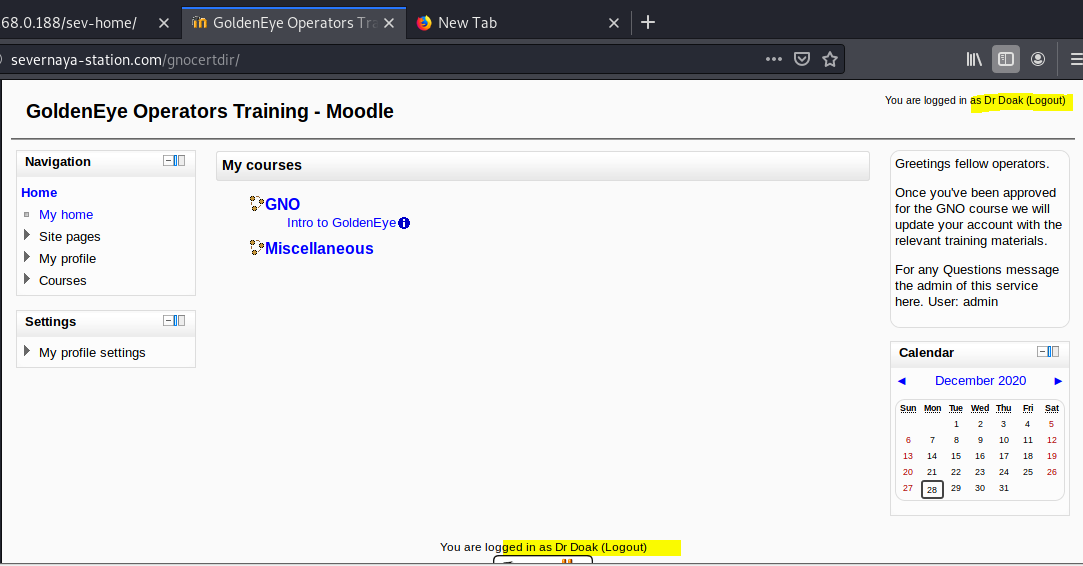
১৯। আপনি দেখতে পাচ্ছেন যে "doak" ব্যবহারকারীর জন্য পাসওয়ার্ডটি সফলভাবে ক্র্যাক করেছে যা "goat"। আসুন pop3 পোর্টে এই ইউজার ও পাসওয়াড দিয়ে লগ ইন করার চেষ্টা করি।



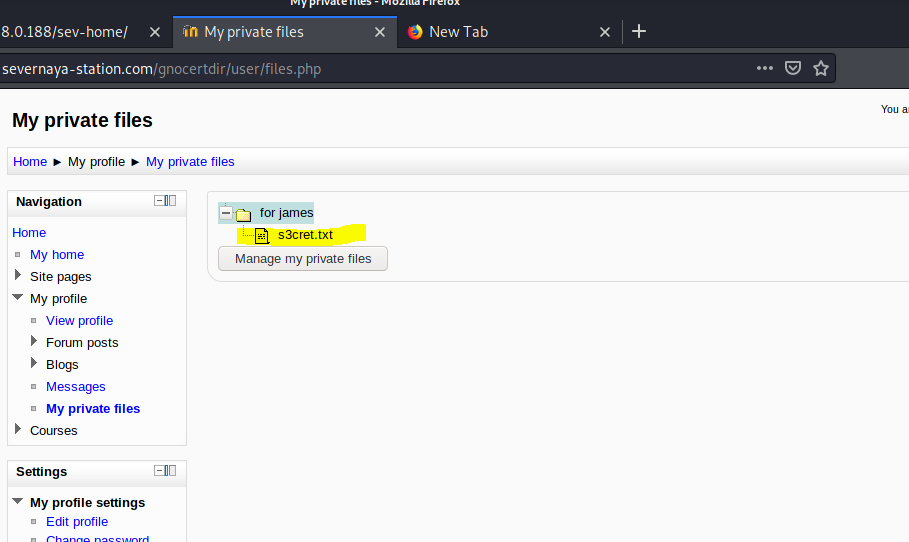
উপরের স্ক্রিনশটে যেমন দেখা গেছে, আমরা pop3 পোর্টের মাধ্যমে ব্যবহারকারী "ডোক" হিসাবে সফলভাবে লগ ইন করেছি।

