**تمرین 1 :**

باج افزار WannaCry چیست؟

باج‌افزار WannaCry یک حمله باج‌افزاری بسیار معروف می باشد که در ماه می 2017 به سرعت در شبکه‌های رایانه‌ای در سراسر جهان گسترش یافت. WannaCry نمونه‌ای از باج‌افزار رمزنگاری است، نوعی نرم‌افزار مخرب (بدافزار) که توسط مجرمان سایبری برای اخاذی استفاده می‌شود. باج‌افزار این کار را با [رمزگذاری](https://afratec.ir/whats-data-encryption/) فایل‌های ارزشمند انجام می‌دهد ،یا دسترسی کاربر را از سیستم کاملا قطع می کند. باج افزاری که از رمزگذاری استفاده می کند، باج افزار رمزنگاری یا باج افزار کریپتو نامیده می شود. نوعی از باج افزار که دسترسی کاربر را از کامپیوتر می بندد ، لاکر یا باج افزار قفل کننده نامیده می شود. مانند سایر انواع باج افزارهای رمزنگاری شده، باج افزار WCry داده های کاربر را گروگان می گیرد و قول می دهد در صورت پرداخت باج، آنها را برگرداند. باج افزار WCry کامپیوترهایی را هدف قرار می دهد که از ویندوز مایکروسافت به عنوان یک سیستم عامل استفاده می کنند. داده‌ها را رمزگذاری می‌کند و برای بازگرداندن ارز دیجیتال بیت‌کوین باج می‌خواهد.

مولفه های حمله WannaCry

* **یک اپلیکیشن که داده ها را رمزگذاری و رمزگشایی می کند :**

دراپر اولیه WannaCry حاوی اپلیکیشنی است که مهاجم را قادر می سازد تا داده ها را رمزگذاری و رمزگشایی کند. مؤلفه رمزگذاری به عنوان Wana Decrypt0r 2.0 شناخته می شود و در داخل آن یک فایل ZIP محافظت شده با رمز عبور قرار داشت.

* **فایل های حاوی کلیدهای رمزگذاری :**

در داخل آن فایل ZIP چندین فایل جداگانه حاوی اطلاعات پیکربندی وجود داشت که به هکر کمک کرد تا حمله خود را انجام دهد. همچنین شامل کلیدهای رمزگذاری است که آنها را قادر می سازد قفل داده ها را باز کنند.

* **یک کپی از Tor :**

فایل ZIP همچنین حاوی یک کپی از شبکه Tor بود که یک مرورگر وب منبع باز است که هدف آن محافظت و پنهان کردن داده‌ها، مکان‌ها و فعالیت آنلاین کاربران از طریق مرور ناشناس است.

منشا حمله باج افزار WannaCry

WannaCry که با نام WCry نیز شناخته می‌شود، یک حمله باج‌افزاری بود که برای اولین بار در می 2017 ظاهر شد. این حمله بسیار مؤثر بود زیرا با استفاده از پروتکل Windows Server Message Block (SMB) که به ماشین‌های ویندوز امکان برقراری ارتباط با یکدیگر را می‌دهد، در سراسر دستگاه‌های یک شبکه گسترش یافت.این حمله با استفاده از EternalBlue، یک آسیب‌پذیری روز صفر در دستگاه‌هایی که از نسخه قدیمی SMB استفاده می‌کنند، پخش شد.واناکرای اولین بار توسط آژانس امنیت ملی ایالات متحده (NSA) کشف شد .گروهی از هکرها به عنوان ShadowBrokers ، باج‌افزار واناکرای را منتشر کرده و قدرت تخریب نهفته در WannaCry نخستین بار توسط NSA (آژانس امنیت ملی آمریکا) شناسایی شد. شرکت‌های بزرگ نرم‌افزاری تولیدکننده سیستم‌عامل مانند مایکروسافت،‌ گوگل و اپل هم بلافاصله دست‌ به‌ کار شده و شروع به رفع معایبی نمودند که می‌توانست توسط WannaCry مورد سوءاستفاده قرار گیرد اما هکرها نیز بیکار ننشستند و نسخه جدیدی از این [بدافزار](https://afratec.ir/what-is-malware/) را تولید کردند تا بتوانند کامپیوتر‌ها و دیوایس‌های بیشتری را مورد حمله قرار دهند.

