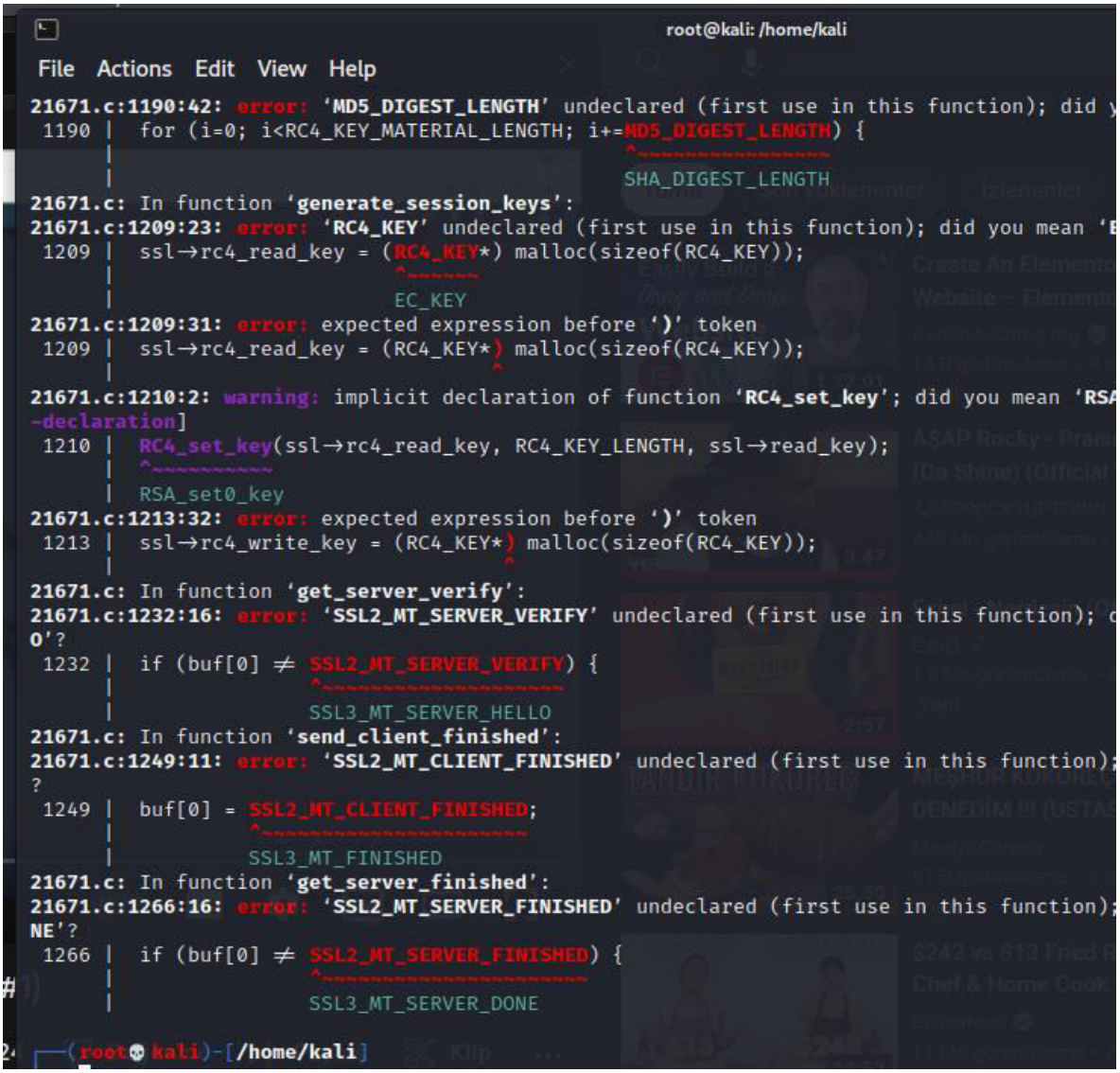
Kioptrix CTF
1-5

Muhammed Fatih YILMAZ
mfth78@hotmail.com

İçerik

Kioptrix 1

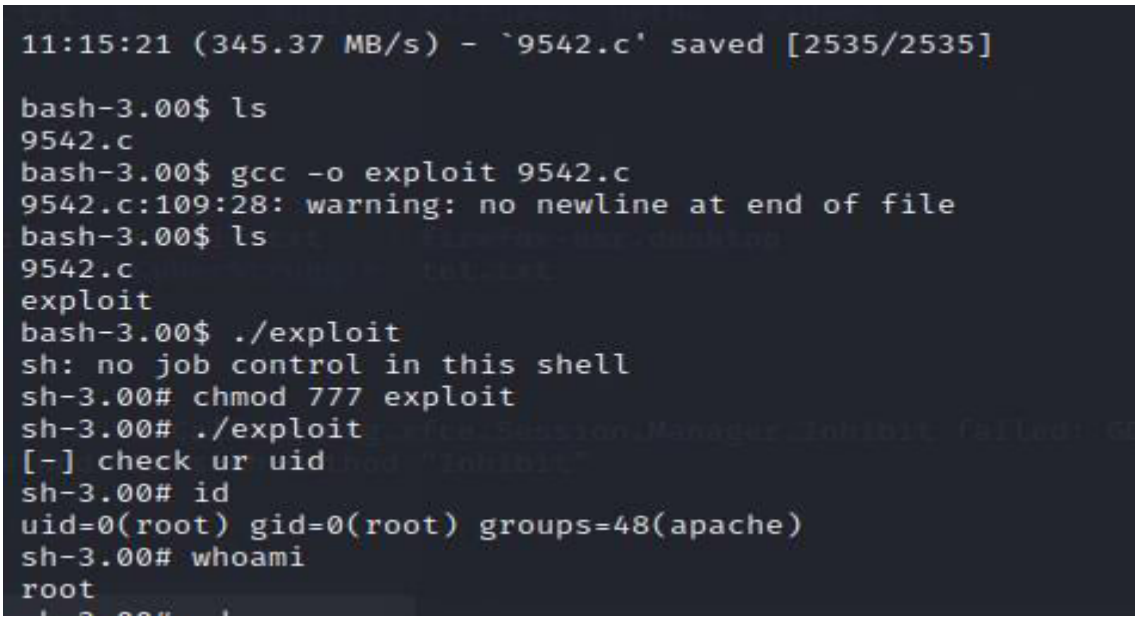
Bu CTF ile alakalı öncelikle nmap taraması yapıp ssh,http,smb netbios portlarının açık olduğunu gördüm 80 portu açık olduğu için tarayıcıma ip adresini yazdım. Çıkan sayfaya sayfa koduna bakıp sömürebileceğim bir şey varmı diye baktım fakat bulamadım ardından gobuster ile wordlist taraması yaptım açık olan portlara baktığımda mod_perl diye directorynin açık olduğunu gördüm exploit edebilmek için internete yazdım fakat elimdeki kullanabileceğim toollarla alakalı bir şey bulamadım ardından tek tek ssh ve smb portlarının versiyonlarını yazıp searchsploit komutuyla taradım OPENFUCK.c adında dosya buldum. Buradan sonra takıldım çünkü dosyayı executable bir dosyaya çevirmeye çalıştığımda hep encryption hatalarını veriyodu internete baktım ancak hala yapamadım. Ardından videolara baktım nasıl çözmüşler diye aynı şekil kodu düzelttim fakat hala bende aynı hatayı vermeye devam etti o yüzden root yetkisine ulaşamadım.