২০। অ্যাপ্লিকেশনটিতে লগ ইন করার জন্য আরও একটি ইউজার ও পাসওয়াড পেয়েছি। আসুন লগইন করার চেষ্টা করি।

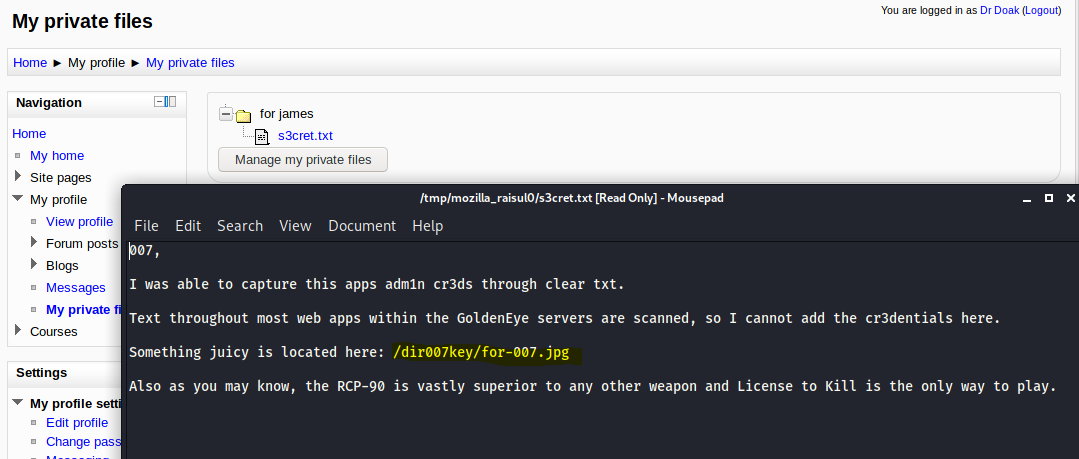
Credentials: dr\_doak  
Password: 4England!



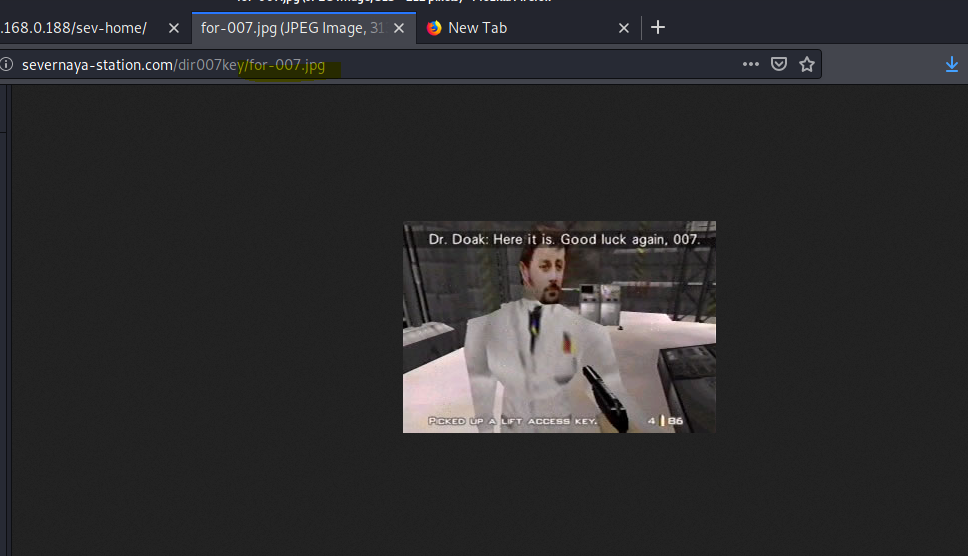
২১। স্ক্রিনশটে, এটি দেখা যায় যে আমরা অ্যাপ্লিকেশনটিতে "dr\_doak" ব্যবহারকারী হিসাবে লগ ইন করেছি। আমি আর কোনও clue এর জন্য অ্যাপ্লিকেশনটি অনুসন্ধান করতে শুরু করেছি। কিছুক্ষণ দেখার পরে, আমি অন্য একটি ব্যক্তিগত ফাইল পেয়েছি:



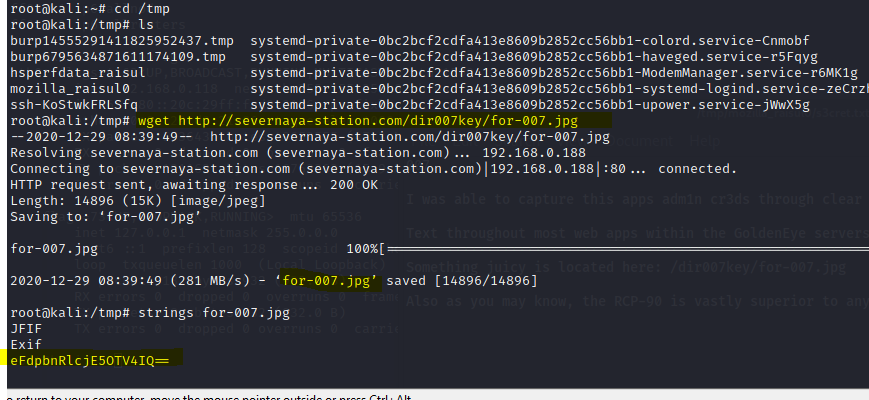
২২। উপরের স্ক্রিনশটে, ব্যক্তিগত ফাইলটি হাইলাইট করা হয়েছে। আমি লক্ষ্য মেশিন থেকে "s3cret.txt" ফাইলটি ডাউনলোড করে নোটপ্যাড দিয়ে খুললাম।



২৩। এখন আমরা ফাইলের বিষয়বস্তু দেখতে পারি। একটি আকর্ষণীয় ইঙ্গিত দেওয়া আছে যেটিতে বলা হয়েছে যে একটি চিত্র ফাইলে credentials লুকানো ছিল। এর সামগ্রীগুলি দেখতে ব্রাউজারে চিত্রটি খুলুন।



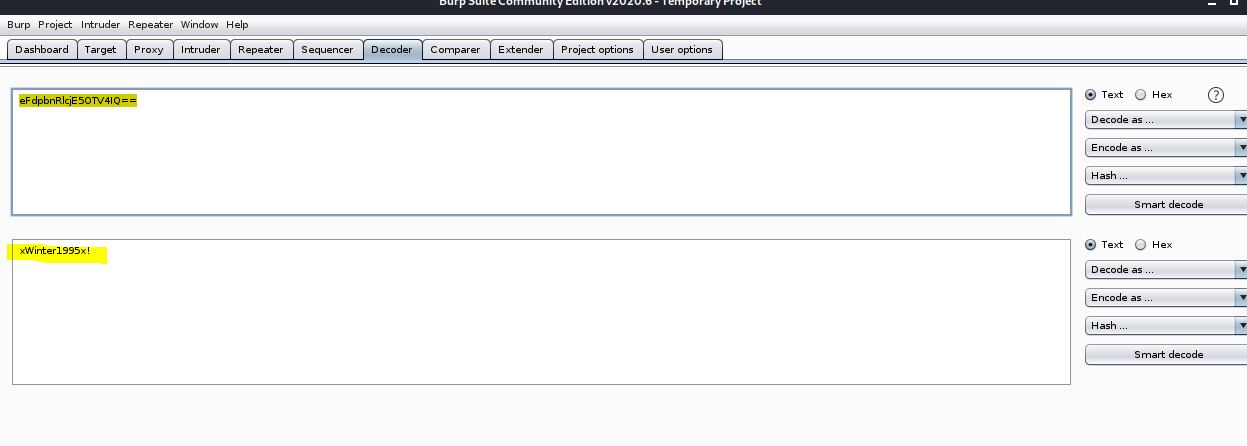
২৪। উপরের স্ক্রিনশটটিতে চিত্র ফাইলটি দেখা যায়, তবে এটি কোনও তথ্য দেয়নি। সুতরাং আমি আরও বিশ্লেষণের জন্য এই চিত্রটি ডাউনলোড করেছি এবং kali linux এর string ইউটিলিটি ব্যবহার করে ফাইলের সমস্ত string তালিকাভুক্ত করেছি। এটি নিম্নলিখিত স্ক্রিনশটে দেখা যাবে।



উপরের স্ক্রিনশটটিতে, একটি base-64 এনকোডেড স্ট্রিং রয়েছে। বেস 64 এনকোডেড স্ট্রিংটি নীচে দেওয়া হয়েছে:

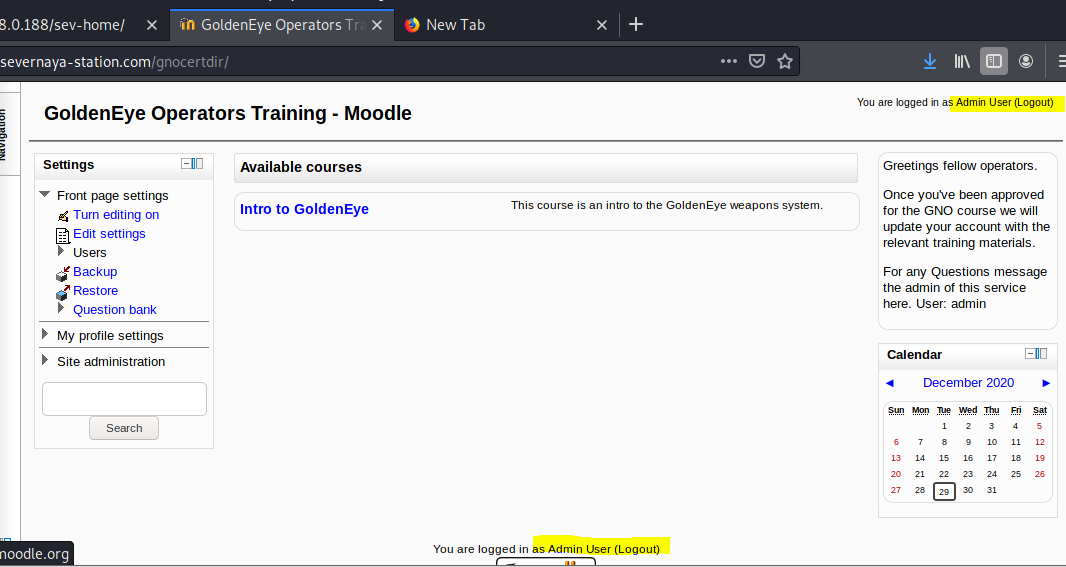
**EFdpbnRlcjE5OTV4IQ==**

২৫। Burp decoder ব্যবহার করে এই স্ট্রিংটি ডিকোড করি।



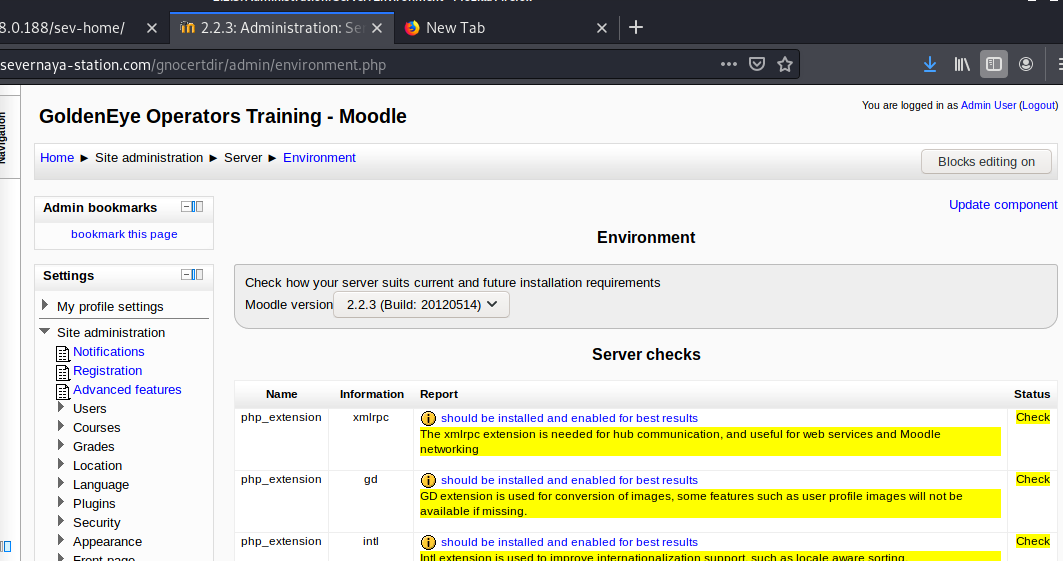
২৬। Base-64 স্ট্রিংটি ডিকোড করার পরে admin হিসাবে অ্যাপ্লিকেশনটিতে লগ ইন করি।

Username: Admin Password: xWinter1995x!