**حمله WannaCry چگونه کار می کند؟**

حمله WannaCry با آلوده کردن رایانه‌های شخصی و انتشار بین دستگاه‌ها ، به صورت خودکار و بدون نیاز به دخالت کاربر یا مهندسی اجتماعی کار می‌کند. از اکسپلویت EternalBlue برای حمله به هر دستگاهی که در برابر آسیب پذیری پچ نشده است استفاده می کند.حمله باج افزار WannaCry با استفاده از دراپر معروف به DoublePulsar، برای حمله به رایانه آلوده عمل می کند. WannaCry سعی می کند به یک URL که به صورت هاردکدینگ در حمله کدگذاری شده، دسترسی پیدا کند. پس از دسترسی، WannaCry را خاموش می کند که به “سوئیچ کشتن” معروف شد. سپس WannaCry فایل‌های مهم دستگاه را جستجو می‌کند، که معمولاً اسناد Microsoft Office، فایل‌های MPEG Audio Layer 3 (MP3) یا فایل‌های MKVهستند. این فایل ها را رمزگذاری می کند، آنها را در دسترس کاربر قرار نمی دهد و درخواست باج را به کاربر نشان می دهد که برای رمزگشایی فایل ها پرداخت کند. این روش تضمین می کند بدافزار WannaCry به صورت رمزگذاری نشده روی دیسک دستگاه نوشته نمی شود، که آن را از برنامه های [آنتی ویروس](https://afratec.ir/afratec-product/endpoint-security/antivirus/) سنتی پنهان می کند. این حمله علاوه بر رمزگذاری فایل‌های قربانی، اشتراک‌گذاری فایل‌های قابل مشاهده را نیز اسکن می‌کند و سیستم‌های متصل به آن‌ها را آلوده می‌کند، که به آن امکان می‌دهد به سرعت در سراسر شبکه‌ها پخش شود.

**اگر باج WannaCry پرداخت نشود چه اتفاقی می افتد؟**

معمولا مهاجمان WannaCry ، از قربانیان درخواست  پرداخت ۳۰۰ یا ۶۰۰ دلار بیت‌کوین ، می‌کنند که در عرض یک هفته پس از حمله به دستگاهشان بپردازند. با این حال، به قربانیان توصیه شد که باج را تسویه نکنند. در بیشتر موارد، مهاجمان داده‌ها را رمزگشایی نمی‌کردند و گمان می‌رفت که از نظر فنی توانایی انجام این کار را ندارند.

**حمله WannaCry چه تأثیری داشت؟**

WannaCry تأثیر بزرگی بر سازمان‌ها در سراسر جهان داشت و بیش از 230000 رایانه را آلوده کرد و میلیاردها دلار خسارت وارد کرد. این امر به دلیل استفاده گسترده از دستگاه‌های ویندوز منسوخ و بدون پچ، تأثیر مخربی بر سازمان‌های مراقبت‌های بهداشتی، از جمله سرویس بهداشت ملی بریتانیا (NHS) داشت. این حمله منجر به از کار افتادن یا در دسترس نبودن تجهیزات و سیستم‌های حیاتی شد که منجر به بسته شدن اتاق‌های اورژانس و ناکارآمد شدن دستگاه‌های نجات بخش مانند تصویربرداری تشدید مغناطیسی (MRI) شد.WannaCry همچنین تأثیر زیادی بر تولیدکنندگان بزرگی که از نسخه‌های آسیب‌پذیر ویندوز استفاده می‌کردند، داشت. بسیاری از آنها دچار قطعی تولید شدند که بسیار پرهزینه بود.

