21 – [illegible] CEH [illegible]

[illegible] CEH [illegible] :([illegible])

[illegible]

[illegible] CEH [illegible]

Privilege Escalation and Exploiting) [illegible] (Vulnerabilities

[illegible]:

■ [illegible]

■ [illegible]

■ [illegible]

■ Web Services Terminal Microsoft [illegible] Remote Desktop Bomgar [illegible]

[illegible] DLL [illegible].

[illegible]

[illegible] StickyKeys [illegible] Shift [illegible] StickyKeys [illegible] cmd.exe [illegible] sethc.exe [illegible] explorer.exe [illegible] exe. [illegible] cmd.exe [illegible] (systemroot%\system32%) [illegible] cmd.exe [illegible] StickyKeys [illegible] shellcode [illegible] LocalSystem [illegible].

StickyKeys [illegible]

[illegible] StickyKeys [illegible] Windows / System32 [illegible] sethc.exe [illegible] sethc_1.exe [illegible] cmd.exe [illegible] Kali [illegible] sethc.exe [illegible] Shift [illegible].

[illegible]

[illegible] 24 [illegible] 32 [illegible].

[illegible] C [illegible] C [illegible]:

```
#include <stdio.h>

int main( void )

{

printf("%s", "Hello, World!");

return 0;

}
```

[illegible] Hello World [illegible]:

Strcpy: [illegible] src [illegible] dest [illegible].

Strncpy: [illegible] N [illegible] dest [illegible].

Gets: [illegible] stdin [illegible].

Strcat: [illegible] src [illegible] dest [illegible].

Memmove: [illegible].

Scanf: [illegible] (stdin) [illegible].

Memcpy: num [illegible] src [illegible].

[illegible] C [illegible]. .

[illegible]

از این مشکل پیرامون نسخههای خاصی از سیستمعاملها یا برنامههای کاربردی است .

یک مثال خوب در این زمینه اکسپلیوت Aurora است که برای دستیابی به سیستمهای آسیبپذیر ویندوزی که اینترنت اکسپلورر 6 را اجرا میکنند استفاده شد . این سوء استفاده باعث خرابی حافظه در مرورگر اینترنت اکسپلورر میشد . این نقص یکی از عوامل پیادهسازی حملات Operation Aurora بود که مرورگر کروم و سایر مرورگرها را هدف قرار میداد . این حمله با انتشار حجم زیادی از دادهها روی حافظه heap انجام میشد . در این حالت حجم زیادی از دادهها توسط shellcode در heap تزریق میشد. هدف از قرار دادن تمام این دادهها روی heap پیادهسازی یک شرایط ایدهآل در حافظه بود تا shellcode اجرا شوند . جاوا نمونه دیگری است که در برخی موارد رد برابر حملات اکسپلیوت آسیبپذیر است . یک نمونه در این زمینه حملات watering-hole بود که در سال 2013 میلادی رخ داد . سرریز بافر مبتنی بر پشته در زیرساختهای Java Stored Procedure این امکان را به کاربران میداد تا کدهای دلخواه را با اتکا بر مجوزهای EXETURE و CONNECT اجرا کنند .

نکته : برای محافظت در برابر چنین حملاتی بهتر است سیستمها و برنامههای کاربردی را بهروز نگه داشته و وصلههای ارائه شده برای برنامهها و سیستمعاملها را نصب کنید .

جعبه اختصاصی

یکی از اولین فعالیتهایی که یك مهاجم در نظر دارد روی سیستم کاربر اعمال کند بهدست آوردن سطح دسترسی بالا است. یکی از راههای انجام اینکار حمله به سایر حسابهای کاربری است . دسترسی به SAM به مهاجمان امکان دسترسی به همه رمزهای عبور را میدهد . SAM شامل گذرواژههای حساب کاربری است که در فرم هش ذخیره شدهاند. SYSKEY لایه دوم رمزگذاری 128 بیتی را اضافه میکند . پس از فعال شدن این کلید هر بار که سیستم راهاندازی میشود توسط آن استفاده میشود تا دادههای رمز عبور برای انجام فعالیتها احراز هویت در دسترس قرار گیرند .

مهاجمان میتوانند SAM را از طریق دسترسی فیزیکی یا منطقی به سرقت برسانند . در صورت دسترسی فیزیکی ، SAM را میتوان از NT ERD سرنام Emergency Repair Disk در مسیر C: \ winnt \ Repair \ sam بهدست آورد. نگارشهای جدیدتر ویندوز یک نسخه پشتیبان را در مسیر C: \ winnt \ Repair \ regback \ sam قرار میدهند، البته در این SYSKEY مانع از آن میشود تا اطلاعات به راحتی شکسته شوند . اگر دسترسی فیزیکی به سامانهای دارید، میتوانید به سادگی از ابزارهایی مانند LINNT و NTFSDOS استفاده کنید تا دسترسی در اختیارتان قرار گیرد . NTFSDOS میتواند هر پارتیشن NTFS را به عنوان یک درایو منطقی در دسترس قرار دهد. NTFSDOS یک درایور سیستم فایلی شبکه فقط خواندنی برای DOS / Windows است. اگر روی درایو سیدی یا حافظه فلش قرار گیرد به یک ابزار دستیابی قدرتمند تبدیل میشود. روش دیگر دسترسی به شیوه منطقی است. بانک اطلاعاتی ویندوز SAM یک فرمت باینری است، بنابراین بررسی مستقیم کار سادهای نیست . به همین دلیل هکرها از ابزارهایی مانند PWdump و LCP برای استخراج و شکستن SAM استفاده میکنند . قبل از بررسی این برنامهها ، اجازه دهید به بررسی این موضوع بپردازیم که ویندوز چگونه گذرواژهها را رمزگذاری کرده و کاربران را تأیید میکند .

