Web Application Penetration Testing Techniques

By Ahmed AL Mutairi

Twitter : HackingKnights
Web : www.HackingKnight.com
E-Mail : Info@ihacker.org

Introduction

في هذه الورقه سوف اتطرق الى الخطوات و الادوات المستخدم في عمليات البحث عن الثغرات في تطبيقات الويب وتتنوع الادوات من حيث لغات البرمجه و طبيعه الاستخدام لهذه الادوات وكذلك الثغرات وطرق استغلالها لذلك لابد من معرفه كل مايتعلق بالفحص والتحليل لكي يستطيع المهاجم بوضع استراتيجيه للهجوم او الوصول للهدف

1- Operating system Vulnerabilities
2- SSL CERT Vulnerabilities
3- Web Products Vulnerabilities
4- Web Services Vulnerabilities
5- Social Engineering Techniques
6- Make plan
7- Conclusion

Testing quote

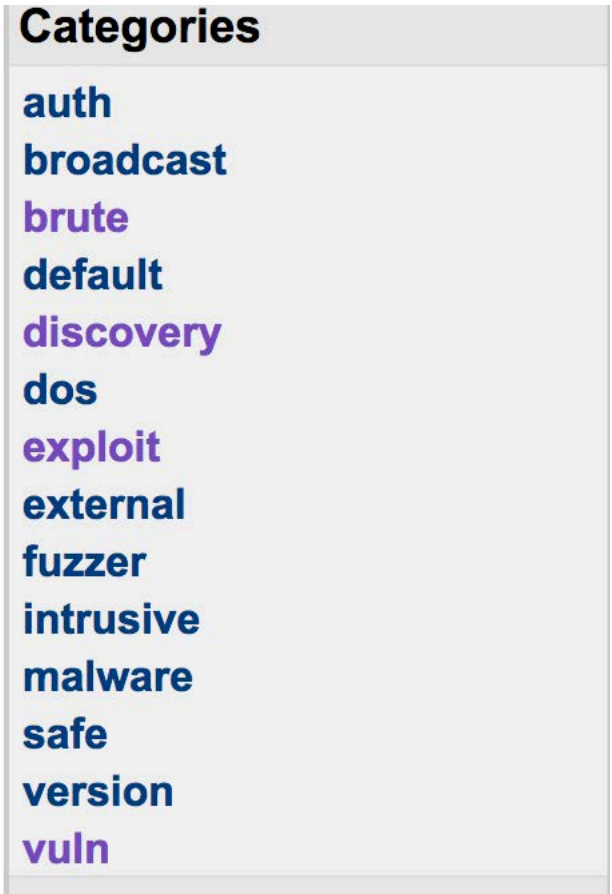
Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

Operating System Vulnerabilities

سوف نبدء في اكتشاف ثغرات الانظمه وافضل مثال لهذا هو الويندوز لذلك سنرى بعض الادوات التي يتم استخدامها لعمل الفحص بالكامل علي الانظمه وكذلك الخدمات ان تم الاستعلام عنها ولكن لكي اقوم بالتفصيل لكل جزء سوف نرى مايمكن ان نصل اليه من خلال هذه الادوات

1- Nmap

في هذه الاداه نستطيع ان نبحث عن ثغرات على الهدف الذي نريده ولذلك سوف نرى بعض الاوامر التي يمكن استغلالها
يوجد في الاداه قائمه بها العديد من الثغرات والهجمات يمكن فحص الانظمه من خلالها في البدء سنرى هذه القوائم واستخدامها



هذي هي القوائم التي يمكننا استخدامها في عمليه فحص الاهداف وكل خيار يوجد به ثغرات عديده او هجمات قد يكون الهدف مصاب بها لمن يريد ان يرى هذه الثغرات سوف اضع الروابط في الخاتمه والان نأتي الي التطبيق استخدام هذه الاوامر يكون كالاتي

nmap --script type ip-Target // type choose anyone of the Categories // ip-Target is our host
For example :
nmap --script default 127.0.0.1 or nmap --script vuln 127.0.0.1

Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

Operating System Vulnerabilities Cont.

