H4CK4SHELL

WHOAMI

ARIJIT BHOWMICK

Security Researcher

eJPT

https://medium.com/@sys41x4

https://sys41x4.github.io

https://www.linkedin.com/in/sys41x4

sys41x4

Network Security

Tools and Techniques

CONTENT OVEVIEW

1. WHOAMI

2. Networking Concepts
    - 2.1. Basics of Networking
        - 2.1.1. Network Topologies
        - 2.1.2. OSI Model
    - 2.2. IP Addresses
        - 2.2.1. ipv4 & ipv6
        - 2.2.2. ipv4 basics & tables
        - 2.2.3. ipv6 basics & tables
        - 2.2.4. Differences between ipv4 & ipv6
    - 2.3. MAC Addresses
    - 2.4. TCP/UDP & 3-Way Handshake
    - 2.5. Common Ports & Protocols

3. Programming Languages
    - 3.1. Foundation Development
    - 3.2. Required
    - 3.3. Recommended

4. Security Teaming
    - 4.1. Red Team
    - 4.2. Blue Team
    - 4.3. Differences Between Red Teaming & Blue Teaming

5. Linux Basics
    - 5.1. Basic Commands & Techniques
        - 5.1.1. cd, ls, pwd, mv, cp, rm, mkdir, echo, whoami, man
        - 5.1.2. cat, less, touch, echo, wc, clear
          history (!<line-Number>, !!, !<line-number>:p, !<command-part-string>, history -c)
        - 5.1.3. grep, su, sudo, passwd, chmod
    - 5.2. File System
        - 5.2.1. File System Structure (root-system,child/parent directories)
        - 5.2.2. Credentials & Important Files
        - 5.2.3. host file
    - 5.3. File Streams
        - 5.3.1. STD I/O
        - 5.3.2. STDIN – File Handle=0
        - 5.3.3. STDOUT – File Handle=1
        - 5.3.4. STDERR – File Handle=2

6. How it is done ? [Theory + practical Demonstration]

6.1. Network Security tools

6.1.1. ping/telnet/dig/traceroute/whois/netstat/route/curl/wget

6.1.2. Wireshark (Network Sniffer/Packet Analyser)

6.1.3. Nessus/OpenVAS (Vulnerability Scanner)

6.1.4. BurpSuite/OWASP-ZAP (web Scanner/Request Modifiers)

6.1.5. snort (IPS)

6.1.6. Ettercap (MITM)

6.1.7. Nmap/Angry IP Scanner/Nikto (Service and port Scanner + vulnerability scanner [Signature Based])

6.2. Brute Forcer

6.2.1. hydra (SSH/WEB/FTP/,etc) (CLI)

6.2.2. ffuf/wfuzz/dirb (CLI)

6.2.3. gobuster (CLI)

6.2.4. Dirbuster (GUI)

6.3. Reverse Engineering & Binary Exploitation

6.3.1. GUI Based

6.3.1.1. Ghidra

6.3.1.2. Immunity Debugger

6.3.1.3. WinDbg

6.3.1.4. IDA (paid)

6.3.2. Console Based

6.3.2.1. gdb

6.3.2.2. radare

6.4. Public Exploits finder

- 6.4.1. searchsploit
- 6.4.2. sodan.io

6.5. MAC Modifiers

- 6.5.1. MACchanger
- 6.4.2. TMAC

6.6. Active Directory & Domain Mapping

- 6.5.1. Blood Hound

6.7. Forensics Tools

- 6.7.1. binwalk
- 6.7.2. stegsolve
- 6.7.3. steghide
- 6.7.4. exiftool
- 6.7.5 zsteg
- 6.7.6. Audacity/Sonic Visualizer
- 6.7.7. volatility

7. Important Websites For payloads & privilege escalations

- 7.1. GTFOBins (https://gtfobins.github.io/)
- 7.2. LOLBAS (https://lolbas-project.github.io/)

8. Prevention & Remidition

    8.1. Firewalls
    8.2. IDS/IPS
    8.3. Antivirus

9. Note Taking

    9.1. Obsidian
    9.2. Notion
    9.3. Joplin
    9.4. OneNote
    etc

10. Practice Grounds

    10.1. TryHackMe
    10.2. HackTheBox + HTB Academy
    10.3. Offensive Security Proving Grounds (OSPG)
    10.3. PortSwigger Labs
    10.4. INE Labs
    10.5. CTFLearn
    10.6. overthewire.org
    10.7. pentesterlab
    10.8. AttackDefense
    10.9. hacker101

11. Professional Certifications
    - 11.1. Certifications Over View
    - 11.2. Red Teaming Certifications
    - 11.3. Blue Teaming Certifications

12. Great Content Creators in WILD
    - 12.1. Content Creators in Network Security
    - 12.2. Content Creators in Malware Analysis & CTF Creators
    - 12.3. Content Creators in Web Pentesting
    - 12.4. Content Creators in Buffer Overflows, Binary Analysis & Hardware Security
    - 12.5. Content Creators in 0-Day & Exploit Developers