**چگونه می توان WannaCry را متوقف کرد؟**

WannaCry می‌توانست با دانلود یک پچ مایکروسافت که بیش از دو ماه قبل از شروع حمله منتشر شده بود، متوقف شود. مایکروسافت پچ امنیتی Microsoft Security Bulletin MS17-010 را که در مارس 2017 منتشر شد، به‌عنوان مهم معرفی کرد، اما بسیاری از سیستم‌ها بدون اصلاح باقی ماندند و آنها را برای WannaCry باز گذاشت.یک ویژگی خودکار تعبیه شده در سیستم های ویندوز 10 تضمین می کند که کاربران در برابر WannaCry محافظت می شوند. با این حال، این پچ در ابتدا فقط برای نسخه‌های ویندوز پشتیبانی‌شده در دسترس بود، که شامل میلیون‌ها سیستم ویندوز XP که به اینترنت متصل بودند، نبود. مایکروسافت بعداً یک پچ برای سیستم‌های ویندوز قدیمی‌تر و غیر قابل پشتیبانی منتشر کرد. سیستم‌های پچ نشده که آلوده بودند تنها با بازگشت به یک نسخه پشتیبان امن قابل بازیابی هستند.

**تمرین 2:**

بستن SMB در ویندوز:

SMB v1 :

Run – optionalfeatures.exe ----برداشتن تیک SMB 1.0/CIFS File sharing Support

SMB v2/v3

Detect:

Get-SmbServerConfiguration | Select EnableSMB2Protocol

Disable:

Set-SmbServerConfiguration -EnableSMB2Protocol $false

Enable:

Set-SmbServerConfiguration -EnableSMB2Protocol $true

**تمرین 3:**

حمله Race Condition

Race Condition اتفاق غیره منتظره ایست که وقتی پیش می آید که یک سیستم تلاش می کند دو کار را همزمان انجام دهد، در حالی که ماهیت سیستم ایجاب می کند که کارهای با توالی خاصی پشت سر هم انجام شوند تا آن سیستم به درستی کار کند.

یکی از بزرگترین تهدیدهای بانکداری آنلاین همین آسیب پذیری حاصل از Race Condition است. این آسیب پذیری با یک خطای ساده ی برنامه نویسی رخ می دهد که این خطا بین برنامه نویسان خیلی رایج است و البته هزینه ی سنگینی هم دارد.

هکر ها با استفاده از آسیب پذیری حاصل از Race Condition  می توانند مبلغ بسیار زیادی پول از بانکهای آنلاین، کارگزاری های سهام و صرافی ها بدزدند. حتی این آسیب پذیری باعث شد تا هکری بتواند به صورت نامحدود از استارباکس قهوه بگیرد!

در علوم کامپیوتر، Concurrency یا همان همزمانی قابلیتی است که بخش های مختلف برنامه بتوانند به صورت همزمان اجرا شوند و بدون اینکه تاثیری روی هم داشته باشند نتیجه ی نهایی حاصل شود.

وقتی یک برنامه، با ذهنیت Concurrency توسعه داده می شود، آن برنامه می تواند از مزایای Multithreading (مولتی تردینگ یا چندنخی) و Multiprocessing (مولتی پروسِسینگ یا چند پردازه ای) بهره مند شده و در نتیجه بهره وری عملکرد آن به شدت افزایش پیدا می کند.

Multithreading توانایی ای است که طی آن می توان چندین Thread  (رشته ای از کارها) را در CPU  اجرا کرد. این Thread ها همزمان اجرا نمی شوند بلکه از قدرت محاسباتی CPU  به نوبت استفاده می کنند. با قابلیت Multithreading هر کدام از Thread ها می توانند از منابع محاسباتی CPU، در زمانی که مثلا thread اصلی منتظر است تا برنامه ورودی ای را دریافت کند، استفاده کنند.

Multiprocessing هم به معنی استفاده از چند CPU برای پردازش همزمان است.

سامان دادن به توالی اجرای چندین Thread را Scheduling (اسکژولینگ یا زمانبندی) می گویند. که الگوریتم های زمانبندی متعدد و مختلفی وجود دارد که هر کدام برای شرایط خاصی بهینه سازی شده اند.

در کامپیوتر Race Condition زمانی اتفاق می افتد که دو بخش از کد، که طراحی شده اند تا برای اجرا از توالی خاصی پیروی کنند به صورتی خارج از آن توالی پیش بینی شده اجرا شوند. از آنجایی که الگوریتم زمان بندی در هر زمان ممکن است Thread خاصی را اجرا کند پس شما نمی توانید دنباله ی کارهایی که Thread اجازه پیدا کرده است تا انجامش بدهد را پیش بینی کنید.