والان ننتقل الي الاداه الثاني في فحص الانظمه واكتشاف ثغراتها وهي مشروع يجتمع به جميع الادوات التي يمكن لمختبر الاختراق الاستفاده منها

2- Metasploit

من هذا المشروع لا نريد الا جزء منه وهو المختص بعمليات البحث والاكتشاف

Auxiliary

يوجد في هذا الجزء **951** فحص لثغره والان نآتي لعمليه الاستخدام

msf> show auxiliary
msf> use [the auxiliary]
msf> show options
msf> run

```
msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > show options

Module options (auxiliary/scanner/ssl/openssl_heartbleed):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   DUMPFILTER                   no        Pattern to filter leaked memory before
 storing
   RHOSTS                       yes       The target address range or CIDR ident
ifier
   RPORT       443              yes       The target port
   STARTTLS    None             yes       Protocol to use with STARTTLS, None to
 avoid STARTTLS  (accepted: None, SMTP, IMAP, JABBER, POP3, FTP)
   STOREDUMP   false            yes       Store leaked memory in a file
   THREADS     1                yes       The number of concurrent threads
   TLSVERSION  1.0              yes       TLS/SSL version to use (accepted: SSLv
```

Operating System Vulnerabilities Cont.

3- Windows Exploit Suggester

بهذه الاداه يمكننا ان نبحث عن في قواعد بيانات المايكروسوفت ما اذا كانت مصاب النظام الهدف بثغره ام لا ولا شك بان الثغرات كثيره في الويندوز ويصعب علينا ان نبحث عنها بشكل يدوي لذلك هذه الاداه مهمه جدا وكذلك سهله الاستخدام ننتقل للتطبيق العملي

بهذا الامر نقوم بعمل تحديث للقاعده كي تصلنا الثغرات الحديثه

update the database

```
$ ./windows-exploit-suggester.py --update
[*] initiating...
[*] successfully requested base url
[*] scraped ms download url
[+] writing to file 2014-06-06-mssb.xlsx
[*] done
```

و طريقه البحث عن الثغرات تكون كالتالي
سنقوم بالبحث عن اصدار معين للويندوز ونرى هل توجد له ثغرات والاصدار الذي نريده هو

"windows server 2008 r2"

```
$ ./windows-exploit-suggester.py --database 2014-06-06-mssb.xlsx --ostext 'windows server 2008 r2'
[*] initiating...
[*] database file detected as xls or xlsx based on extension
[*] getting OS information from command line text
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 196 potential bulletins(s)
[*] there are now 196 remaining vulns
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Im
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) -
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (98279
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
```

الجزء الذي تم تظليله هي الثغرات المصابه فيها النظام المستهدف

Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

SSL CERT Vulnerabilities

مع الاحداث الاخير في عالم التقنيه ظهرت الكثير من الثغرات التي تواجدت في اجزاء و خدمات يتم تركيبها في الخوادم والمواقع من باب الامان ولذلك سوف اتطرق الي طرق اكتشاف هذه الثغرات والادات المستخدمه في عمليه التحليل والبحث في هذه البروتوكولات

1- Testssl.sh: Testing TLS/SSL Encryption

في هذه الاداه يتم اختبار التشفير في العده بروتوكولات وكذلك في حال تم وجود ثغره يتم اخبارك عنها وبيانات هذه الثغره ولا تكتفي في برتوكول واحد وانها تعمل بحث في العديد من البروتوكولات لذلك هذه الاداه من الادوات المهمه في عمليه البحث عن هذا النوع من الثغرات

https -ftp -smtp-xmpp-imap

هذه هي بعض البروتوكولات التي يتم فحصها والان سوف نتطرق للجانب العملي لهذه الاداه

./testssl.sh host.com //https

./testssl.sh --starttls smtp <smtphost>.<tld>:587 //SMTP

./testssl.sh --starttls ftp <ftphost>.<tld>:21 //FTP

./testssl.sh -t xmpp <jabberhost>.<tld>:5222 /Jabber

./testssl.sh -t xmpp --xmpphost <XMPP domain> <jabberhost>.<tld>:5222 /Jabber

./testssl.sh --starttls imap <imaphost>.<tld>:143 //IMAP

```
Testing HTTP header response @ "/"

HTTP Status Code             200 OK
HTTP clock skew              +8 sec from localtime
Strict Transport Security    --
Public Key Pinning           --
Server banner                Apache/2.2.22 (Debian)
Application banner           X-Powered-By: PHP/5.5.30-1~dotdeb+7.1
Cookie(s)                    1 issued: NOT secure, NOT HttpOnly
Security headers             X-Frame-Options sameorigin
                             X-UA-Compatible IE=edge
Reverse Proxy banner         --


Testing vulnerabilities

Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224)                       not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
Secure Renegotiation (CVE-2009-3555)      not vulnerable (OK)
Secure Client-Initiated Renegotiation     VULNERABLE (NOT ok), DoS threat
CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
BREACH (CVE-2013-3587)                    potentially NOT ok, uses gzip HTTP compression. - only supplied "/" tested
                                          Can be ignored for static pages or if no secrets in the page
POODLE, SSL (CVE-2014-3566)               VULNERABLE (NOT ok), uses SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported
SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers
FREAK (CVE-2015-0204)                     not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected
BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                          TLS1: AES128-SHA AES256-SHA DES-CBC3-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA
                                          VULNERABLE -- and no higher protocols as mitigation supported
LUCKY13 (CVE-2013-0169)                   VULNERABLE, uses cipher block chaining (CBC) ciphers
RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5
```

