20 – [illegible] CEH [illegible]

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

[illegible] keylogger [illegible]. [illegible] keylogger [illegible] [illegible].

[illegible] CEH [illegible].

NTP [illegible]

[illegible] Network Time Protocol [illegible] (NTP) [illegible] Kerberos [illegible]. [illegible] NTP [illegible] UDP 123 [illegible]. [illegible]:

■ Ntpdate: [illegible].

■ Ntptrace: [illegible].

■ Ntpdc: [illegible]

■ Ntpq: [illegible]

[illegible] NTP [illegible]:

■ PresebTense Time Server

■ NTP Server Scanner

■ LAN Time Analyzer

SMTP [illegible]

[illegible] Simple Mail Transfer Protocol [illegible] (SMTP) [illegible] SMTP. [illegible] TCP 25 [illegible] SMTP. [illegible] SMTP [illegible] RCPT [illegible] EXPN [illegible] VRFY [illegible]. Netcat [illegible] SMTP [illegible]:

Nc IP Address 25

[illegible] SMTP [illegible]:

■ NetScanTools Pro

■ Nmap

■ Telnet

DNS [illegible]

[illegible] DNS [illegible] (DNS) [illegible]. DNS [illegible] IP [illegible] DNS [illegible] DNS [illegible] Nslookup [illegible] DNS.

[illegible]

شیرجه در سطل زباله (Dumpster diving): یک تکنیک عملی برای پیدا کردن اطلاعاتی که اجازه میدهند در یک حمله استفاده شود شیرجه در سطل زباله است. کدهای دستیابی، یادداشتها، رمزهای عبور و حتا اطلاعات حساب ممکن است پیدا شوند.

مهندسی اجتماعی: ما در آینده زمان بیشتری را صرف مهندسی اجتماعی خواهیم کرد، اما در حال حاضر آنچه مهم است بدانیم این است که مهندسی اجتماعی فریب مردن و متقاعد کردن آنها به انجام کارهایی است که باعث فاش شدن اطلاعات میشود.

حملات تکنیکی مربوط به گذرواژهها

حملات فنی رمز عبور به ابزارهای خاصی نیاز دارند . این حملات همچنین بر اساس اطلاعاتی که در مراحل قبلی به دست آمدهاند پیادهسازی میشوند . ابزارهای مورد استفاده در هنگام شمارش، شبیه به Hyena ، مانیتور عملکرد شبکه و Nbtstat ممکن است سرنخهای ارزشمندی در مورد حسابهای خاص ارائه کنند . در حال حاضر، شما ممکن است نام حساب را بدانید، درباره مدیر حساب شناخته اولیه بهدست آورده باشید، اطلاعاتی درباره خطمشیهای امنیتی بهدست آورده باشید یا حتا درباره نامهایی که به شکل باز بهاشتراک قرار گرفتهاند اطلاعات اولیه را بهدست آورده باشید . از مهمترین تکنیکهای حمله فنی رمز عبور به موارد زیر میتوان اشاره کرد :

- حدس زدن رمز عبور

حدس زدن خودکار رمز عبور

- شنود رمز عبور

- نصب کیلاگرها روی سامانه قربانی

امروزه هکرها برای موفقیت در انجام فعالیتهای خود هر دو رویکرد حملات فنی و غیر فنی را به یک شکل به کار میگیرند .

حدس زدن گذرواژه

حدس زدن نام کاربری و گذرواژهها مستلزم مرور نتایج است . به یاد داشته باشید که مستندات خوب همیشه در طول تست نفوذ به کار میآیند . بنابراین مطمئن شوید که تمام فعالیتهای قبلی خود را ثبت کردهاید . رمز عبورهای عبور به این دلیل شکسته میشوند که افراد دوست دارند از کلمات یا عبارات ساده استفاده کنند . یک کارشناس تست نفوذ یا نفوذگر سعی میکند بر مبنای سرنخهای ظریفی که در طول مراحل شمارش بهدست آورده، کلمات یا عباراتی که صاحب حساب از آنها استفاده کرده را آزمایش کند . همچنین یکسری منابع آنلاین نیز وجود دارند که دسترسی به گذرواژههای نقض شده را فراهم میکنند . Recon-ng یک ابزار شناسایی کامل است که دارای یک جستوجوی pwned است. همچنین سایتها با بانکهای اطلاعاتی قابل جستجو برای حسابهای تحت نفوذ قرار گرفته Have I Been Pwned به نشانی https://haveibeenpwned.com/ وجود دارند . شکل زیر رابط کاربری این سایت را نشان میدهد :

net use * \\IP_address\share * /u:name

C:\ >net use * \\192.188.13.10\c$ * /u:jack

Type the password for \\172.20.10.79\c$:

The command completed successfully

■ FAR و FRR: هي النسبة المئوية لعدد المرات التي يتم فيها قبول مستخدم غير مصرح له (FAR) ورفض مستخدم مصرح له (FRR). على سبيل المثال، إذا كان FAR يساوي 1%، فهذا يعني أنه من بين كل 100 محاولة وصول غير مصرح بها، سيتم قبول واحدة منها. أما FRR، فإذا كان يساوي 5%، فهذا يعني أنه من بين كل 100 محاولة وصول مصرح بها، سيتم رفض 5 منها.

■ CER: هي النقطة التي تتساوى عندها قيمة FAR مع قيمة FRR، وتسمى أيضًا بمعدل تساوي الخطأ (CER). كلما كانت قيمة CER أقل، كان النظام أكثر دقة. على سبيل المثال، إذا كان FAR يساوي 2% وFRR يساوي 2%، فإن CER يساوي 2%. وإذا كان FAR يساوي 1% وFRR يساوي 3%، فإن CER يساوي 2% أيضًا.

■ Strength: هي قوة الخوارزمية المستخدمة في النظام، وكلما كانت الخوارزمية أقوى، كان النظام أكثر دقة. على سبيل المثال، إذا كان النظام يستخدم خوارزمية ضعيفة، فقد يتم قبول مستخدم غير مصرح له بسهولة.

■ Acceptance: هي مدى قبول المستخدمين لاستخدام النظام، وكلما كان النظام سهل الاستخدام وغير مزعج، كلما زاد قبول المستخدمين له.

كيف يمكن اختراق هذه الطريقة

هناك عدة طرق لاختراق هذه الطريقة، ولكن أسهلها هو استخدام أداة net use في نظام التشغيل Windows. يمكن استخدام هذه الأداة لمحاولة الاتصال بالنظام المستهدف باستخدام قائمة من أسماء المستخدمين وكلمات المرور. على سبيل المثال، يمكن استخدام الأمر التالي:

1. في هذا المثال، credentials.txt هو ملف يحتوي على قائمة بأسماء المستخدمين وكلمات المرور.

2. يمكن استخدام أداة FOR في Windows لتكرار الأمر net use لكل سطر في الملف credentials.txt:

C:\ > FOR /F "token=1, 2*" %i in (credentials.txt) do net use \\

target\IPC$ %i /u:%j

في هذا المثال، target هو اسم النظام المستهدف، و%i و%j هما متغيران يمثلان اسم المستخدم وكلمة المرور على التوالي. يمكن أيضًا استخدام أدوات مثل THC Hydra أو Brutus لتنفيذ هجمات القوة الغاشمة.

هناك عدة طرق لمنع هجمات القوة الغاشمة، مثل استخدام كلمات مرور قوية، وتعطيل حساب المستخدم بعد عدد معين من المحاولات الفاشلة، واستخدام نظام كشف التسلل. ومع ذلك، لا توجد طريقة مضمونة 100% لمنع هذه الهجمات، ولكن يمكن أن تجعل من الصعب على المهاجم اختراق النظام. على سبيل المثال، يمكن أن يؤدي تعطيل حساب المستخدم بعد عدد معين من المحاولات الفاشلة إلى منع المهاجم من تجربة المزيد من كلمات المرور، ولكنه يمكن أن يؤدي أيضًا إلى هجوم حجب الخدمة (DoS).

كيف يعمل النظام

يعتمد النظام على مبدأ أن كل مستخدم لديه مجموعة فريدة من الخصائص البيولوجية، مثل بصمة الإصبع أو بصمة الوجه أو بصمة الصوت. يتم تخزين هذه الخصائص في قاعدة بيانات، ويتم مقارنتها بالخصائص التي يقدمها المستخدم عند محاولة الوصول إلى النظام. إذا تطابقت الخصائص، يتم منح المستخدم حق الوصول. وإذا لم تتطابق، يتم رفض الوصول.