انواع تأیید اعتبار در سیستمعامل ویندوز

ویندوز از بیشتر پروتکلهای تأیید هویت پشتیبانی میکند از جمله این پروتکلها میتوان به احراز هویت شبکه، تأیید شمارهگیری و تأیید اعتبار اینترنت استفاده میکند . برای تأیید اعتبار شبکه و کاربران محلی ویندوز از Windows NT Challenge / Response پشتیبانی میکند که بهنام NTLM معروف است. الگوریتمهای تأیید اعتبار ویندوز با گذشت زمان بهبود یافتهاند . احراز هویت اصلی LAN Manager (LM) توسط NTLMv2 جایگزین شده است. پروتکلهای تأیید اعتبار ویندوز شامل موارد زیر است :

- LM authentication: توسط Me / 95/98 استفاده میشود و مبتنی بر DES است.

- NTLM authentication: توسط NT سرویس پک 3 استفاده میشد و مبتنی بر DES و MD4 است.

- NTLM v2 authentication: توسط post-NT Service سرویس پک 3 استفاده میشد و مبتنی بر MD4 و MD5 است

■ Kerberos: ابتدا در ویندوز 2000 پیادهسازی شد و در ادامه توسط سایر سیستمعاملهای ویندوز همچون سرور 2012 و ویندوز 10 به کار گرفته شد. به دلیل سازگاری با نسلهای قبل، LM ممکن است هنوز هم در برخی شرایط استفاده شود. گذرواژههای رمزگذاری شده با LM به راحتی قابل رمزگشایی هستند، زیرا کلمات عبور در حالت بزرگ قرار دارند و در مجموع متشکل از 14 کاراکتر هستند که به دو قسمت 7 کاراکتری تقسیم میشوند. فرض کنید الگوریتم LM گذرواژهای را به Dilbert!: رمزگذاری شده است.

1. زمانیکه این گذرواژه با الگوریتم LM رمزگذاری میشود، تمامی حروف این گذرواژه به DILBERT! بزرگ میشوند.

2. سپس رمز عبور با کاراکترهای خالی پر شده است تا طول آن 14 نویسه شود: DILBERT!_ _ _ _ _ _

3. قبل از رمزگذاری این گذرواژه، رشته 14 کاراکتری به دو قطعه 7 کاراکتری تقسیم میشود : DILBERT و! _ _ _ _ _ _ _

4- هر رشته بهصورت جداگانه رمزگذاری میشود و نتایج با هم جمع میشوند.

با آگاهی از نحوه ایجاد رمزهای عبور LM کافی است دو موجودیت رمز عبور زیر را از SAM و PWdump7 استخراج کنید.

```
Bart: 1001:

B79135112A43EC2AAD3B431404EE:

DEAC47322ABERTE67D9C08A7958A:

Homer: 1002:

B83A4FB0461F70A3B435B51404EE:

GFAWERTB7FFE33E43A2402D8DA37:
```

دقت کنید که چگونه هر ورودی از دو فیلد کاراکتری جداگانه استخراج شدهاند. همانگونه که مشاهده میکنید، نیمه اول از هر بخش به هشی با مقدار 1404EE خاتمه پیدا کرده است. برنامههای کرک رمز عبور تنها LM بر مبنای همین اطلاعات و آگاهی از طول رمزهای عبور اقدام به شکست گذرواژههای میکنند. در صورت استخراج، یک بخش هفت کاراکتری واژه Dilbert! را در نظر بگیرید را نگه Dilbert کاراکتر میدارد، در حالی که دیگری فقط کاراکتر (!) را نگهداری میکند. کرک کردن 1 کاراکتر یا حتی 7 سادهتر از کرک کردن 14 کارکتر است. خوشبختانه، ویندوز به الگوریتمهای رمز عبور ایمنتری سوییچ کرده است. همانگونه که در ادامه مشاهده میکنید، ویندوز اکنون میتواند از شش سطح تأیید اعتبار استفاده کند. استفاده از رمزهای عبور طولانیتر بیشتر از 14 کاراکتر و الگوریتمهای قوی یکی از بهترین دفاعها در برابر نرمافزارهای قفلشکن گذرواژهها است.

Attribute	LM	NTLM	NTLMv2
Password	Yes	No	No
Hash	DES	MD4	MD5
Algorithm	DES	DES	HMAC

نکته : تأیید هویت Kerberos کار خود را با سیستمعامل ویندوز 2000 آغاز کرد و به عنوان مکانیزم تایید اعتبار پیشفرض برای تمامی سیستمعاملهای ویندوز شناخته میشود. کربروس یک شکل قوی از احراز هویت به شمار میرود.

در شماره آینده مبحث فوق را ادامه میدهیم.

برای مطالعه رایگان تمام بخشهای دوره **CEH** روی لینک زیر کلیک کنید :

آموزش رایگان دوره CEH

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
14:35 - 22/02/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش رایگان CEH10 - طبقهبندی مخاطرات امنیتی - هک اخلاقی - حمیدرضا تائبی - ترفیع امتیاز - Privilege Escalation

---

نشانی
:□□□□https://www.shabakeh-mag.com/security/16849/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-c
eh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-
%D8%B3%D9%81%DB%8C%D8%AF-
%DA%AF%D8%B0%D8%B1%D9%88%D8%A7%DA%98%D9%87%E2%80%8C%D9%87%D8%A7-
%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%B4%DA%A9%D8%B3%D8%AA%D9%87-
%D9%85%DB%8C%E2%80%8C%D8%B4%D9%88%D9%86%D8%AF%D8%9F