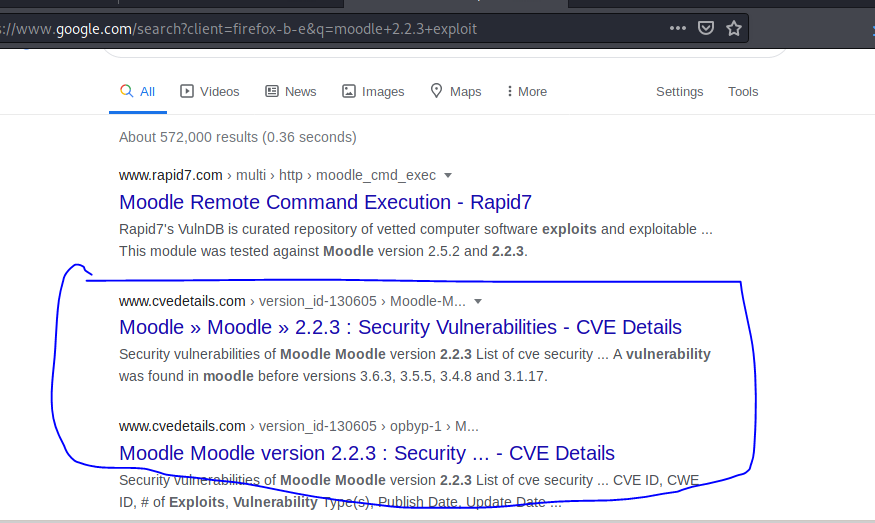


আমরা এখন অ্যাডমিন ব্যবহারকারী হিসাবে অ্যাপ্লিকেশনটিতে লগইন করেছি। এখন আমাদের কাছে টার্গেট মেশিনের রুট অ্যাক্সেস পাওয়া আমাদের মূল লক্ষ্য।

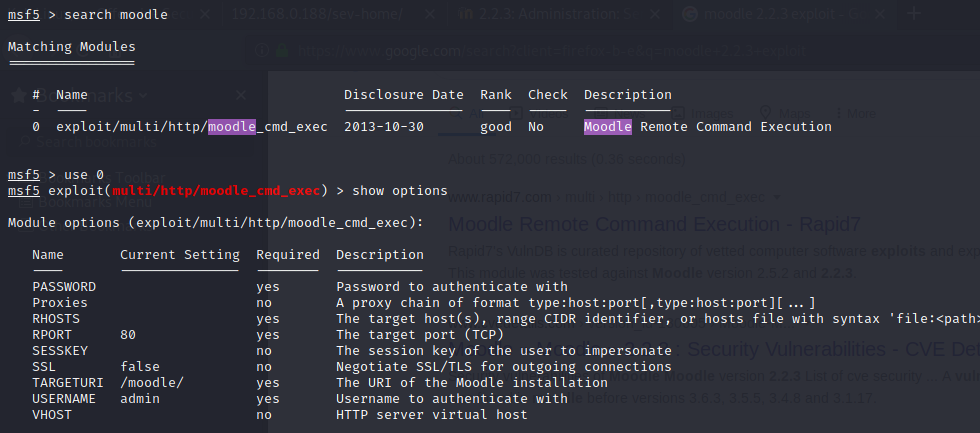
আমি অ্যাডমিন ব্যবহারকারী হিসাবে অ্যাপ্লিকেশনটি অন্বেষণ করতে গিয়েছিলাম। আমরা দেখতে পাচ্ছি যে অ্যাপ্লিকেশনটির নাম "moodle" এবং এটি ২.২.৩ সংস্করণ ব্যবহার করছে যা এটি নীচের স্ক্রিনশটেও দেখা যায়।



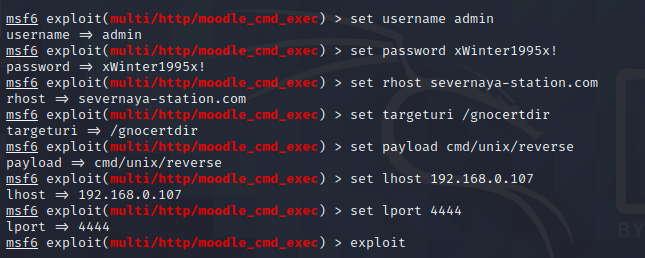
২৭। সংস্করণটির নাম পাওয়ার পরে, আমি গুগলে অনুসন্ধান করেছি। কিছু আকর্ষণীয় ফলাফল ছিল:



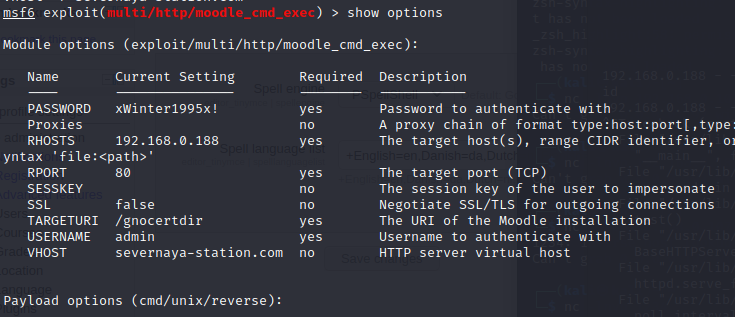
২৮। যেহেতু আমাদের টার্গেট মেশিনে shell access পাওয়া দরকার, এই জন্য একটি metasploit module দরকার। সুতরাং এর জন্য metasploit কনফিগার করা যাক।



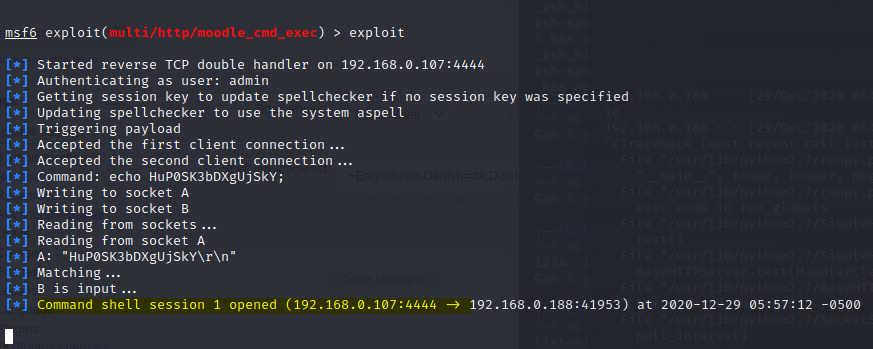
২৯। Exploit এর জন্য প্রয়োজনীয় ডেটা কনফিগার করা যাক:



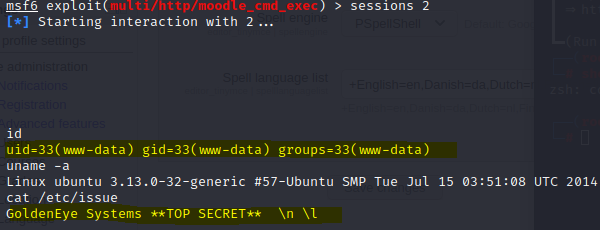
এখন আমরা সমস্ত প্রয়োজনীয় বিবরণ সেট করেছি। বিকল্পগুলি সেট করার পরে, চূড়ান্ত exploit নিম্নলিখিত স্ক্রিনশটের মতো দেখাবে:



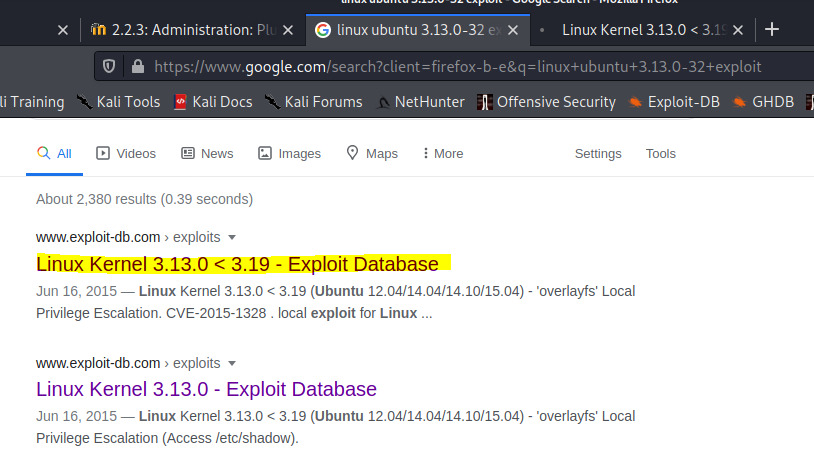
৩০। এখন আসুন লক্ষ্য সিস্টেমে কমান্ড লাইন অ্যাক্সেস পেতে exploit চালু করি।