ونستطيع ان نرى بعد عمل فحص للهدف اتضح اصابته بعده ثغرات ويتبين لنا نوع الثغره وماذا يمكن ان تعمل بالهدف

Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

Web Products Vulnerabilities

في هذا القسم سو نتطرق الي عده ادوات مما لا شك فيه ان هناك الكثير من التطبيقات المستخدمه في المواقع مثل جوملا والورد بريس والكثير منها ولكن القاسم بين هذه التطبيقات هي طريقه البحث و صطياد هذه النقاط التي قد تكون مخفيه عن بعض المطورين لذلك سوف نتطرق لعده هجمات لكي تكون الصوره واضحه لنا في عمليات وضع الاستراتيجيه ولابد ان تعلم بان مايميز مختبر الاختراق ليس الادوات ولكن طريقه تفكيره ودراسته الجيده للهدف في الاداه الاول التي سوف نستخدمها هي

1-Web Application Vulnerabilities Tools

في هذا القسم سوف نرى بعض الادوات المستخدمه في اكتشاف ثغرات تطبيقات الويب والمساعده في تحليلها

A- WebSploit

في الاداه هذي تتيح لنا عمل الكثير من الخيارات و على عده مستويات من الشبكات الي المواقع والسيرفرات ننتقل الان للجانب العملي وطريقه التعامل مع هذه الاداه

```
root@testing:~# websploit
WARNING: No route found for IPv6 destination :: (no default route?)

db    d8b   db d88888b d8888b. .d8888. d8888b. db       .d88b.  d888888b d888888b
88    I8I   88 88'     88  `8D 88'  YP 88  `8D 88      .8P  Y8.    `88'   `~~88~~'
88    I8I   88 88ooooo 88oooY' `8bo.   88oodD' 88      88    88     88       88
Y8    I8I   88 88~~~~~ 88~~~b.   `Y8b. 88~~~   88      88    88     88       88
`8b d8'8b d8' 88.     88   8D db   8D 88      88booo. `8b  d8'    .88.      88
 `8b8' `8d8'  Y88888P Y8888P' `8888Y' 88      Y88888P  `Y88P'  Y888888P    YP

                --=[WebSploit Advanced MITM Framework
        +---**---==[Version :3.0.0
        +---**---==[Codename :Katana
        +---**---==[Available Modules : 20
                --=[Update Date : [r3.0.0-000 20.9.2014]


wsf >
```

لنري مايتعلق بفحص المواقع

```
wsf > show modules

Web Modules                    Description
-------------------            --------------------
web/apache_users               Scan Directory Of Apache Users
web/dir_scanner                Directory Scanner
web/wmap                       Information Gathering From Victim Web Using (Metasploit Wmap
web/pma                        PHPMyAdmin Login Page Scanner
web/cloudflare_resolver        CloudFlare Resolver
```


Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

والان سوف ننتقل الي طريقه تحضير الجلسه للعمل

```
wsf > use web/dir_scanner
wsf:Dir_Scanner > show options

Options          Value
---------        --------------
TARGET           http://google.com

wsf:Dir_Scanner > set TARGET http://host.com
TARGET =>  host.com
wsf:Dir_Scanner > run
[*] Your Target : host.com
[*]Loading Path List ... Please Wait ...
[index] ... [400 Bad Request]
[images] ... [400 Bad Request]
[download] ... [400 Bad Request]
[2006] ... [400 Bad Request]
```

B- WPForce - Wordpress Attack Suite

مايميز هذه الاداه ليس كميه الخيارات المتاحه من خلالها لكن هذه الاداه ليس بيها الا تقنيتين الاوله الهجوم العنيف بالتخمين والاخرى رفع ملفات خبيثه وكذلك يمكن ان يتم ربطها باكثر من مشروع موجوده في كالي لنكس وهذه الاداه مختصه في الهجوم على تطبيق الورد بريس الشهير

```
python wpforce.py -i usr.txt -w pass.txt -u "http://www.[website].com"

   ,-~~-.___.       __        __ ____   _____
  / |  x     \      \ \      / /|  _ \ |  ___|___   _ __  ___  ___
 (  )         0      \ \ /\ / / | |_) || |_  / _ \ | '__|/ __|/ _ \.
  \_/-, ,----'  ____  \ V  V /  |  __/ |  _|| (_) || |  | (__|  __/
     ====      ||   \_ \_/\_/   |_|    |_|   \___/ |_|   \___|\___|
    /  \-'~;   ||     |
   /  __/~| ...||__/|-"   Brute Force Attack Tool for Wordpress
 =(  _____||________|                  ~n00py~

Username List: usr.txt (3)
Password List: pass.txt (21)
URL: http://www[website].com
```


Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

C- Fimap - LFI/RFI bugs

في هذه الاداه تتيح لنا عمل بحث عن الثغرتين ولكن طبيعه عملها هو المثير للهتمام من خلال هذه الاداه يمكننا ان نبحث عن هذه الثغرات في محركات البحث الشهيره مثل

Google - Bing

وكذلك يمكننا عمل تدقيق لعده اهداف بآمر واحد والان ننتقل الي الجانب العملي

```
## Examples:
  1. Scan a single URL for FI errors:
        ./fimap.py -u 'http://localhost/test.php?file=bang&id=23'
  2. Scan a list of URLS for FI errors:
        ./fimap.py -m -l '/tmp/urllist.txt'
  3. Scan Google search results for FI errors:
        ./fimap.py -g -q 'inurl:include.php'
  4. Harvest all links of a webpage with recurse level of 3 and
     write the URLs to /tmp/urllist
        ./fimap.py -H -u 'http://localhost' -d 3 -w /tmp/urllist
```

في الامر الاول يتم عمل فحص لهدف واحد
في الامر الثاني يتم عمل فحص لعده اهداف
في الامر الثالث يتم عمل فحص على نتائج محرك البحث قوقل
في الامر الرابع يتم عمل فحص لجميع الصفحات علي المستوي الثالث لهدف واحد

2- Grep

هذا الامر هو امر موجود في الانظمه مفتوحه المصدر ولكن يمكن لنا ان نستخدمه في عمليه البحث عن الثغرات بطريقه مبتكره ولكن يجب علينا ان نقوم بتحميل هذا التطبيق قبل عمليه الفحص وسيكون تطبيق الامر علي المجلد الذي يحمل ملفات التطبيق والان نرى الاوامر التي يتم تطبيقها من خلال الترمينال

XSS:

```
grep -Ri "echo" .
```

```
grep -Ri "\$_" . | grep "echo"
```

```
grep -Ri "\$_GET" . | grep "echo"
```

```
grep -Ri "\$_POST" . | grep "echo"
```

```
grep -Ri "\$_REQUEST" . | grep "echo"
```


Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

ثغرات تطبيق الاوامر يتم البحث عنها بالطريقه هذه

Command execution:

```
grep -Ri "shell_exec(" .
```

```
grep -Ri "system(" .
```

```
grep -Ri "exec(" .
```

```
grep -Ri "popen(" .
```

```
grep -Ri "passthru(" .
```

```
grep -Ri "proc_open(" .
```

```
grep -Ri "pcntl_exec(" .
```

وثغرات قواعد البيانات وحقن الاكواد

Code execution:

```
grep -Ri "eval(" .
```

```
grep -Ri "assert(" .
```

```
grep -Ri "preg_replace" . | grep "/e"
```

```
grep -Ri "create_function(" .
```

SQL Injection:

```
grep -Ri "\$sql" .
```

```
grep -Ri "\$sql" . | grep "\$_"
```


Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

3-Grabber

في هذه الاداه يمكننا ان نعمل فحص واطلاق العناكب كذلك لنرى اهم مميزاته

Features:

- Cross-Site Scripting
- SQL Injection (there is also a special Blind SQL Injection module)
- File Inclusion
- Backup files check
- Simple AJAX check (parse every JavaScript and get the URL and try to get the parameters)
- Hybrid analysis/Crystal ball testing for PHP application using PHP-SAT
- JavaScript source code analyzer: Evaluation of the quality/correctness of the JavaScript with JavaScript Lint
- Generation of a file [session_id, time(t)] for next stats analysis.

طريقه الاستخدام كالتالي

```
root@kali:~# grabber --spider 1 --sql --xss --url http://192.168.1.224
Start scanning... http://192.168.1.224
runSpiderScan @  http://192.168.1.224  |   # 1
Start investigation...
Method = GET  http://192.168.1.224
[Cookie]    0   :   <Cookie PHPSESSID=2742cljd8u6aclfktf1sh284u7 for 192.168.1.224/>
[Cookie]    1   :   <Cookie security=high for 192.168.1.224/>
Method = GET  http://192.168.1.224
[Cookie]    0   :   <Cookie PHPSESSID=2742cljd8u6aclfktf1sh284u7 for 192.168.1.224/>
[Cookie]    1   :   <Cookie security=high for 192.168.1.224/>
```


Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

Web Services Vulnerabilities

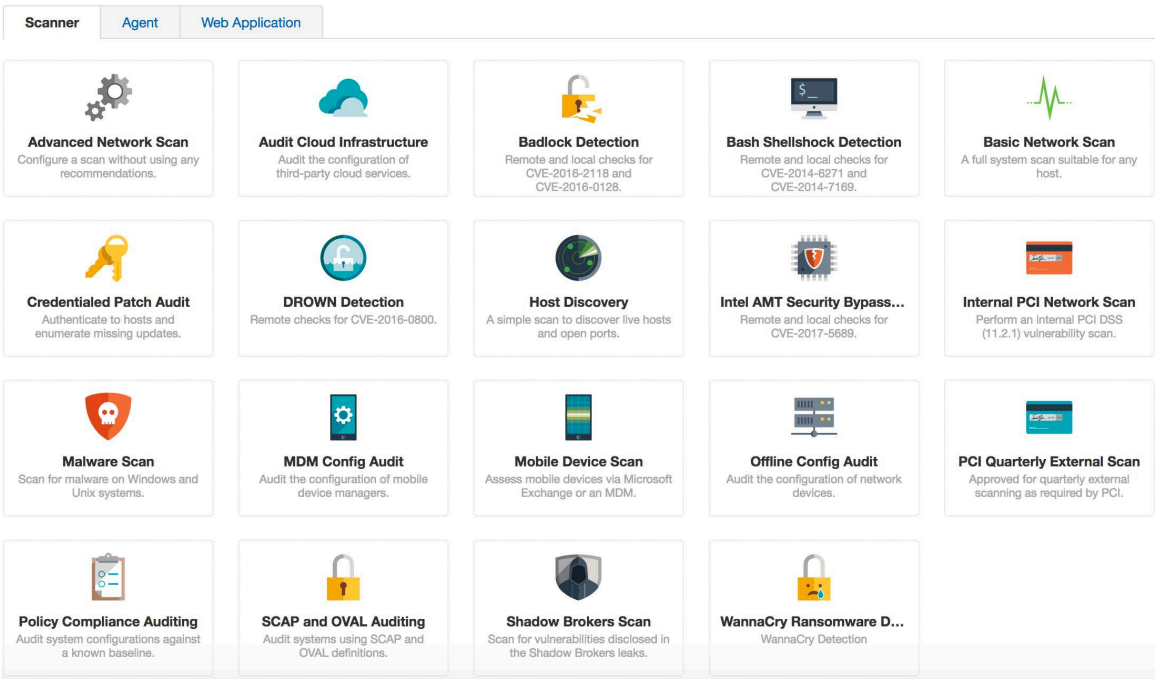
في الغالب يصعب العثور على ثغرات امنيه في الخدمات التي يتم استخدامها على الخوادم وذلك لسرعه التحديث فيها ولكن هناك طرق لاستغلال هذه الخدمات لعمل هجوم عليها وسوف نتطرق لهذه الهجمات في هذا القسم

1-Nessus vulnerability scanner

هذا المشروع لا يكتفي بعمل فحص لجزء معين للهدف ولكن يعمل فحص لجميع الخدمات والانظمه يتيح لك كذلك عمل فحص على نطاقات عديده و يمكنك استخدام العديد من عمليات الفحص المختلفه ومن الجميل ايضا يمكنك استدعاء المشروع هذا داخل الميتاسبلويت عن طريق الامر

```
msf > load nessus
[*] Nessus Bridge for Metasploit 1.1
[+] Type nessus_help for a command listing
[*] Successfully loaded plugin: nessus
```

ولكن مايهمنا هو الخدمه السحابيه التي توفرها الشركه المطوره لهذا الموقع ويستطيع اي شخص ان يستخدمها بشكل مجاني لمده 60 يوم علي الرابط https://www.tenable.com سنرى الخدمات التي يمكن عمل فحص من خلالها



Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

وبعد اختيار نوع الفحص يتم وضع البيانات المطلوبه وسوف نرى بعض النتائج لاهداف تم فحصها

Sev	Name	Family	Count
●	PHP Unsupported Version Detection	CGI abuses	1
●	PHP < 5.2.11 Multiple Vulnerabilities	CGI abuses	1
●	PHP < 5.3.11 Multiple Vulnerabilities	CGI abuses	1
●	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	CGI abuses	1
●	PHP < 5.3.9 Multiple Vulnerabilities	CGI abuses	1
●	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CGI abuses	1
●	CGI Generic XSS (extended patterns)	CGI abuses : XSS	1
●	PHP < 5.2.10 Multiple Vulnerabilities	CGI abuses	1
●	PHP < 5.2.12 Multiple Vulnerabilities	CGI abuses	1
●	PHP < 5.2.9 Multiple Vulnerabilities	CGI abuses	1