13. Doubt Session

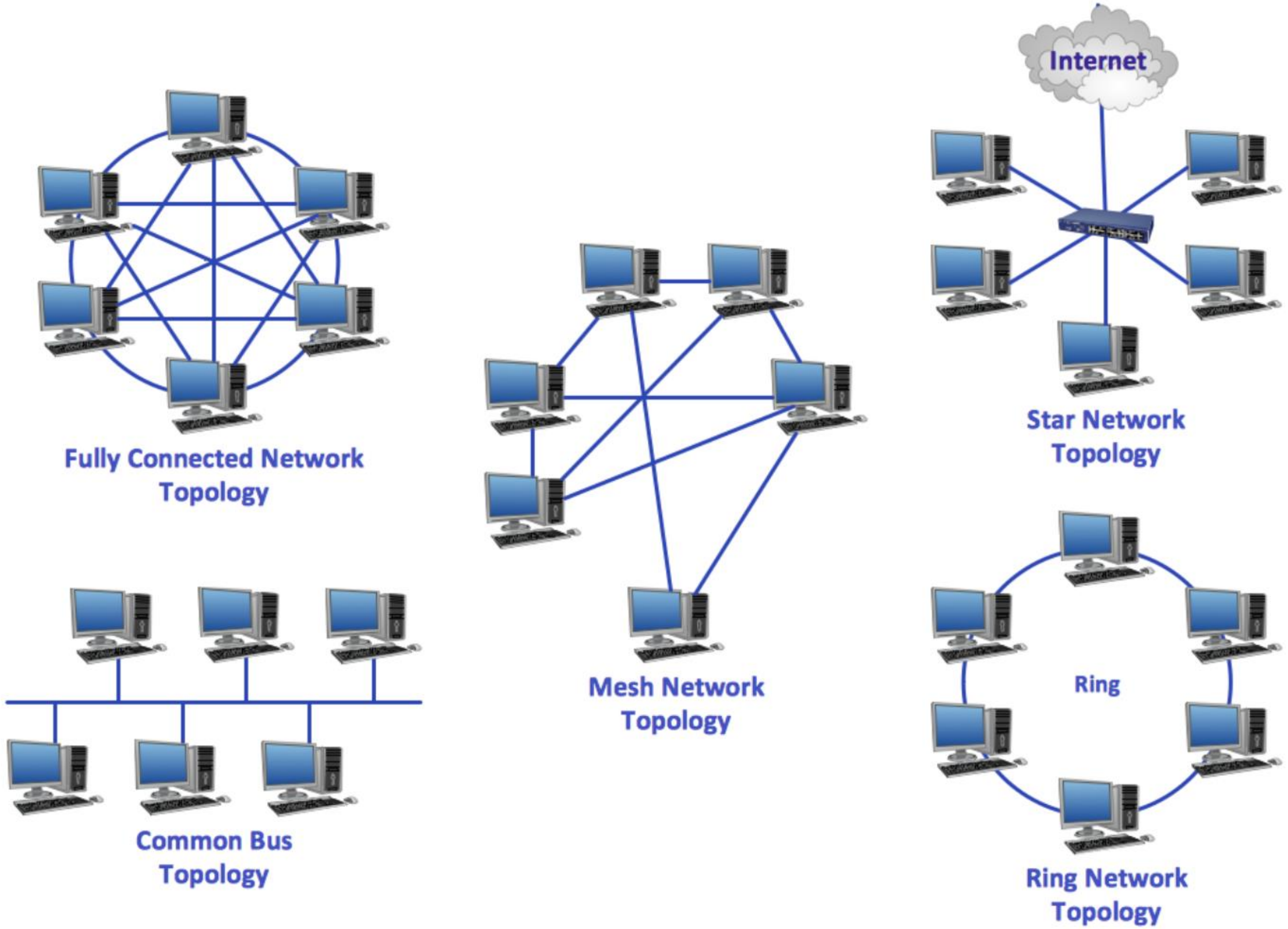
14. Thankyou

Networking Concepts

2.1

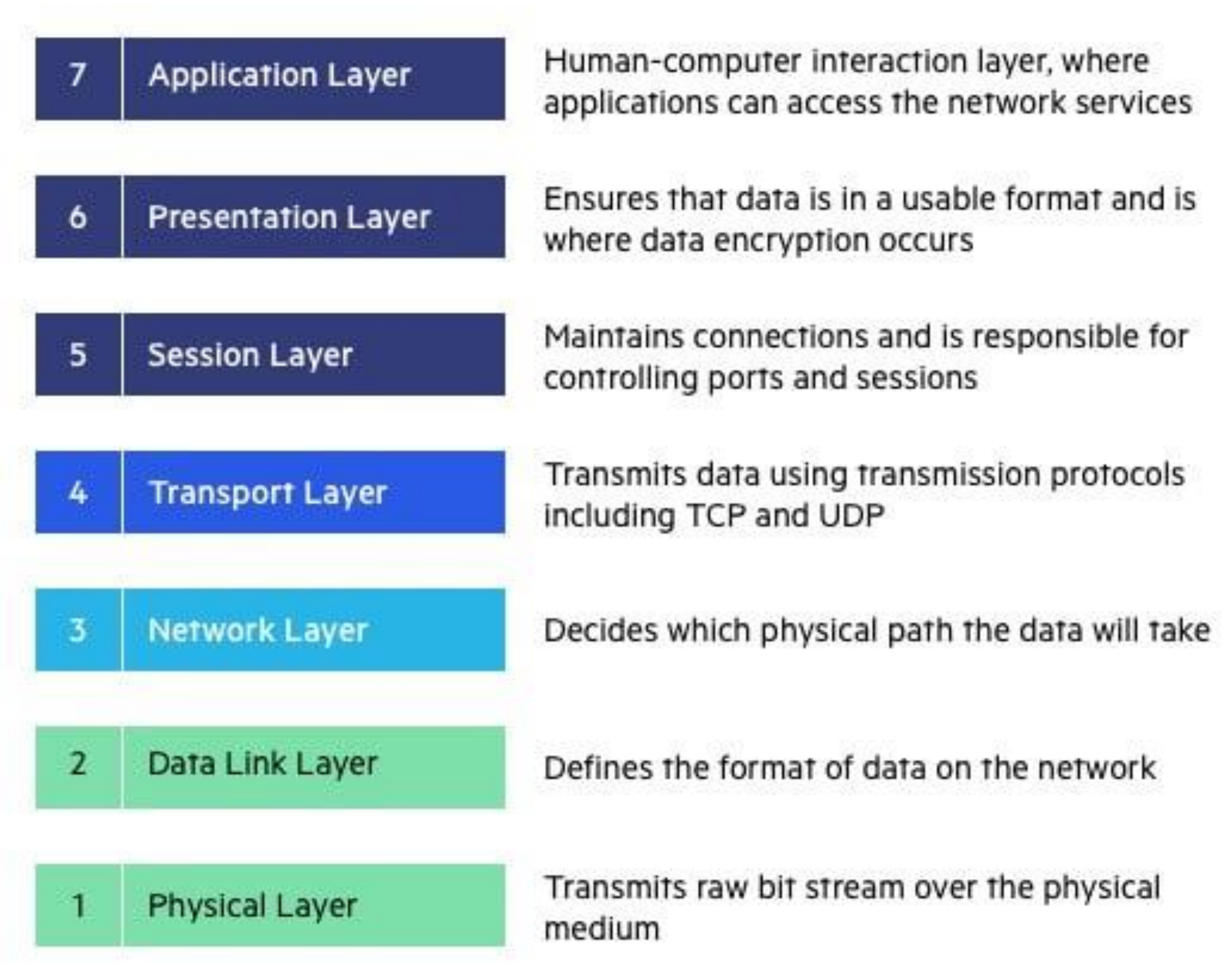
Basics of Networking

Network Topologies



OSI Model

The **OSI Model** (Open Systems Interconnection Model) is **a conceptual framework used to describe the functions of a networking system**. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software.



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

IP Addresses

IPv4 & IPv6

ipv4 → Example **192.168.41.41**

ipv6 → Example **2402:3a80:1132:5533:b111:7114:810:da13**

MAC Addresses

A media access control address (MAC address) is **a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment**. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth.

Example **01-00-5e-7f-ff-fa**

2.4

TCP/UDP & 3-Way handshake

3-Way Handshake → **SYN/SYN-ACK/ACK**

Common Ports & Protocols

HTTP – Port 80

HTTPS – 443

FTP – 21

FTPS / SSH – 22

Telnet - 23

POP3 – 110

POP3 SSL – 995

IMAP – 143

IMAP SSL – 993

SMTP – 25 (Alternate: 26)

SMTP SSL – 587

MySQL – 3306

Programming Languages

Foundation Languages

C

C++

Python

Required

Python

Bash

C/C++

js

Recommended

C/C++

Java

Python

Bash

SQL

Js

,etc

Security Teaming

Red Team

Red Teaming is **the practice of testing the security of your systems by trying to attack/test them**. A Red Team can be an externally contracted group of pen testers or a team within your own organization, but in all cases, their role is the same: to emulate a genuinely malicious actor and try to break into your systems.