1. 1 Hata mesajı

KİOPTRİX 2

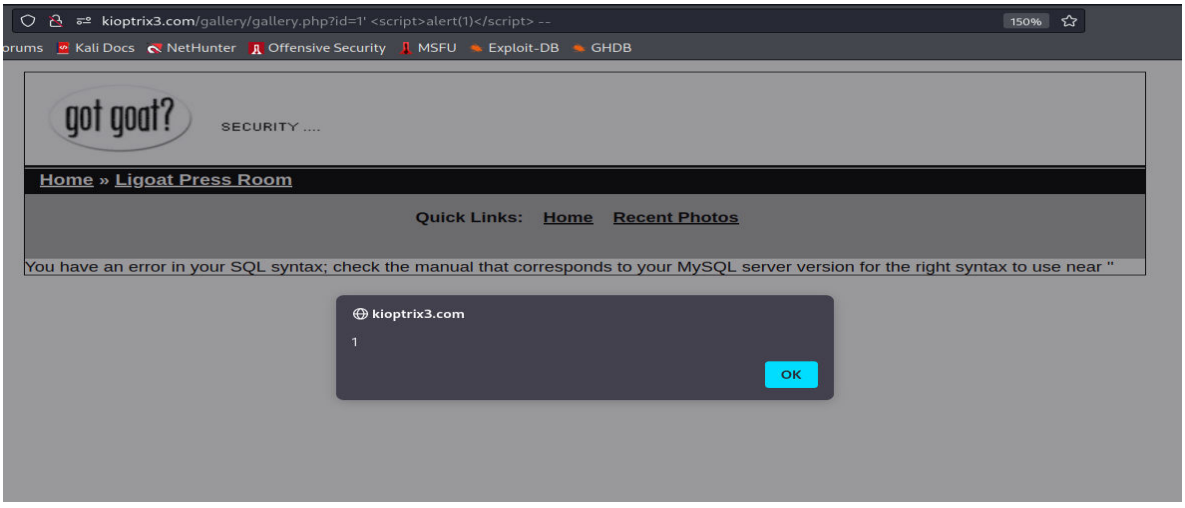
Bu CTF en rahat çözdüğüm CTFlerden biriydi. Nmap taraması yapıp çıkan sonuçlara baktım. Yine ssh,http portları açıktı bu sefer farklı olarak arkada mysql portu da çalışıyordu ve açıktı yine her zaman yaptığım gibi ip sini girip web sunucusuna göz attım. Remote system admin login sayfasıyla karşılaştım ardından aklıma gelen ilk zaafiyet sqli oldu. İnject komutlarını denedim ve admin olarak içeri girdim. Ping machine to network yazan bir ekranla karşılaştım.Localhosta ping göndermeyi denedim normal ping komutu gibi konsolda çıkan yazılar ortaya çıktı. ; semicolonla fakrlı iki kodu aynı satırda çalıştırabileceğimi biliyordum. Bunu yazıp kendi pwd yazdım dizini gösterdi. Ardından netcat komutuyla reversshell yapmayı denedim ancak burada da nc komutu karşı pc de çalışmadığından başarılı olamadım reverse Shell yazdım Google a bin/bash üzerinden reverse Shell yapan bir payload gördüm kendi ip ve port bilgilerimi yazıp bağlantıyı kurdum. Whoami yazdığımda Apache gözüküyodu bakmak roota ulaşmak için find komutuyla sticky bit e sahip olan kullanıcıları aradım fakat başarılı olamadım. Burada tıkalı kaldım internete başvurdum çözüm üzerinden Central OS 4.5 zaafiyeti varmış bunun scriptini ana makineye alıp çalıştırdım root erişimine ulaştım.