ولتفاصيل اكثر نقوم بستعراض الثغره عن طريق الضغط عليها والجميل بهذا المشروع هو يمكن ان يخبرك اذا ما تم وجود استغلال في مشروع الميتاسبلويت ام لا

Vulnerability Information

CPE: cpe:/a:php:php

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: 05/03/12 at 12:00 AM

Vulnerability Pub Date: 05/03/12 at 12:00 AM

2- hydra – Very fast network logon cracker

في هذا الجزء سنتحدث عن هجمات الدخول العنيف او **"Brute Force"**

في خدمات الخوادم يمكننا ان نستغله هذه الهجمه عليها والوصول للهدف باسرع وقت ممكن ولكن يعتمد علي عده امور مثل مثلا فهمك للهدف وطريقه اختياره لكلمات المرور مثلا اذا كان يعتمد علي عمل كلمات مرور مركبه والمقصود بها لنفترض ان فهد موظف بالشركه الهدف سيكون فهد١٢٣٢١

Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

في هذه الحاله يجمع ان نقوم بتكوين ملف لكلمات المرور ونضع بها جميع الاحتمالات ومن اهم الادوات لتكوين كلمات المرور هو

Crunch

وهي اداه سهله الاستخدام وكذلك تتيح لنا عده خيارات في اختيار كلمات المرور وتركيباتها

```
EXAMPLES
       Example 1
       crunch 1 8
       crunch will display a wordlist that starts at a and ends at zzzzzzzz

       Example 2
       crunch 1 6 abcdefg
       crunch will display a wordlist using the character set abcdefg that starts at a and ends at gggggg

       Example 3
       crunch 1 6 abcdefg\
       there is a space at the end of the character string.  In order for crunch to use the space you will need to escape it using the \ character.  In this example you could also put quotes around
       the letters and not need the \, i.e. "abcdefg ".  Crunch will display a wordlist using the character set abcdefg  that starts at a and ends at (6 spaces)

       Example 4
       crunch 1 8 -f charset.lst mixalpha-numeric-all-space -o wordlist.txt
       crunch will use the mixalpha-numeric-all-space character set from charset.lst and will write the wordlist to a file named wordlist.txt.  The file will start with a and end with "       "

       Example 5
       crunch 8 8 -f charset.lst mixalpha-numeric-all-space -o wordlist.txt -t @@dog@@@ -s cbdogaaa
       crunch should generate a 8 character wordlist using the mixalpha-number-all-space character set from charset.lst and will write the wordlist to a file  named  wordlist.txt.  The  file  will
       start at cbdogaaa and end at "  dog   "

       Example 6
       crunch 2 3 -f charset.lst ualpha -s BB
       crunch with start generating a wordlist at BB and end with ZZZ.  This is useful if you have to stop generating a wordlist in the middle.  Just do a tail wordlist.txt and set the -s parameter
       to the next word in the sequence.  Be sure to rename the original wordlist BEFORE you begin as crunch will overwrite the existing wordlist.

       Example 7
       crunch 4 5 -p abc
       The numbers aren't processed but are needed.
       crunch will generate abc, acb, bac, bca, cab, cba.

       Example 8
       crunch 4 5 -p dog cat bird
       The numbers aren't processed but are needed.
       crunch will generate birdcatdog, birddogcat, catbirddog, catdogbird, dogbirdcat, dogcatbird.
```

في الامثله هذه يتم شرح طريقه الاستخدام

اذا بعد عمل ملف كلمات المرور نحدد عمليه الهجوم على الخدمه المراد الوصول اليها مثلا

pop3 - imap -smtp -mysql - ftp -ssh -http

ويكون تطبيق الاوامر كالتالي

```
root@testing:~# hydra
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-SOuvVd46] [service://server[
:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel (per host, default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] mss
ql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres rdp redis rexec rlogin rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
root@testing:~#
```


Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

```
root@kali:~# hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 6 ssh://192.168.1.123
```