Blue Team

A blue team is a **group of individuals who perform an analysis of information systems to ensure security, identify security flaws**, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation.

5

Linux Basics

5.1

Basic Commands & Techniques

5.1.1

cd = Change Directory

ls = list directory

pwd = get location of current directory

mv = move

cp = copy

rm = remove

mkdir = make directory

echo = output provided string (print)

whoami = current user

man = manual

cat = output content of any file

less = get a peak of content of any file

touch = create empty file

wc = word count

clear = clear the current terminal output

history = get history of commands

(!<line-Number>, !!, !<line-number>:p, !<command-part-string>, history -c)

5.1.3

grep = get part of any file/directory mentioned

su = switch user

sudo = run command as root (mandatory to have a
user sudo permissions in that machine)

passwd = change current user password

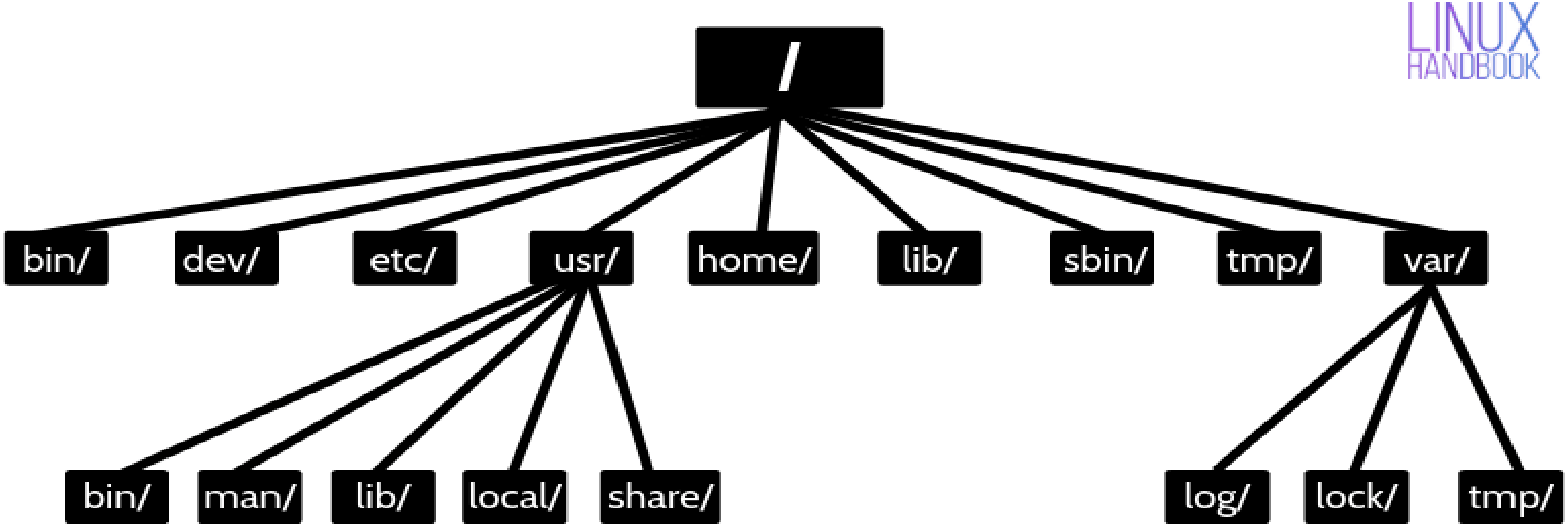
chmod = change file access permission

5.2

File System

5.2.1

/ = Parent/root Directory



LINUX HANDBOOK

Credentials & Important Files

/etc/hosts = hostname files

/etc/passwd = password files

/etc/shadow = password hashes (accessed by sudo users)

/var/www = html files

Cron jobs

5.2.3

/etc/host = host file

It is a very important file and can be some time use by an attacker to redirect traffics to a verified domain to an un verified domain

5.3

File Streams

STD I/O

STDIN => File Handle=0

STDOUT => File Handle=1

STDERR => File Handle=2

2>/dev/null == Error redirected to a null location

How it is done ?

(Theory + Practical)

Network Security Tools

ping/telnet/dig/traceroute/whois/netstat/route/curl/wget
Wireshark (Network Sniffer/Packet Analyser)
Nessus/OpenVAS (Vulnerability Scanner)
BurpSuite/OWASP-ZAP (web Scanner/Request Modifiers)
snort (IPS)
Ettercap (MITM)
Nmap/Angry IP Scanner/Nikto (Service and port Scanner + vulnerability scanner [Signature Based])

Brute Force Tools

hydra (SSH/WEB/FTP/,etc) (CLI)

ffuf/wfuzz/dirb (CLI)

gobuster (CLI)

Dirbuster (GUI)

Reverse Engineering & Binary Exploitation

Ghidra [GUI]

Immunity Debugger [GUI]

WinDbg [GUI]

IDA (paid) [GUI]

gdb [CLI]

radare [CLI]

6.4.x

Public Exploits Finder

searchsploit [CLI]

sodan.io [CLI + Web Client]

6.5.x

MAC Modifiers

macchanger

TMAC

Active Directory & Domain Mapping

Blood Hound [CLI+GUI]

Forensics Tools

binwalk [CLI]

stegsolve [GUI]

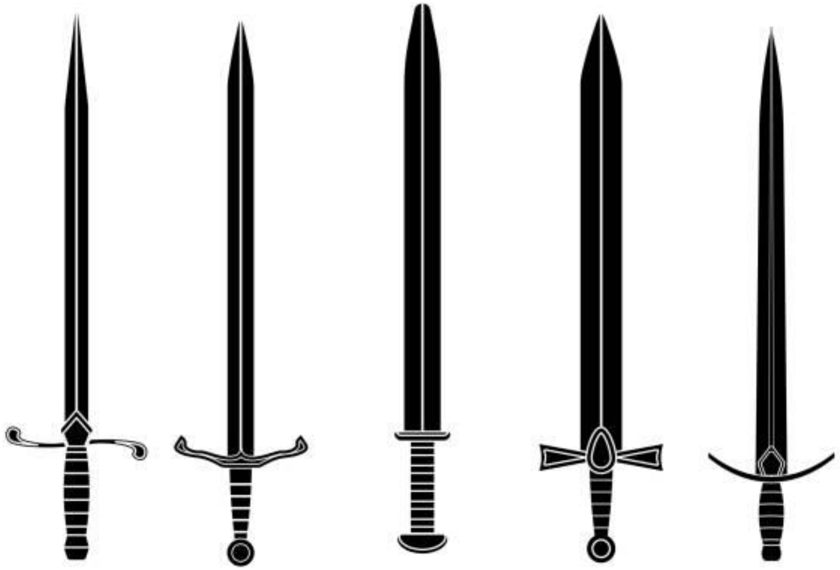
steghide [CLI]

zsteg [CLI]