**تمرین 5:**

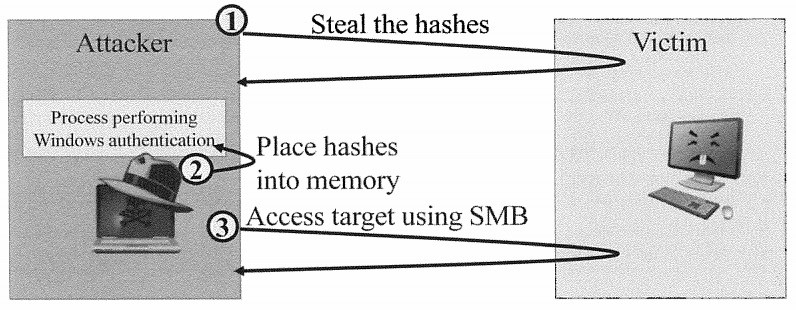
## حمله Pass The Hash

در بخش پیشین در مورد نحوه شکستن کلمات عبور رمز شده توضیحاتی را خدمتتان ارائه نمودیم. در این بخش قصد داریم تا به حمله‌ای بپردازیم که در آن یک نفوذگر با داشتن تنها هش مربوط به کلمات عبور و بدون دانستن کلمه عبور اصلی می‌تواند به یک سیستم نفوذ نماید.

فرض کنید که یک نفوذگر بوسیله ابزارهایی مانند pwdump یا fgdump توانسته است تا هش‌های مربوط به کلمات عبور یک سیستم را استخراج نماید. در این مرحله به جای اقدام برای شکستن هش‌های کلمات عبور و رسیدن به کلمات عبور اصلی، نفوذگر می‌تواند اقدام به انجام حمله Pass the Hash نماید.

ماشین‌های ویندوزی، عملیات احراز هویت تحت شبکه را که معمولا با روش‌های LANMAN Challenge/Response، NTLMv1 یا NTLMv2 صورت می‌گیرد، به وسیله کلمه عبور کاربر انجام نمی‌دهند، به جای آن با استفاده از هش رمز عبور کاربر، احراز هویت را صورت می‌دهند که در پروسس مربوط به احراز هویت در مموری ذخیره می‌شود. این پروسس LSASS می‌باشد که مخفف Local Security Authority Subsystem Service بوده و به طور معمول LSASS در حال اجرا بر روی دستگاه کلاینت است.

بنابراین نفوذگر می‌توان زمان گیر بودن مرحله شکستن کلمه عبور را نادیده گرفته و به وسیله استخراج هش کلمات عبور، قرار دادن آن در مموری و احراز هویت با هش به دست آمده از طریق پروتکل SMB در ویندوز، اقدام به حمله Pass the Hash نموده و به سیستم قربانی بدون شکستن یا کرک کلمه عبور، دسترسی پیدا کند.



تصویر بالا، معماری مربوط به یک حمله Pass the Hash را نشان می‌دهد.

در گام اول نفوذگر به روش‌های مختلفی اقدام به سرقت هش مربوط به کلمات عبور سیستم می‌نماید. این فرآیند می‌تواند به وسیله ابزارهایی مانند pwdump یا متاسپلویت انجام شده باشد.

در گام دوم نفوذگر از یک ابزار مربوط به Pass the Hash برای جایگزین نمودن هش‌های کاربر به مموری سیستم خود استفاده می‌کند و با این کار هش قربانی را در سیستم خود بارگذاری می‌نماید تا در مرحله بعد برای احراز هویت از آن استفاده نماید.

در گام سوم نفوذگر به وسیله یکی از ابزارهای ارتباطی از راه دور که بر اساس SMB کار می‌کنند مانند دستور Net use، می‌تواند به سیستم قربانی متصل شود و با این کار با توجه به اینکه از هش قربانی استفاده می‌شود، کاربر در سیستم قربانی به صورت مجاز تلقی شده و تایید اعتبار می‌گردد.