مثال للاوامر المستخدمه في الهيدرا للهجوم على

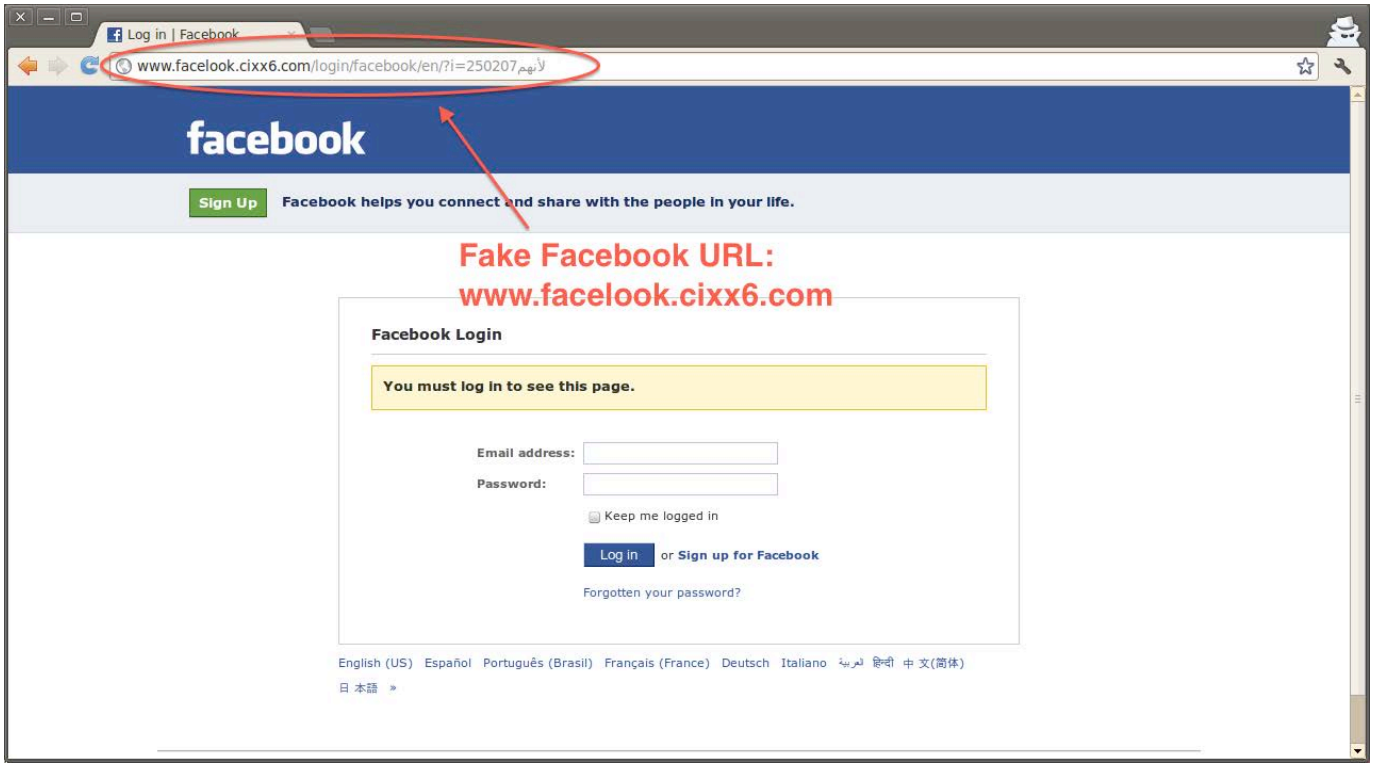
SSh

Social Engineering Techniques

في هذا القسم سوف نتحدث عن اهم التقنيات المستخدمه والتي تعتمد علي التواصل المباشر مع الاشخاص لغايه الاختراق مايميز هذا القسم من الهجمات هو دراستك للشخص المستهدف

1-PHISHING

وهي الهجمات المتعارف عليها مثلا الرسائل التي تصلنا عن طريق الايميلات او مواقع وصفحات مزوره ويكون الهدف منها اما جمع معلومات او زرع برمجيات خبيثه في الجهاز تختلف الاهداف لكن التقنيه هذه هي الاكثر انتشارا ورواج



2- PRETEXTING

في هذه التقنيه مشابهه لتقنيه التصيد ولكن مايميز مستخدميها هو السيناريو او العذر او الحبكه والسبب من ذلك هو اقناع الهدف بظروره ارسال المعلومات او باسرع وقت لكي لا تعطيه وقتا للتفكير

Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

3- Vishing

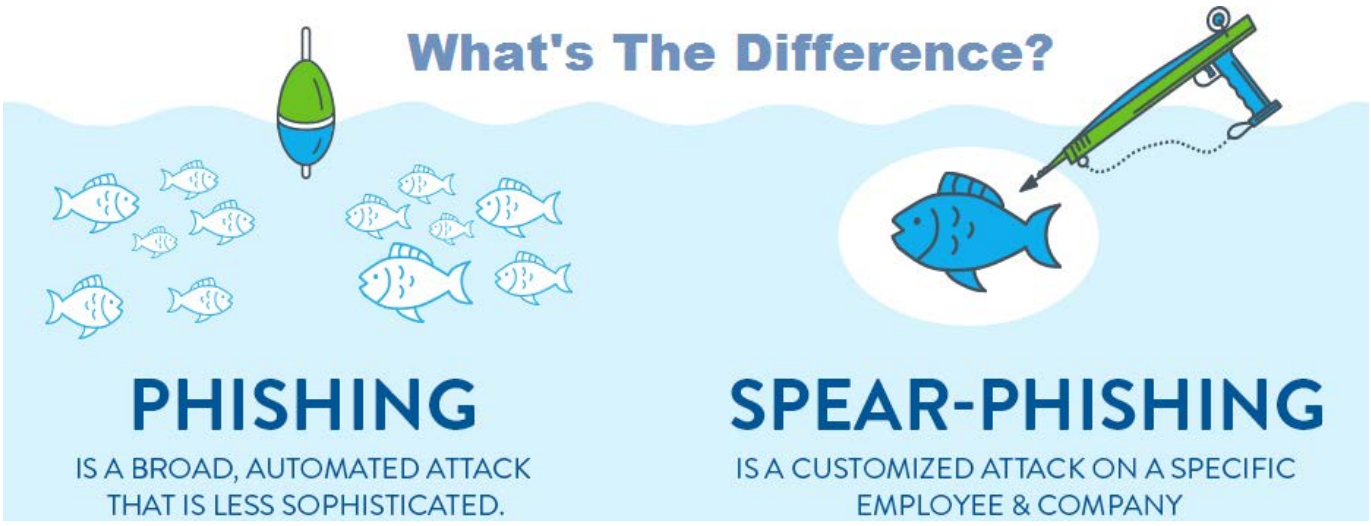
في هذه التقنيه يعتمد المهاجم على الهاتف الخلوي وخدمه الرد الصوتي التفاعلي لكي يستفيد من ثقه الهدف بشركه الاتصالات التي قام بالاشتراك بها بحيث يقوم المهاجم بخداع الهدف عن طريق الاتصال به وجعل الرد الالي يخبره بان المكالمه من شركه الاتصال ويتوجب عليه ادخال معلومات صوتيا او عن طريق لوحه الادخال في الهاتف

4- BAITING

تقنيه الطعم ومايميزها ليس الطلب المباشر ولكن تقديم شي مقابل شي يريده المهاجم بحيث يجعل الهدف يثق بمصداقيه المهاجم مثلا يعطي المهاجم خدمات تم اختراقها مسبقا للضحيه ومقابل خدمه افضل عليه تحميل البرنامج الخاص بشركه (برمجيات خبيثه) ويكون قد وصل للنقطه التي يريدها المهاجم

5- Spear Phishing

لا يميز هذه الهجمه سوا انها عمليه استهداف شخصيا بحيث تكون على درايه تام بالهدف وتملك معلومات عنه مثل الاسم رقم الهاتف مكان الوظيفه بحيث تكون الهجمه اكثر اقناعا ومليئه معلومات يستحيل عملها على مجموعه كبيره من الناس



Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org

Make plan

لقد تطرقت للعديد من التقنيات والادوات التي تم ذكرها في هذا البحث ولكن معرفتها دون وضع خطه يتم التعامل معها بكل دقه لن تصل لكل هدف تريده في كل شركه مختصه بآمن المعلومات يتم وضع خطه زمنيه يتم خلالها عمل جميع عمليات الفحص على الاهداف لكي تكون الخطوات واضحه واساس نجاح كل هجمه يكون بمعرفتك للهدف من موظفين الي الاجهزه وروتين العمل والتعامل مع المستخدمين لكن احيانا تكون بعض الهجمات الهدف منها جمع المعلومات لهدف اكبر من ذلك وفي الصوره القادمه مثال على خطوات عمل مختبر الاختراق

Conclusion

وفي الخاتمه اتنمي ان يكون هذا العمل نال على اعجابكم واني وفقت به وبالتوفيق للجميع

References:

https://github.com/GDSSecurity/Windows-Exploit-Suggester
https://github.com/drwetter/testssl.sh
http://tools.kali.org/web-applications/websploit
https://github.com/n00py/WPForce
http://tools.kali.org/web-applications/fimap
http://tools.kali.org/web-applications/grabber
http://tools.kali.org/password-attacks/crunch
https://github.com/dustyfresh/PHP-vulnerability-audit-cheatsheet
https://www.tenable.com
https://en.wikipedia.org/wiki/Social_engineering_(security)

Ahmed AL Mutairi => @HackingKnights
E-Mail => Info@ihacker.org