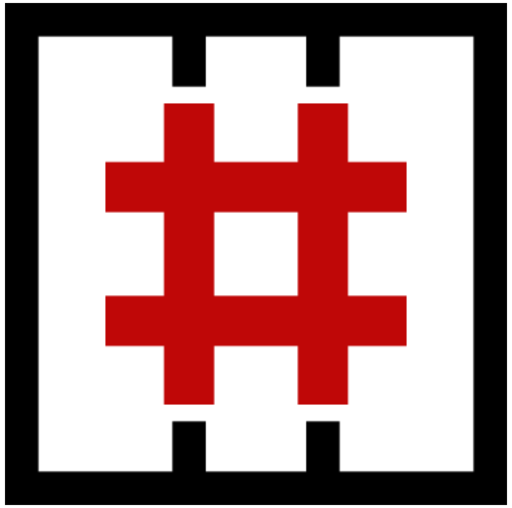
Audacity/Sonic Visualizer [GUI]

Volatility [CLI]

Important Websites for Payloads & Privilege Escalation



7.1



GTFOBins

(https://gtfobins.github.io/)

7.2

LOLBAS

(https://lolbas-project.github.io/)

Prevention & Remidition

8.1

Firewalls

A firewall is **a network security device that monitors incoming and outgoing network traffic** and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for over 25 years. A firewall can be hardware, software, or both.

IDS/IPS

Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. Intrusion Prevention Systems (IPS) also analyzes packets, but can also stop the packet from being delivered based on what kind of attacks it detects — helping stop the attack.

Antivirus

Antivirus is **a kind of software used to prevent, scan, detect and delete viruses from a computer**. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

9

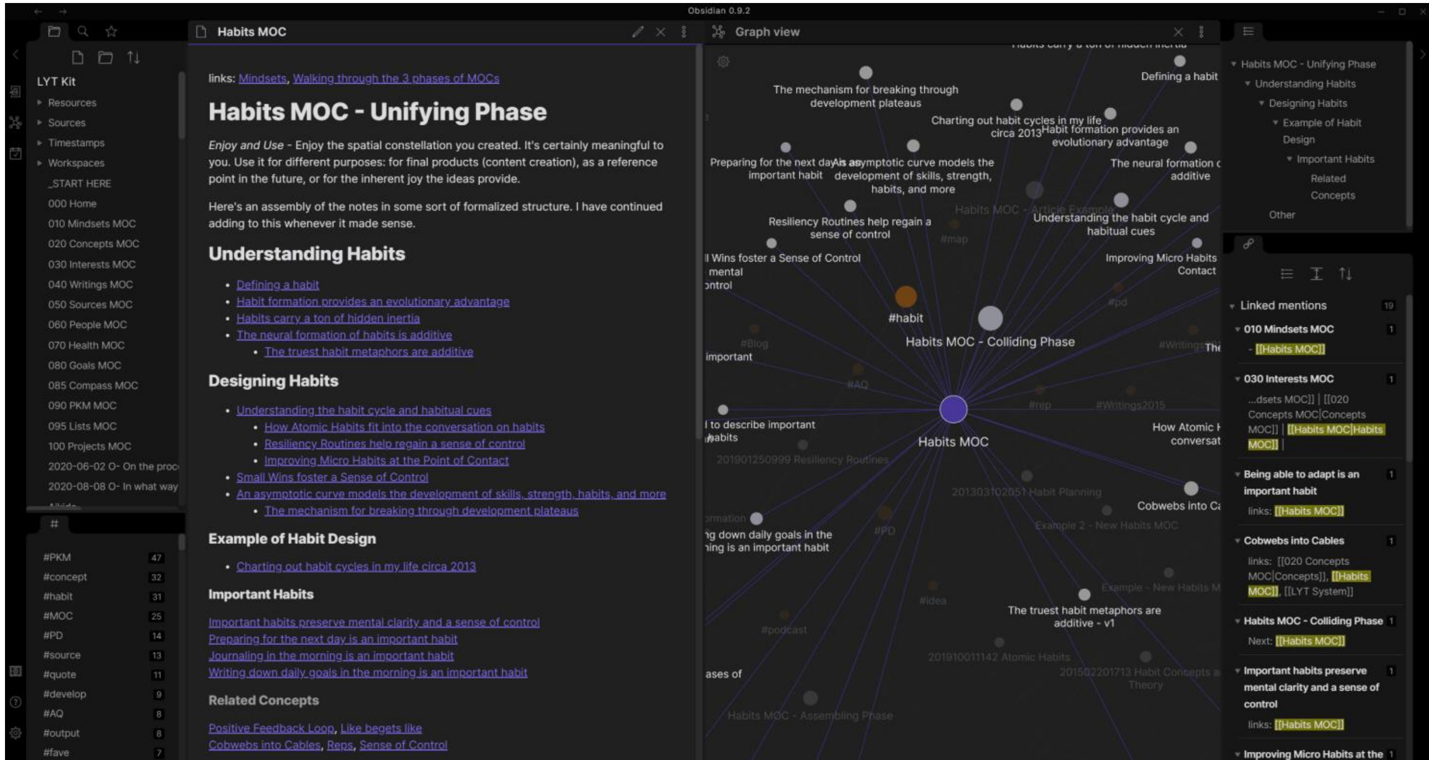
Note Taking

9.1

H4CK4SHELL

Obsidian

https://obsidian.md/



Obsidian 0.9.2
LYT Kit
Resources
Sources
Timestamps
Workspaces
_START HERE
000 Home
010 Mindsets MOC
020 Concepts MOC
030 Interests MOC
040 Writings MOC
050 Sources MOC
060 People MOC
070 Health MOC
080 Goals MOC
085 Compass MOC
090 PKM MOC
095 Lists MOC
100 Projects MOC
2020-06-02 O- On the proc
2020-08-08 O- In what way
#
#PKM 47
#concept 32
#habit 31
#MOC 25
#PD 14
#source 13
#quote 11
#develop 9
#AQ 8
#output 8
#fave 7
Habits MOC
Graph view
Defining a habit
The mechanism for breaking through development plateaus
Charting out habit cycles in my life circa 2013
Habit formation provides an evolutionary advantage
Preparing for the next day is an important habit
An asymptotic curve models the development of skills, strength, habits, and more
The neural formation of habits is additive
Resiliency Routines help regain a sense of control
Understanding the habit cycle and habitual cues
Improving Micro Habits at the Point of Contact
#habit
Habits MOC - Colliding Phase
Habits MOC
Cobwebs into Cables
The truest habit metaphors are additive - v1
Habits MOC - Assembling Phase
Habits MOC - Unifying Phase
Understanding Habits
Designing Habits
Example of Habit Design
Important Habits
Related Concepts
Other
Linked mentions 19

links: Mindsets, Walking through the 3 phases of MOCs

Habits MOC - Unifying Phase

Enjoy and Use - Enjoy the spatial constellation you created. It's certainly meaningful to you. Use it for different purposes: for final products (content creation), as a reference point in the future, or for the inherent joy the ideas provide.