يتم تخزين كلمات المرور في نظام التشغيل Windows في ملف يسمى SAM. يحتوي هذا الملف على تجزئة لكل كلمة مرور، وليس على كلمة المرور نفسها. عندما يقوم المستخدم بإدخال كلمة المرور، يتم تجزئتها ومقارنتها بالتجزئة المخزنة في ملف SAM. إذا تطابقت التجزئتان، يتم منح المستخدم حق الوصول. ومع ذلك، يمكن للمهاجم استخدام أدوات مثل Mimikatz لاستخراج تجزئات LM و/أو NTLM من ذاكرة LSASS. بمجرد حصول المهاجم على تجزئة hash، يمكنه استخدامها لمحاولة الوصول إلى النظام دون الحاجة إلى معرفة كلمة المرور الأصلية. هذه الطريقة تسمى هجوم Pass-the-Hash. لمنع هذا النوع من الهجمات، يجب تعطيل LM و NTLM واستخدام بروتوكول Kerberos بدلاً منهما. يمكن أيضًا استخدام أدوات مثل Credential Guard لحماية LSASS من الوصول غير المصرح به.

حالت مهاجمان به جای تلاش برای شکستن هش، به سادگی میتوانند آنها را مجدداً مورد استفاده قرار دهند تا دسترسی غیرمجاز بهدست آورند . ابزار فوق از این آدرس https://github.com/gentilkiwi/mimikatz در دسترس است.

نکته : در ویندوز 8 و ویندوز 10 گذرواژهها به شکل متن ساده در LSASS ذخیره نمیشوند . به همین دلیل حملات هش با موفقیت کمتری اجرا میشوند.

علاوه بر ابزارهای ضبط احراز هویت ویندوز ابزارهای دیگری نیز برای شکستن احراز هویت مربوط به Kerberos وجود دارد . پروتکل Kerberos به منظور فراهم آوردن زیرساختی مطمئن برای احراز هویت متقابل بین کلاینت و سرور تهیه شده است . پروتکل فوق سازمانها را قادر میسازد تا رویکرد (SSO) را پیادهسازی کنند . اگر سازمانی از Kerberos استفاده کندبه احتمال زیاد در مرحله اولیه از پورت 88 که درگاه پیشفرض برای Kerberos است باید کار اسکن را آغاز کنید . KerbCrack ابزاری از NTSecurance.nu است که میتواند برای حمله به Kerberos استفاده شود. این برنامه شامل دو برنامه جداگانه است. بخش اول شنودکننده است که به درگاههای Kerberos در پورت 88 گوش میدهد و بخش دوم به عنوان یک برنامه شکستن است که بر مبنای لغتنامه یا جستوجوی فراگیر گذرواژه را بهدست میآورد .

کیلاگرها

کیلاگرها برنامههای نرمافزاری یا مولفههای سختافزاری هستند که برای ضبط فعالیتهای آنلاین به کار گرفته میشوند . برخی از keylogger سختافزاری از وایفای استفاده میکنند به این معنی که به محض استقرار keylogger مهاجم نیازی به بازیابی دستگاه ندارد و میتواند از طریق ارتباط بیسیم یا بلوتوث با آن ارتباط برقرار کند . در نمونههای نرمافزاری این کیلاگر میان سیستمعامل و صفحهکلید قرار میگیرد . اکثر این برنامههای نرمافزاری ساده هستند، اما برخی از آنها پیچیدهتر هستند و حتی میتوانند کلیدهای وارد شده را به یک آدرس از پیش تنظیم شده ارسال کنند . آنچه در همه آنها مشترک است این است که آنها در حالت خفا کار میکنند و میتوانند تمام متنی را که کاربر وارد میکند ضبط کنند . از نرمافزارهای رایج در این زمینه به موارد زیر میتوان اشاره کرد :

Product	URL
PC Activity Monitor	http://pcactivitymonitor.org
RemoteSpy	http://www.remotespy.com
Veriato Investigator	http://www.veriato.com/products/veriato-investigator
KeyStrokeSpy	http://www.keylogger-software.com

کیلاگر یکی از روشهای بهدست آوردن گذرواژه و نام کاربری است .

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 :
14:20 - 20/02/1399
برچسب:
دوره CEH - آموزش رایگان CEH - آموزش رایگان دوره CEH - هکر کلاه سفید - آموزش CEH v10 - آموزش

□□□□□
https://www.shabakeh-mag.com/security/16843/%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-
%D8%AA%DA%A9%D9%86%DB%8C%DA%A9%E2%80%8C%D9%87%D8%A7%DB%8C-
%D8%B1%D8%A7%DB%8C%D8%AC-%D8%A8%D8%B1%D8%A7%DB%8C-
%D9%86%D9%81%D9%88%D8%B0-%D8%A8%D9%87-
%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7