৩১। উপরের স্ক্রিনশটে আমরা দেখতে পাচ্ছি যে exploit সফল হয়েছিল। আমাদের শেষ পর্যন্ত লক্ষ্য মেশিনের reverse shell! কিন্তু আমি যখন id কমান্ডটি চালাচ্ছি, এটি দেখায় যে এটি কোনও রুট ব্যবহারকারী নয়; এটি নিম্ন-সুবিধাযুক্ত ব্যবহারকারী যা www-ডেটা।



৩২। আমরা উপরের স্ক্রিনশটে দেখতে পাচ্ছি যে আমাদের অপারেটিং সিস্টেম এবং কার্নেল সংস্করণ নম্বর রয়েছে। তাই আমি স্থানীয় exploit এর জন্য গুগলে অনুসন্ধান করেছি এবং বেশ কয়েকটি বিকল্প পেয়েছি।



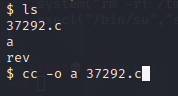
৩৩। আমি প্রথম exploit ব্যবহার করেছি এবং এটি টার্গেট মেশিনের "temp" ফোল্ডারে ডাউনলোড

করেছি। এটি নিম্নলিখিত স্ক্রিনশটে দেখা যাবে।

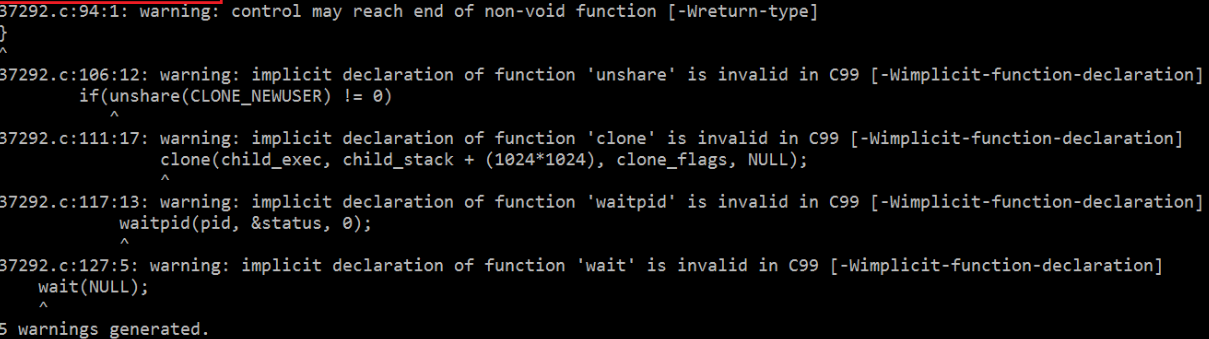


৩৪। উপরের স্ক্রিনশটে, আমরা দেখতে পাচ্ছি যে exploit টি লক্ষ্য মেশিনে "37292.c" হিসাবে

ডাউনলোড করা হয়েছে। তারপরে আমি CC সংকলকটি টার্গেট মেশিনে exploit করতে ব্যবহার করেছি,



৩৫। আপনি দেখতে পাবেন যে exploit কয়েকটি সতর্কতার সাথে সংকলিত হয়েছে। আসুন লক্ষ্য মেশিনে exploit কার্যকর করার চেষ্টা করি। এটি নিম্নলিখিত স্ক্রিনশটে দেখা যাবে।

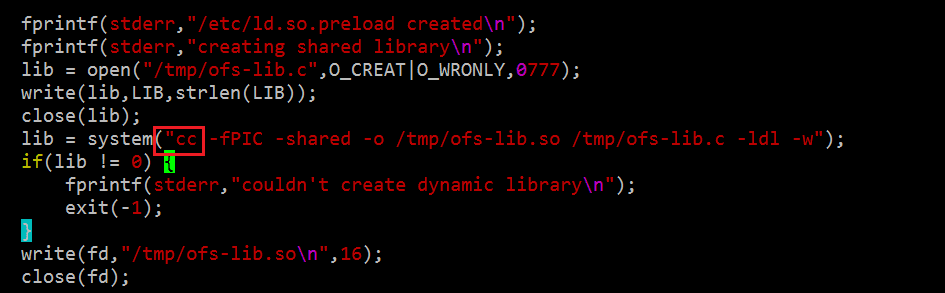


৩৬। যদি আপনি দেখতে পান যে সম্মতিযুক্ত exploit সফলভাবে সম্পাদন করা যায়নি। আমি এটি কার্যকর