Here's an assembly of the notes in some sort of formalized structure. I have continued adding to this whenever it made sense.

Understanding Habits

- Defining a habit
- Habit formation provides an evolutionary advantage
- Habits carry a ton of hidden inertia
- The neural formation of habits is additive
    - The truest habit metaphors are additive

Designing Habits

- Understanding the habit cycle and habitual cues
    - How Atomic Habits fit into the conversation on habits
    - Resiliency Routines help regain a sense of control
    - Improving Micro Habits at the Point of Contact
- Small Wins foster a Sense of Control
- An asymptotic curve models the development of skills, strength, habits, and more
    - The mechanism for breaking through development plateaus

Example of Habit Design

- Charting out habit cycles in my life circa 2013

Important Habits

Important habits preserve mental clarity and a sense of control
Preparing for the next day is an important habit
Journaling in the morning is an important habit
Writing down daily goals in the morning is an important habit

Related Concepts

Positive Feedback Loop, Like begets like
Cobwebs into Cables, Reps, Sense of Control

010 Mindsets MOC 1
- [[Habits MOC]]

030 Interests MOC 1
...dsets MOC]] | [[020 Concepts MOC|Concepts MOC]] | [[Habits MOC|Habits MOC]] |

Being able to adapt is an important habit 1
links: [[Habits MOC]]

Cobwebs into Cables 1
links: [[020 Concepts MOC|Concepts]], [[Habits MOC]], [[LYT System]]

Habits MOC - Colliding Phase 1
Next: [[Habits MOC]]

Important habits preserve mental clarity and a sense of control 1
links: [[Habits MOC]]

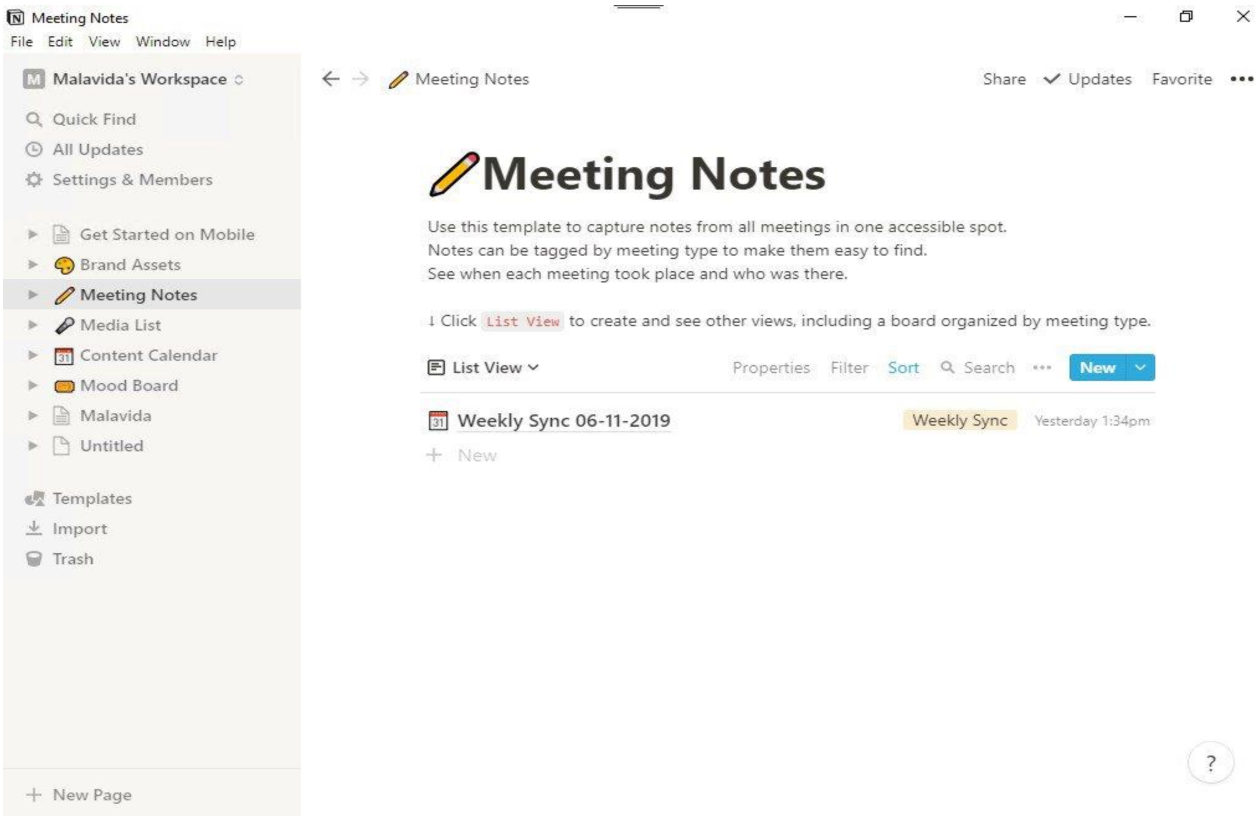
Improving Micro Habits at the 1

sys41x4

9.2

Notion

https://www.notion.so/



Meeting Notes

Use this template to capture notes from all meetings in one accessible spot.
Notes can be tagged by meeting type to make them easy to find.
See when each meeting took place and who was there.

↓ Click `List View` to create and see other views, including a board organized by meeting type.

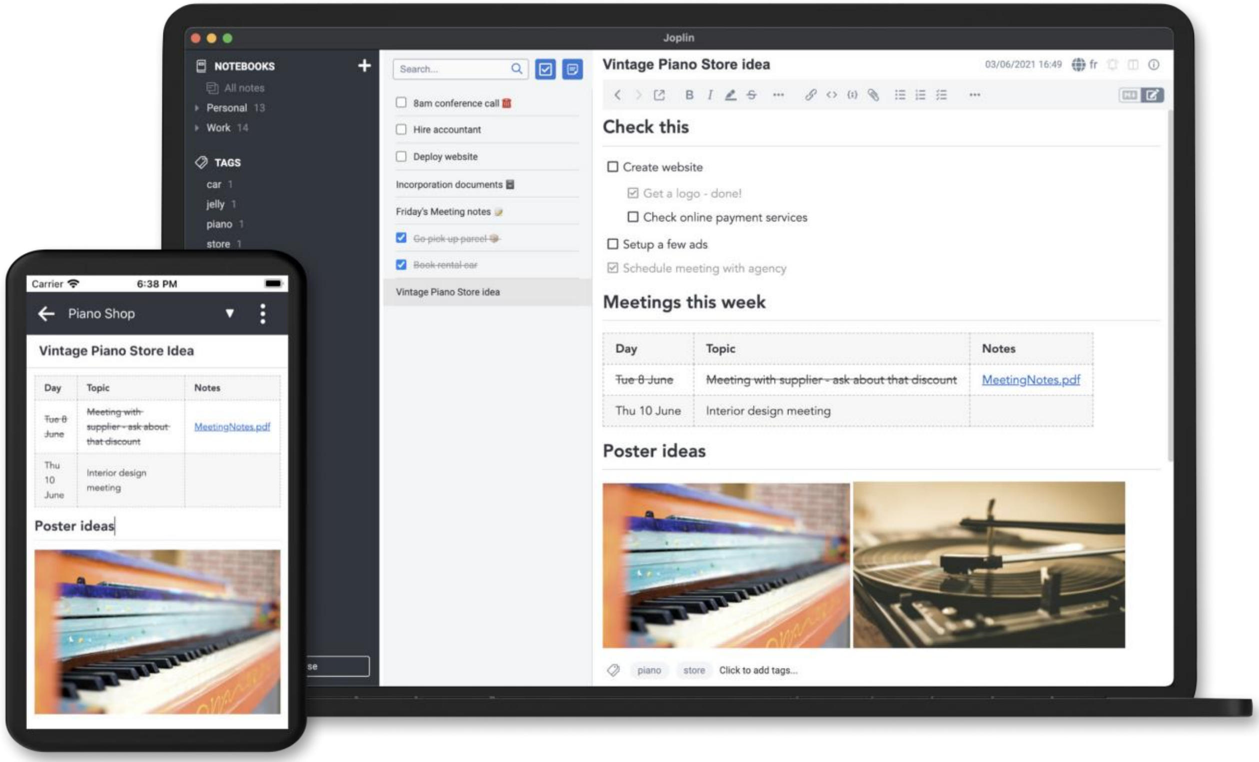
Weekly Sync 06-11-2019	Weekly Sync	Yesterday 1:34pm