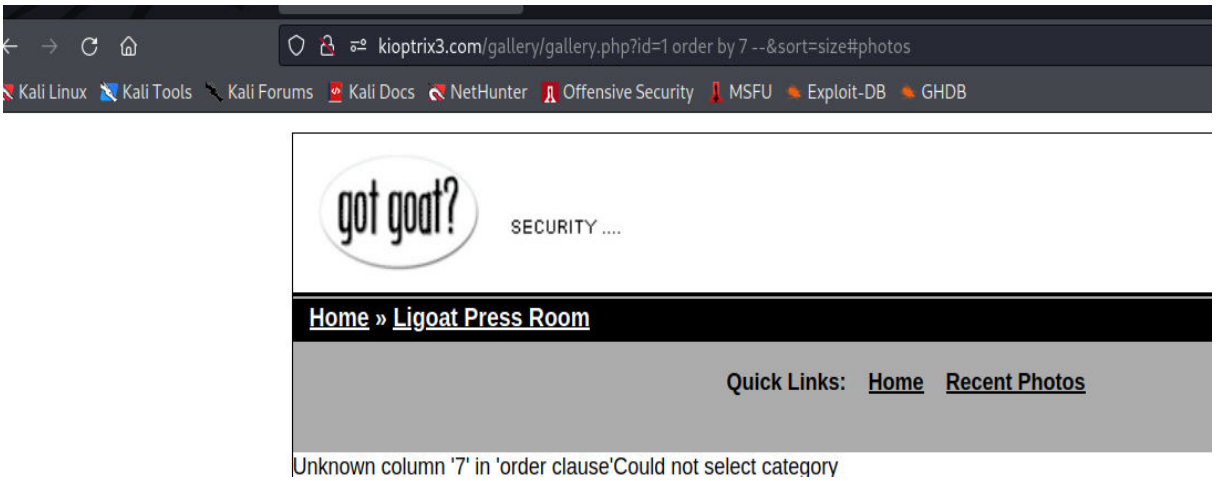
Root Access

KİOPTRİX 3

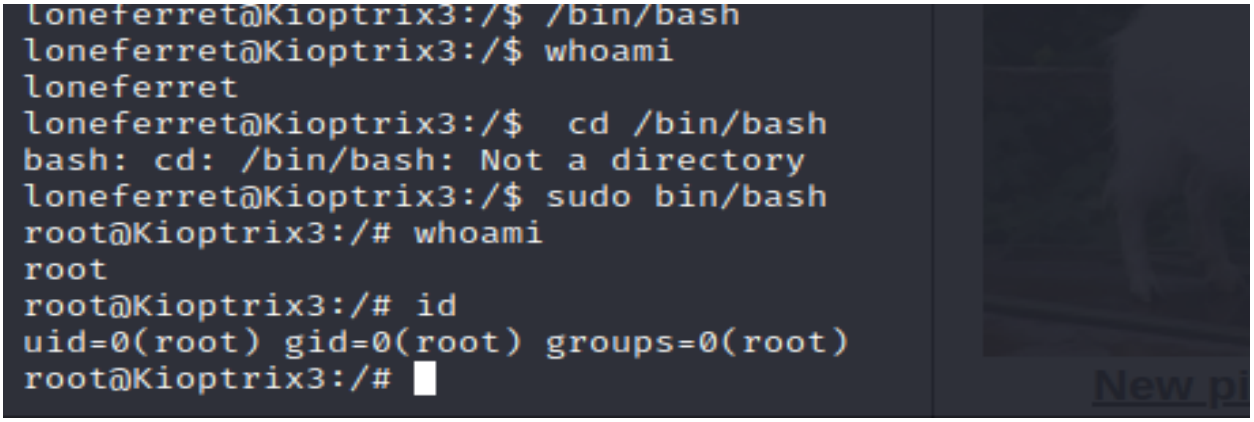
Bu CTF de ise standart olarak nmap taramasıyla başladım yaptığım tarama sonucu ssh portunun http portunun açık olduğunu gördüm her zamanki gibi taraya tarayıcıya 80 HTtp portunu yazdım ardından çıkan sayfayı inceledim home blok login adında 3 tane link gördüm direk login kısmına yöneldim herhangi bir sql injection olmasına karşın sql sorgularını denedim. Gobuster taramasıyla phpmyadmin açık olduğunu gördüm login kısmına denediğim sorularla birlikte içerisine şifresiz giriş yapabildi fakat phpmyadmin de kendim zafiyet bulamadım ardından diğer linklere tıklayarak sayfa kodlarını inceledim galeri kısmına geldiğimde fotoğraflarla karşılaştım fotoğrafların üzerine tıkladıktan sonra linkte sql sorgularını çalıştığını gördüm bunun üzerine sql sorgularını zafiyet içerip içermediğini anlamak için denedim sonrasında mysql databasesesi hata mesajı döndü zafiyetin olduğunu anladım. Zafiyeti sömürmek için mysql insjection cheat sheet taraması yaptım union sqli denedim. Union based sql injection da column numberın aynı olması gerektiğinden column sayısını bulmak için order by ı kullanarak 6 tane column olduğunu ogrendim. Sonra UNION SELECT 1,2,3,4,5,6 yaparak dönen değeri kontrol ettim 2 ve 3 değerlerinde herhangi bişey dönmüyodu oralara database() i bulmak için sorgular yazdım. Aynı zamanda id kısmında XSS zaafiyetide buldum. Dev accounts adında table buldum burdan username ve pass çekerek 2 tane kullanıcıya ulaştım encode edilmiş şifreleri decode ederek kullanıcı adlarıyla ssh servera bağlandım. CompanyPolicy adında readme dosyasında yeni bişey oluşturmak için sudo ht kullanın yazıyordu bende bunu kullanmaya çalıştım. Terminali export ederek xterm yaptım ardından mavi bi ekran açıldı burada nasıl zaafiyeti alacağımı bilmediğimden uğraştıktan sonra internete başvurdum. Sudoers dosyasını açıp içine /bin/bash eklediklerini gördüm yaptıktan sonra basha geldiğimde root yetkisini elde etmiştim.