### ابزارهای مربوط به حمله Pass the Hash

Hernan Ocha یک ابزار به نام WCE را منتشر نموده است که از ویندوز ویستا، 7 و 2008 پشتیبانی می‌کند و نسخه‌های اخیر آن نیز علاوه بر Pass the Hash از تکنیک Pass The Token که مربوط به Kerberos می‌شود، پشتیبانی می‌کنند.

مورد دیگر ابزار psexec در متاسپلویت می‌باشد که با استفاده از آن می‌توان اقدام به انجام حمله Pass the Hash نمود. در این ماژول شما باید مقادیر مربوط به SMBUser که نام کاربری قربانی است و SMBPass که هش کلمه عبور قربانی می‌باشد را وارد نمایید تا با استفاده از این ماژول بتوان حمله Pass the Hash را انجام داد.

ابزار دیگری که امکان استخراج کلمات عبور به صورت Clear text را از LSASS فراهم می‌کند، ابزار Mimikatz می‌باشد که از طریق لینک زیر قابل دسترسی است.

### روش‌های جلوگیری از حملات Pass the Hash

یکی از راه‌های مقابله با حملات Pass the Hash، ایمن سازی کلاینت‌هاست. برای این کار شما می‌بایست بروزرسانی سیستم‌عامل و Hardening آن را با روش‌های مختلف انجام دهید. علاوه بر این استفاده از سوئیت‌های Endpoint Security که شامل آنتی ویروس، فایروال شخصی (personal firewall)، سیستم تشخیص نفوذ مبتنی بر میزبان (host-based IPS) و ضد جاسوس افزار (antispyware) می‌باشد، نیز بسیار مفید خواهد بود.

استفاده از فایروال‌های مبتنی بر کلاینت یا همان Host-base Firewall‌ها هم می‌تواند برای جلوگیری از این حملات مفید باشد. در این فایروال‌ها باید پیکربندی به صورتی باشد که اجازه اتصال به پروتکل SMB تنها از طریق سیستم‌های مدیر صورت بگیرد و نه سیستم‌های دیگر.

استفاده از مدیریت کلمه عبور تصادفی و منحصربه فرد برای هر دستگاه، یکی دیگر از تکنیک‌هایی است که برای مقابله با حملات Pass The Hash می‌توان از آن استفاده نمود.

برای پیاده سازی این تکنیک شما می‌توانید از ابزار (LAPS) Local Administrator Password Solution استفاده نمایید. این ابزار برای شرکت مایکروسافت بوده و به وسیله آن برای هر دستگاه یک کلمه عبور منحصر به فرد ایجاد می‌شود که راه کاری برای مقابله با حملات Pass The Hash می‌باشد.

**نکته:** در حملات Pass The Hash معمولا به یک سیستم دسترسی پیدا نموده و سپس به سیستم‌های دیگر دسترسی پیدا می‌کنند و این امر به دلیل وجود کلمات عبور یکسان استفاده شده برای اغلب سیستم‌ها می‌باشد.

در واقع مدیران شبکه با توجه به اینکه اغلب از یک سیستم‌عامل ایمیج تهیه می‌کنند و همان را در داخل شبکه اصطلاحا Deploy می‌کنند، کلمات عبور این سیستم‌ها یکسان است و نفوذگر با توجه به پیدا کردن هش کلمات عبور یک سیستم، در حقیقت به تمام سیستم‌ها دسترسی دارد. ویژگی LAPS با ایجاد کلمات عبور متفاوت و پیچیده، از این مورد جلوگیری به عمل می‌آورد.

برای شناسایی این حملات باید اتصالات SMB را مانیتور نمود، به این خاطر که حملات Pass The Hash از SMB برای اتصال خود استفاده می‌کنند. البته به صورت واحد این کار با دستور Net sessions امکان پذیر می‌باشد.

در انتها هم برای محافظت از سیستم‌ها، اگر مشکوک به این هستید که احتمالا هش‌ها به خطر افتاده اند، باید رمز‌های عبور سیستم‌ها را به سرعت تغییر دهید.