9.3

H4CK4SHELL

Joplin

https://joplinapp.org/



□ 8am conference call
□ Hire accountant
□ Deploy website
Incorporation documents
Friday's Meeting notes
☑ ~~Go pick up parcel~~
☑ ~~Book rental car~~
Vintage Piano Store idea

Vintage Piano Store idea 03/06/2021 16:49 fr

Check this

- □ Create website
  - ☑ Get a logo - done!
  - □ Check online payment services
- □ Setup a few ads
- ☑ Schedule meeting with agency

Meetings this week

Day	Topic	Notes
~~Tue 8 June~~	~~Meeting with supplier - ask about that discount~~	MeetingNotes.pdf
Thu 10 June	Interior design meeting	

Poster ideas

piano store Click to add tags...

Vintage Piano Store Idea

Day	Topic	Notes
~~Tue 8 June~~	~~Meeting with supplier - ask about that discount~~	MeetingNotes.pdf
Thu 10 June	Interior design meeting	

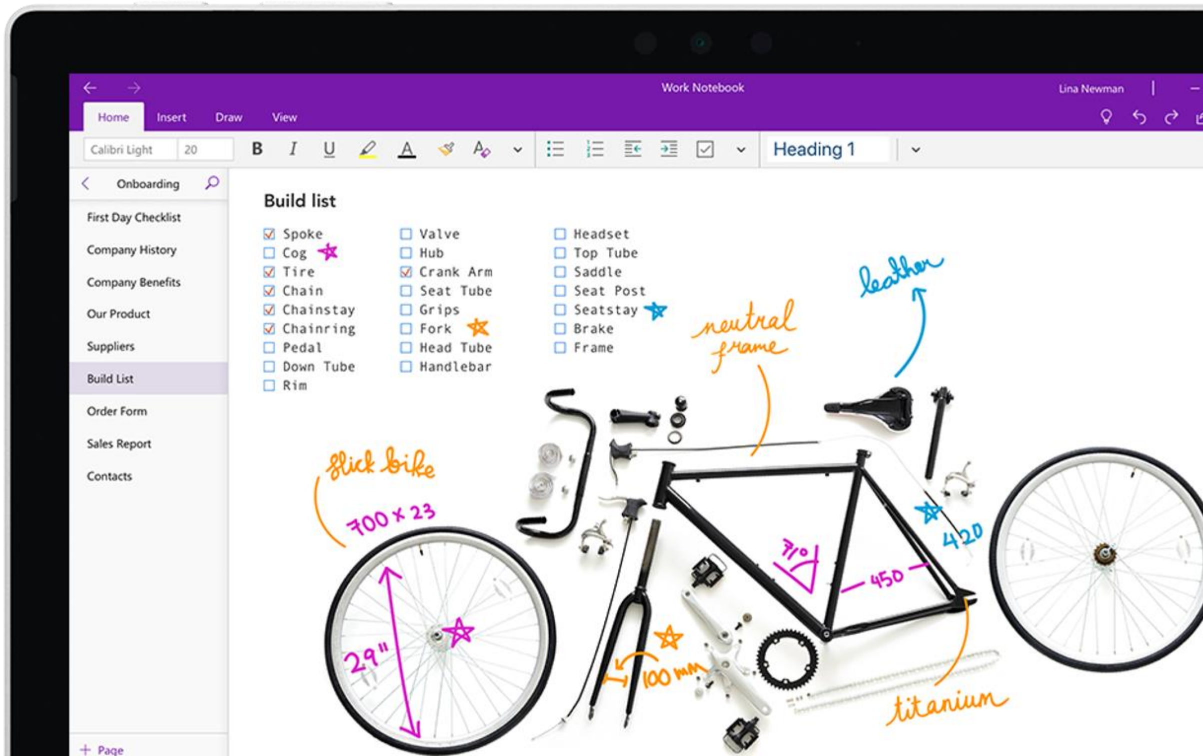
Poster ideas

sys41x4

9.4

OneNote

https://www.onenote.com



Build list

☑ Spoke
□ Cog
☑ Tire
☑ Chain
☑ Chainstay
☑ Chainring
□ Pedal
□ Down Tube
□ Rim

□ Valve
□ Hub
☑ Crank Arm
□ Seat Tube
□ Grips
□ Fork
□ Head Tube
□ Handlebar

□ Headset
□ Top Tube
□ Saddle
□ Seat Post
□ Seatstay
□ Brake
□ Frame

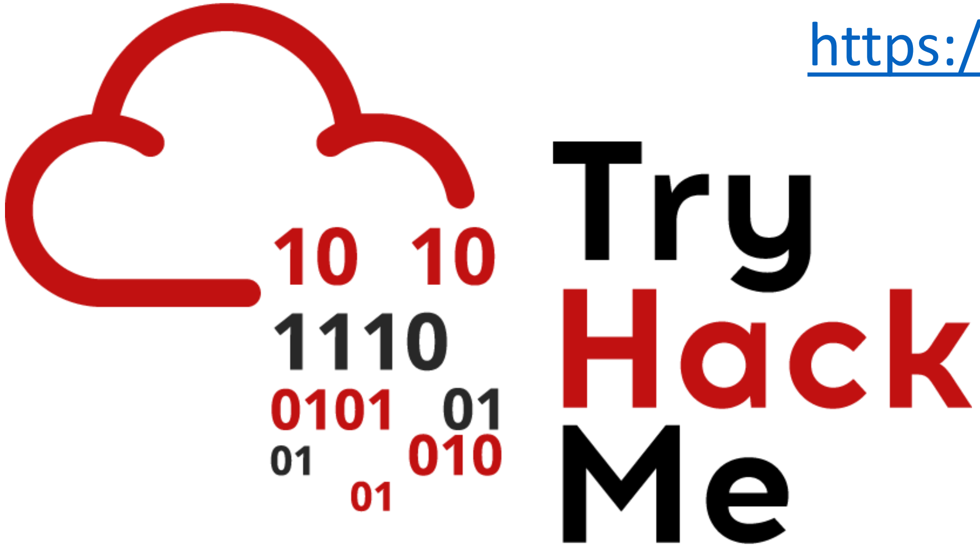
10

Practice Grounds

10.1

TryHackMe

https://tryhackme.com/



10.2

HackTheBox + HTB Academy

https://www.hackthebox.com/

https://academy.hackthebox.com/

HACKTHEBOX

HTB ACADEMY

10.3

Offensive Security Proving Grounds (OSPG)

