Cyber Security basic Cheat Sheet

by Jianmin Feng (taotao) via cheatography.com/79308/cs/19793/

Udemy Nathan cyber security basic

https://www.stationx.net/canarytokens/

Basic theory - asset and vulnerability

Protect valued	confidential, not afford to lose, irrepaceable, cost most damages, impact reputation

privacy(confidential), anonymity (identity hiding),Preudonymity (false identity, such as bitcoin)

security and vulnerabilities (ssh, https, 2FA, vpn etc)

threats (virus malware, hacking, spyware, rootkits, adware, phishing,vishing,exploit kits)

adversaries (hacker, cyber criminals, spies, creackers, law enforcement goverments

assets and protection, granularity, risk assessments

risk =vulnerability X threads X consequences, trade off risk and beneficial

select - implement - assess -monitor

security vs privacy vs anonymity: conflict

cinfidentiality(keep your self), integrity (accuracy unmodified) availability (functional): CIA Tiad

Defense in depth: prevention- detection - recovery

Zero trust model, the less trust, including yourself, the safer. trust nothing trust nobody. never put online. nothing is safe online

basic theory - current threat and vulnerability

Value of hack: not a person, but a Bot -automate AI software to continuous attacking you.hijacking

Top 3 things need to stay safe online?

security bugs:always exist, as human writing code.OS, firmware, app, web browser (js, java), known bug + patches, unknown bugs + zero days , no patch

https://www.cvedetails.com/

https://exploit.db.com: public available, patch available, can be used to exploit unpatched system

basic theory - current threat and vulnerability (cont)

hacker-white (ethnic legal hacking) and black hacker (cyber criminals)

cracker- crack the key of a software

cyber criminal (black hacker,

malware:macro virus,stealth virus, polymorphic virus,self-garbling, bots and zombies, worms OS rootkit(bed in kernel), firmware Rootkit,key logger, trojan, Romote access tool (RAT)

Ransomware: designed to deny access to a computer system or data until a ransom is paid, usu by phishing.

spyware(spy), adware(formal spyware, highjack web searching), browser hijacking, scareware(fake info to scare you to pay), pup (potentially unwanted programs)

phishing(trick you to click, easy and high successful rate, 30% people still be fooled, email is common way to phishing): google.xxxxx.com, check HLD high level domain, goog1e, g00gle, hidden URLs

fake link

vishing: phone/voice

smsmhing: sms

spamming: unsolicited message, email, message etc. minimal cost, high earning.

doxing:ren-rou, googling/anything to get info for some body

social engineering: - scams, cons, tricks, fraud

cpu hijackers: crypto mining malware and cryptojackers

darknet (only accessible with special tools) vs clearnet(google, amazon)

dark market: access through darknet

exploit kits

government, spies, and secrete stuff: 5 eyes

regulating encryption, mandating insecurity and legalizing spying

trust and backdoors: formal methods, closed, open source, binaries, hash,digital signature

censorship

encryption

plan text ->cipher text ->plan text: encryption (ciper) decryption(decipher)
algorithm: public/lock
key: secrete/password
winzip: encryption method 256, 128, legacy(zip 2.0) key length and key space
AES(Advance encryption Standard): symetric algorithm (uses 1 Key private) password becomes the key
DES(data encryption standard,3 DES (triple-DES), blowfish, RC4-6 brutle force,dictionary force, hybride the two
Asymetric encryption: 2 keys(public and private),
RSA(Rivest shamir adleman), ECC(Elliptic curve cryptosystem):digtal signature; D (diffie hellman), EL Gamal
Key exchange and agreement:encrypt with one, decrypt with another.
Confidentiality(private key): decrypt with receiver's private key
authentication(private key): encrypt with sender's private key-signature
NOnrepudiation
integrity:
Asymmetric better key distr, scalability,authentication and non repudiation(not deniable), slow,mathematically intensive
Symetric: fast, strong
RSA:AES(1024-80, 2048-112, 3072-128, 15360-256)
hybrid cryptosystem: RSA(key distribution/encapsulation) and AES(data encryption encapsulation)
Https:handshaking(client hello/server hello)-->exchange certificate (authenication,authorized server issue their private key encrypted certificate, name, domain, public key of server usu, client is not required in general) -->exchange key(server public key, client symmetric key)

https://robertheaton.com/2014/03/27/how-does-https-actually-work/
https://nickfishman.com/post/50557873036/reverse-engineering-native-apps-by-intercepting-network
https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work

SSL TLS

Secure Sockets Layer (SSL) -> Transport layer security TLS(1.0-1.3)
Confifential(symmetric key AES), authenticated(public key, digital signature) and integrity(integrity check, hash value ectc)
cipher suites setup on server
Session Encryption Negotiation
1 shared larger prime number
2 AES algorithm
3 generated primes as private key
4 private key +shared prime + AES > public key > distribute to another party
5 private key +shared prime + public key of the other > shared symmetric key,generated indepently but the same
6.the shared key is used to encrypt the connection
Authentication:
client password and user nameor SSH Key Pairs.

https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work
https://www.hostinger.com/tutorials/ssh/how-to-set-up-ssh-keys

Https

Https:handshaking(client hello/server hello)
-->exchange certificate (authenication,authorized server issue their private key encrypted certificate, name, domain, public key of server usu, client is not required in general)
-->exchange key(client sends symmetric key)
ssh stripping: client>http > middle man > https>server
usingkali, or hardware
avoid: https only, tunnelling(VPN/SSH), only trusted website
sniffdet
arpwatch
VLAN:virtual LAN
ssllabs.com
SNI server name Indication

https://robertheaton.com/2014/03/27/how-does-https-actually-work/
https://nickfishman.com/post/50557873036/reverse-engineering-native-apps-by-intercepting-network
VLAN: virtual LAN

Hash

Integrity: hash function, checksum
MD5, Sha-256
powershell: get-filehash -Algorithm Sha512 c:\test.txt.
download checksum comparison: verify download
hash password to save d to use as verification, original password not saved.
HMAC: haseh based msg authentication code

digital signature

hash algorithm - hash value --> sender private key - signed msg
authentication, nonrepudation, integrity
signed msg --sender's publick key -hash value
windows device guide

digital certifictes and https

digital signature from well know trusted company(third parties)
local library of digital cert library auto loaded (roots)
local digital cert manually loaded(self signed, trusted parties)
compromised/fake digital cert: really risk
CA Ecosystem
CA example mistaks
SSL sniff
CA patrol
cert fingerprints
pinning

E2EE, steganography

E2EE end to end encryption:PGP ZRTP OTR SSL/TLS
use E2EE always possible
steganography: the practice of concealing a file, message, image, or video within another file, message, image, or video.
openpuff

Setup testing environments

type2 Hosted: hard ware ->OS ->hypervisor->OS
type 1 native: hardware >hypervisor->OS
vmware or virtualbox
testing environment |security options
install virtual OS: physical DVD, virtual DVD (ISO), prebuilt virtual disk/image (.ova form virtual box)
Kali: debian, 600 penetration testing tools.
osboxes.org for prebuilt images