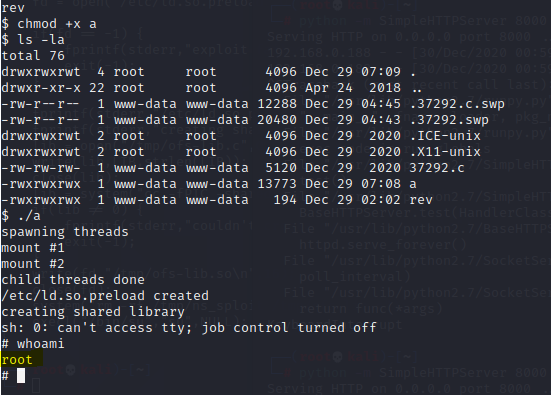
করার জন্য যে কোনও সম্ভাব্য উপায় সন্ধান করার জন্য exploit টি পরীক্ষা করে দেখেছি যে একটি gcc

কমান্ড ব্যবহার করছে। যেহেতু gcc লক্ষ্য মেশিনে উপলভ্য ছিল না, তাই আমি exploit টি সংশোধন করে

"gcc" পরিবর্তন করে "cc" করেছি।

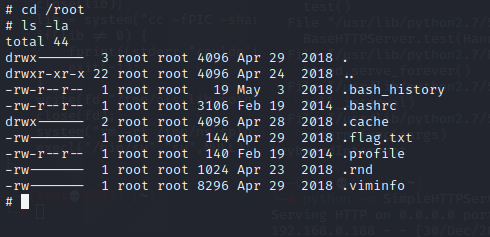


৩৭। Exploit এর পরিবর্তনগুলি সংরক্ষণ করার পরে, আমাদের এটি আবার cc কম্পাইলারের সাথে সংকলন করতে হবে এবং এটি কার্যকর করার চেষ্টা করা উচিত।

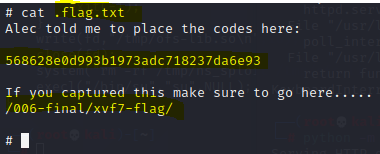


উপরের স্ক্রিনশটে আমরা দেখতে পাচ্ছি যে আমাদের লক্ষ্য মেশিনের মূল অ্যাক্সেস রয়েছে। এটি whoami কমান্ড দ্বারা নিশ্চিত করা হয়েছে।

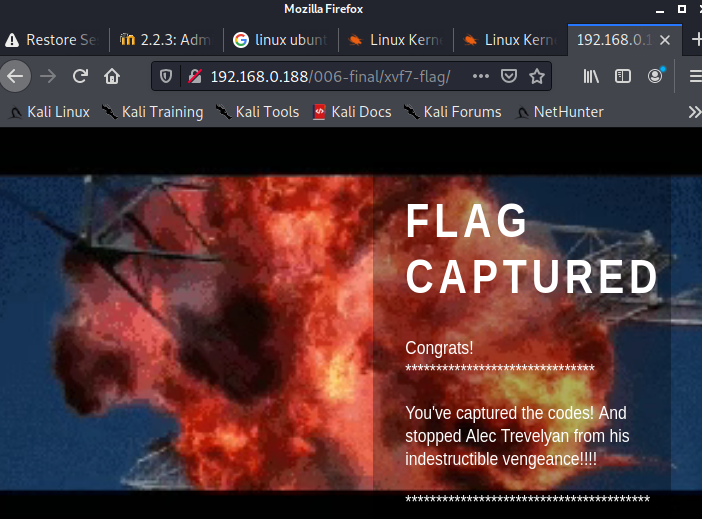
৩৮। চ্যালেঞ্জের বর্ণনা অনুযায়ী লক্ষ্য মেশিন থেকে দুটি flag নেওয়া। উভয় পতাকাই মূল ডিরেক্টরিতে ছিল বলে এটি কোনও কঠিন কাজ ছিল না।



৩৯। flag গুলি পড়ি।



৪০। আপনি দেখতে পাচ্ছেন যে দ্বিতীয় flag এর জন্য একটি পথ দেওয়া আছে। সুতরাং এর সামগ্রীগুলি পড়ার জন্য এটি ব্রাউজারে চালানো যাক।



আমরা এটা করেছি!

যেহেতু আমরা উভয় ফ্ল্যাগ ফাইলগুলি সাফল্যের সাথে পড়েছি, এটি CTF সম্পূর্ণ করে। আমি আশা করি আপনি এই যন্ত্রটি উপভোগ করেছেন।