https://www.offensive-security.com/labs/

10.3

PortSwigger LABS

https://portswigger.net/web-security/all-labs

PortSwigger

10.5

INE LABS

https://ine.com/

10.6

CTFLearn

https://ctflearn.com/

10.7

overthewire

https://overthewire.org/wargames/

10.8

Pentesterlab

https://pentesterlab.com/

PentesterLab

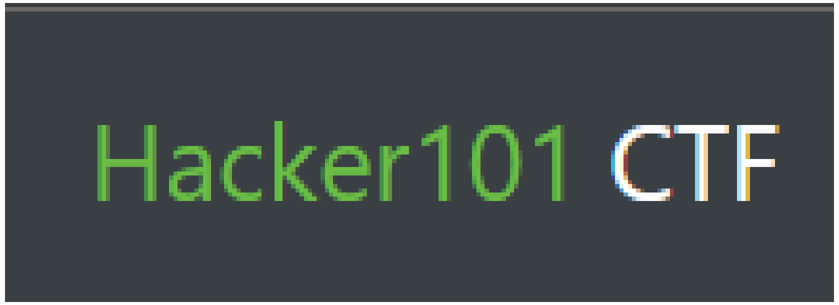
AttackDefense

https://attackdefense.com/

10.10

hacker101

https://ctf.hacker101.com/



Hacker101 CTF

11

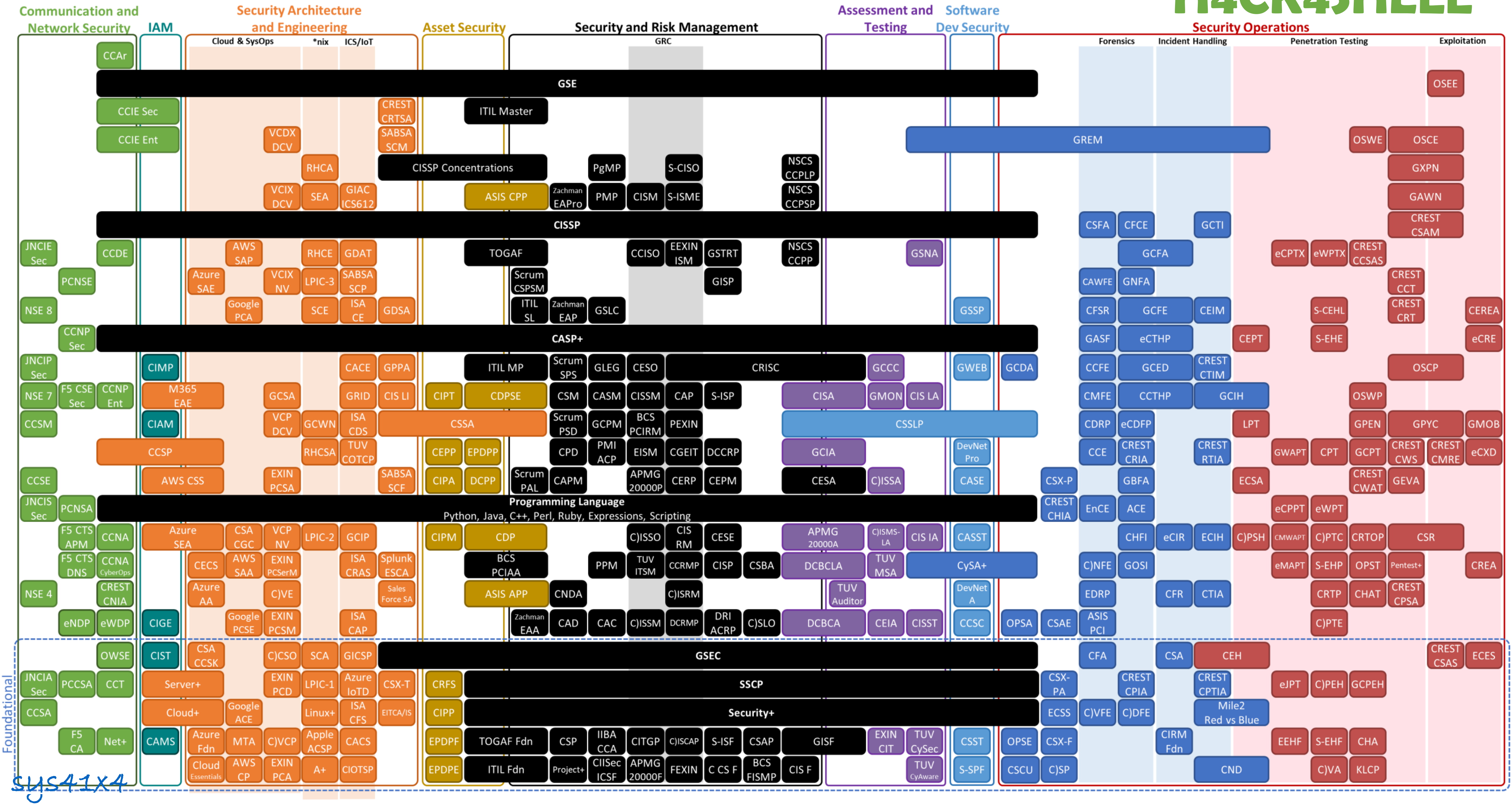
Professional Certifications

11.1

Certifications Over View

Security Certification Progression Chart 7.0 | (ISC)² CBK Security Domain Alignment

More info @ www.pauljerimy.com/security-certification-roadmap | 356 certs listed | October 2020



GSE

CISSP

CASP+

Programming Language
Python, Java, C++, Perl, Ruby, Expressions, Scripting

GSEC

SSCP

Security+

Communication and Network Security: CCAr, CCIE Sec, CCIE Ent, JNCIE Sec, CCDE, PCNSE, NSE 8, CCNP Sec, JNCIP Sec, NSE 7, F5 CSE Sec, CCNP Ent, CCSM, CCSE, JNCIS Sec, PCNSA, F5 CTS APM, CCNA, F5 CTS DNS, CCNA CyberOps, NSE 4, CREST CNIA, eNDP, eWDP, OWSE, JNCIA Sec, PCCSA, CCT, CCSA, F5 CA, Net+