**تمرین 6:**

### Golden Ticket

در صورتی که یک هکر فایل long-tern key را جهت krbtgt به کار گیرد ، قادر خواهد بود به راحتی log on را به طور کاملاً مشابه ایجاد نماید. محتویات تیکت ممکن است حاوی کلمه کاربری جعلی به انضمام حق عضویت در domain admin باشد. هکرها می توانند اطلاعات را سرقت نمایند و از آنها سوء استفاده کنند. دسترسی ها تا هنگامی که اکانت krbtgt ریست نگردد ، در خطر هستند.

### Silver Ticket

کاربر این امکان را دارد که جهت تمامی سرویس ها در دامین ، تقاضای تیکت کند. زمانی که تیکت سرویس توسط long-tern key که مرتبط با اکانت است رمزی داشته باشد ، مورد سرقت واقع می شود. حملاتی صورت گرفته و اطلاعات ربوده می شوند. حملات صورت گرفته فرصت را برای هکرها پدید می آورند که به ماشین های موردنظر خود دستیابی داشته باشند.

**تمرین 7:** Global catalog

Global Catalog یک مخزن داده توزیع شده قابل جستجو است که اطلاعات تقریبی از کلیه اشیائی که در ساختار Forest وجود دارند را در اختیار دارد و بیشترین کاربرد را برای انجام جستجوها در ساختارهای اکتیودایرکتوری های Multidomain که در آنها جستجوی اشیاء به کندی انجام می شود را دارد .Global Catalog بر روی دامین کنترلرهایی ذخیره می شود که برای سرویس دهی Global Catalog طراحی شده اند و توسط Replication بین Domain Controller ها اطلاعات خود را توزیع می کند . جستجوهایی که به سمت Global Catalog سرورها هدایت می شوند نسبت به سایر جستجوها سریعتر انجام می شوند زیر دیگر نیازی به مراجعه به دامین کنترلر های مختلف را نخواهند داشت .

Global Catalog علاوه بر تنظیمات و کپی schema directory partition هر دامین کنترلر در forest یک نسخه کامل قابل نوشتن از directory partitionرا در خود نگه می دارد . بنابراین یک دامین کنترلر صرفا می تواند اشیائی را مکان یابی کند که در همان دامین قرار دارند . مکان یابی یک شیء در دامین دیگر به دسترسی کاربری و یا نرم افزار کاربردی نیاز دارد که بتواند به شیء مورد نظر دسترسی و آن را مکان یابی کند.

Global Catalog این قابلیت را به شما می دهد که بتوانید بدون نیاز به اینکه اطلاعاتی در خصوص نام سایر دامین ها داشته باشید بتوانید اشیاء را در آنها مکان یابی و جستجو کنید . Global Catalog سرور در حقیقت یک دامین کنترلر در دامین است که علاوه بر اینکه دارای یک نسخه کامل از directory partition است یک نسخه فقط خواندنی و البته سطحی از کلیه directory partition های موجود در forest را در خود نگه می دارد .

این نسخه اضافی که از سایر دامین کنترلرها در Global Catalog سرور قرار می گیرد به این دلیل سطحی و سبک است که تمامی خاصیت های اشیاء در آن وجود ندارند و صرفا برخی از این خواص محدود در آن وجود دارند. با مجتمع کردن و متمرکز سازی خاصیت های ویژه ای از اشیاء که صرفا برای جستجوی آن شی مورد استفاده قرار می گیرند شما می توانید یک پایگاه داده کامل از هر شیء موجود در دامین را در یک Global Catalog سرور داشته باشید .

همانطوری که اشاره کردیم Global Catalog اطلاعات خود را به وسیله Replication بین دامین کنترلرها یکسان سازی و بروز می کند ، به خاطر داشته باشید که بیشترین و مهمترین کاربرد GC انجام جستجوهای بین Forest ای است ، یعنی زمانی GC به کمک شما می آید که شما نیاز به جستجو و یا احراز هویت کاربران در Forest های دیگر داشته باشید . این ساده ترین و خلاصه ای از معرفی Global Catalog است که امیدوارم مورد توجه شما قرار گرفته باشد