XSS



SQL İNJECTİON BELİRLENMESİ

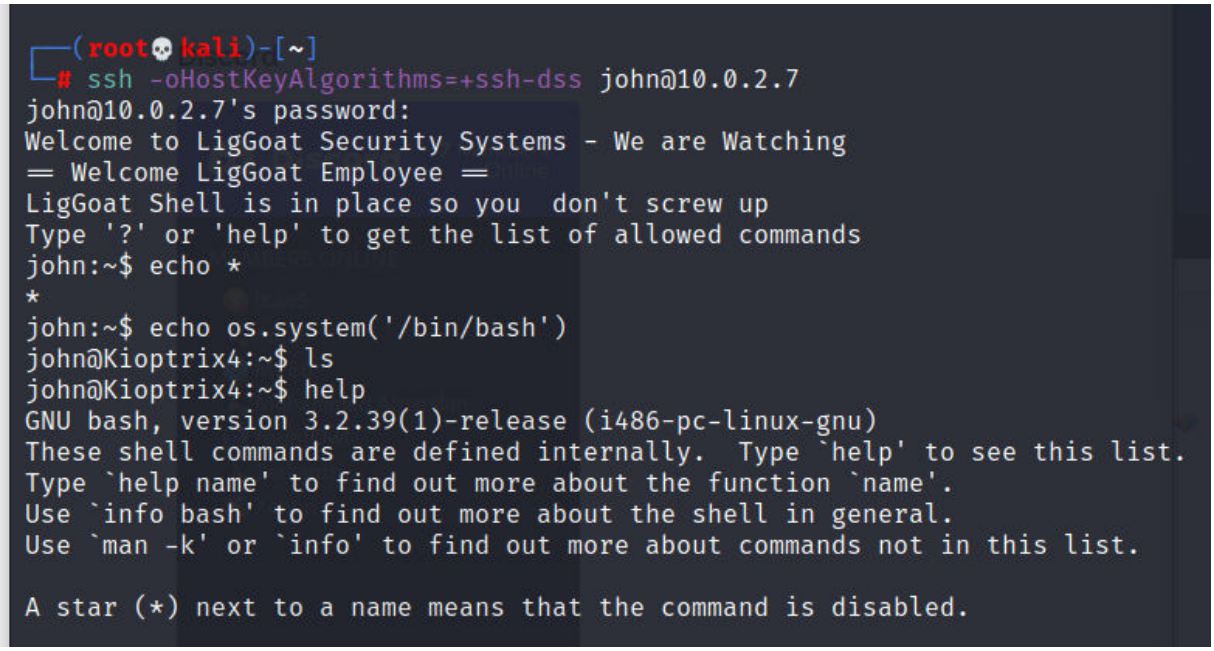


ROOT ACCESS

KİOPTRİX 4

Bu CTF te çözerken baya zorlandım hatta en son çözümünü izleyip anlamadığım CTFtir kendisi. Her zaman uyguladığım nmap ve gobuster taramalarını gerçekleştirdim. John ve robert adında 2 kişinin php dosyalarını gördüm ama içine girilmiyodu login ekranına yönlendiriyodu.Burada da karşıma bir login ekranı geldi normalde denediğim sql injection sorguları burada çalışmadı cheat sheetten baktım. 1'or '1'='1 sorgusunu denedim çalıştı. Kullanıcıların adlarını girerek denedim karşıma johnun passwrodu geldi sql injectionla giriş yapınca, aynısı robertte de gerçekleşti. Ssh ın içine bu kullanıcı adı ve pswd la girmeye çalıştım. Girince kısıtlı bir Shell vardı herhangi bi linux komutunu çalıştırmıyodu. Belli başlı kendi içinde izin verdiği sınırlı komutlar vardı. İnternet üzerinden arayınca bunun limited Shell olduğunı öğrendim. Daha sonra echo komutunun Python kodlarını çalıştırabildliğni öğrendim[Şekil 1]. Buradan bash scripte geçtim ve devamında sudoers dosyası aradım iznim

yoktu internetten zafiyetlere baktım fakat bulamadım youtubdan çözümünü izledim hiç bilmediğim sql sorguları yazıp root Access sağlamışlardı ama kafamda tam oturtamadım.