IAM: CIMP, CIAM, CIGE, CIST, CAMS

Security Architecture and Engineering: CREST CRTSA, VCDX DCV, SABSA SCM, RHCA, VCIX DCV, SEA, GIAC ICS612, AWS SAP, RHCE, GDAT, Azure SAE, VCIX NV, LPIC-3, SABSA SCP, Google PCA, SCE, ISA CE, GDSA, CACE, GPPA, M365 EAE, GCSA, GRID, CIS LI, VCP DCV, GCWN, ISA CDS, CSSA, CCSP, RHCSA, TUV COTCP, AWS CSS, EXIN PCSA, SABSA SCF, Azure SEA, CSA CGC, VCP NV, LPIC-2, GCIP, CECS, AWS SAA, EXIN PCSerM, ISA CRAS, Splunk ESCA, Azure AA, C)VE, Sales Force SA, Google PCSE, EXIN PCSM, ISA CAP, CSA CCSK, C)CSO, SCA, GICSP, Server+, EXIN PCD, LPIC-1, Azure IoTD, CSX-T, Cloud+, Google ACE, Linux+, ISA CFS, EITCA/IS, Azure Fdn, MTA, C)VCP, Apple ACSP, CACS, Cloud Essentials, AWS CP, EXIN PCA, A+, CIOTSP

Asset Security: ASIS CPP, CIPT, CDPSE, CEPP, EPDPP, CIPA, DCPP, CIPM, CDP, ASIS APP, CRFS, CIPP, EPDPF, EPDPE

Security and Risk Management: ITIL Master, CISSP Concentrations, PgMP, S-CISO, NSCS CCPLP, Zachman EAPro, PMP, CISM, S-ISME, NSCS CCPSP, TOGAF, CCISO, EEXIN ISM, GSTRT, NSCS CCPP, Scrum CSPSM, GISP, ITIL SL, Zachman EAP, GSLC, ITIL MP, Scrum SPS, GLEG, CESO, CRISC, CSM, CASM, CISSM, CAP, S-ISP, Scrum PSD, GCPM, BCS PCIRM, PEXIN, CPD, PMI ACP, EISM, CGEIT, DCCRP, Scrum PAL, CAPM, APMG 20000P, CERP, CEPM, C)ISSO, CIS RM, CESE, BCS PCIAA, PPM, TUV ITSM, CCRMP, CISP, CSBA, CNDA, C)ISRM, Zachman EAA, CAD, CAC, C)ISSM, DCRMP, DRI ACRP, C)SLO, TOGAF Fdn, CSP, IIBA CCA, CITGP, C)ISCAP, S-ISF, CSAP, GISF, ITIL Fdn, Project+, CIISec ICSF, APMG 20000F, FEXIN, C CS F, BCS FISMP, CIS F

Assessment and Testing: GSNA, GCCC, CISA, GMON, CIS LA, CSSLP, GCIA, CESA, C)ISSA, APMG 20000A, C)ISMS-LA, CIS IA, DCBCLA, TUV MSA, CySA+, TUV Auditor, DCBCA, CEIA, CISST, EXIN CIT, TUV CySec, TUV CyAware

Software Dev Security: GSSP, GWEB, DevNet Pro, CASE, CASST, DevNet A, CCSC, CSST, S-SPF

Security Operations: GREM, GCDA, CSX-P, CREST CHIA, OPSA, CSAE, CSX-PA, ECSS, OPSE, CSX-F, CSCU, C)SP

Forensics: CSFA, CFCE, GCFA, CAWFE, GNFA, CFSR, GCFE, GASF, eCTHP, CCFE, GCED, CMFE, CCTHP, CDRP, eCDFP, CCE, CREST CRIA, GBFA, EnCE, ACE, CHFI, C)NFE, GOSI, EDRP, ASIS PCI, CFA, CREST CPIA, C)VFE, C)DFE

Incident Handling: GCTI, CEIM, CREST CTIM, GCIH, CREST RTIA, eCIR, ECIH, CFR, CTIA, CSA, CEH, CREST CPTIA, Mile2 Red vs Blue, CIRM Fdn, CND

Penetration Testing: OSWE, eCPTX, eWPTX, CREST CCSAS, CREST CCT, S-CEHL, CREST CRT, CEPT, S-EHE, OSCP, OSWP, LPT, GPEN, GPYC, GWAPT, CPT, GCPT, CREST CWS, ECSA, CREST CWAT, GEVA, eCPPT, eWPT, C)PSH, CMWAPT, C)PTC, CRTOP, CSR, eMAPT, S-EHP, OPST, Pentest+, CRTP, CHAT, CREST CPSA, C)PTE, eJPT, C)PEH, GCPEH, EEHF, S-EHF, CHA, C)VA, KLCP

Exploitation: OSEE, OSCE, GXPN, GAWN, CREST CSAM, CREA E, eCRE, GMOB, CREST CMRE, eCXD, CREA, CREST CSAS, ECES

11.2

H4CK4SHELL

Red Teaming Certifications

Offensive Security --> OSCP/OSWP/OSEP/OSWA/OSWE/OSED/OSMR/OSEE
eLearnSecurity --> eJPT/eWPTv1/eWPTXv2/eMAPT/eCXD/eCPTX/eCPPTv2
Pentester Academy --> CRTP/CARTP/CRTE
Comptia --> Pentest+/CySA+/CASP+
TCM Security --> PNPT

sys41x4

Blue Teaming Certifications

GIAC --> GCIH/GREM/GMON/GCIA
CISCO --> CCNA/CCNP/CISSP
Offensive Security --> OSDA
eLearnSecurity --> eCDFP/eCIR/eCMAP/eCRE/eCTHPv2/eNDP/eWDP
securityblue.team --> BTL1/BTL2/BTL3
Comptia --> Network+/ Security+/Linux+/Cloud+
Juniper --> JNCIA-SEC/JNCIS-SEC/JNCIP-SEC/JNCIE-SEC

Great Content Creators in WILD

12.1

H4CK4SHELL

Content Creators in Network Security

David Bombal
Network Chuck
Chuck Black
ITJunkie
TCM-(The Cyber Mentor)

sys41x4

12.2

H4CK4SHELL

Content Creators in Malware Analysis & CTF Creators

John Hammond
IppSec
DarkSec
MurilandOracle
0day
Hackersploit

sys41x4

Content Creators in **Web Pentesting**

InsiderPhD
zseano
NahamSec
Cristi Vlad

12.4

H4CK4SHELL

Content Creators in Buffer Overflows, Binary Analysis & Hardware Security

LiveOverFlow
Stacksmashing
Professor Messer
hackaday
hackster.io

sys41x4

Content Creators in **0-Day & Exploit Developers**

steventseeley
s1guza
itszn13
xerub
gf_256

Doubt Session

THANK YOU