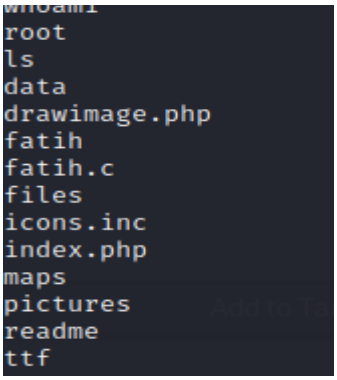


Şekil 1

KİOPTRİX 5

CTF için önceden çözdüklerimde deneyim kazanarak daha rahat çözdüm. Sayfayı açıp standart tarama aşamalarını uyguladım. Ssh portunun kapalı olduğunu gördüm. 80 ve 8080 portu açıktı. Tarayıcıya yazdığımda ıt Works yazan ekranla karşılaştım. Inspect element yapıp içerikte bişey saklanmışmı diye baktığımda pchart urlsi gördüm url kısmına ekledim. Chart dosyaları karşıma çıktı içindeki değerler değiştirilebiliyordu. XSS varmı diye kontrol ettim bu kısımda XSS buldum. Başka işime yarar dosya bulamadım pchartı internete yazıp exploit varmı diye taradım. Exploit buldum directory treversal ile verdiği urlyi linkime ekledim etc/paswd dosyasına ulaştım. Web sunucusnun conf dosyasına nasıl erişeceğimi bulmaya çalıştım 8080 portuna bağlantıya izin vermyodu çünkü araştırmalarım sonucunda buldum. Burada Apache 2 yazan linki yapıştıdım fakat karşıma herhangi bir şey çıkmadı bende yanlış yaptığımı düşünerek 1.5 saatimi harcadım ardından youtuba yazıp baktığımda 22 yazdıklarını gördüm bunu görünce daha çok sinirlendim. 8080 portuna erişebilmek için mozilla 4 sürümünden bağlanmak gerekiyormuş burp u açıp Proxy isteği olarak isteği attım. Phptax adında bölüm açıldı pcharta yaptığım zaafiyet araştırmasının aynısını buna da yaptım.Metasploitten birkaç tane phptax zaafiyeti buldum. Bunları denedim. Bunuda yaparken kanser gibi oldum çünkü payload seçmek gerekiyormuş reverse Shell için ben seçmemiştim. Bunuda youtube sayesinde öğrendim gerekli RHOST RPORT LHOST adreslerini girerek shelle ulaştım. Bundan sonra Privlige escalitionu youtubdan izledim. FreeBSD üzerinden zaafiyet taraması yapıp gerekli c dosyasını nc ile reverse Shell yapıp karşı pc ye aktardım. Chmod +x yetkisi verip root olarak giriş sağlamış oldum.


root@kali: ~
File Actions Edit View Help
(root kali)-[~]
msfconsole
=[metasploit v6.1.4-dev]
+ -- --=[2162 exploits - 1147 auxiliary - 367 post]
+ -- --=[594 payloads - 45 encoders - 10 nops]
+ -- --=[8 evasion]
Metasploit tip: Use sessions -1 to interact with the
last opened session
msf6 > use exploit/multi/http/phptax_exec
msf6 exploit(multi/http/phptax_exec) > ls
[*] exec: ls
Desktop Documents Downloads dsniff.services go Music Pictures Public Templates Videos
msf6 exploit(multi/http/phptax_exec) > show options
Module options (exploit/multi/http/phptax_exec):
Name Current Setting Required Description


whoami
root
ls
data
drawimage.php
fatih
fatih.c
files
icons.inc
index.php
maps
pictures
readme
ttf