Practice test 5

Monday, October 16, 2023 12:01 PM

Measures of disorder

entropy - measure of cryptographic unpredictability

high entropy = more security

lack of = "vulnerable and unable to encrypt data securely"

nonce - random or semi-random # generated for specific use and only used once

longevity - operational life of a key based on sensitivity of key and how much data

integrity - confidence that data, files, system configs have not been modified

PDU - power protection and management system; monitors and manage voltage and electrical current in one

UPS - collection of batteries and charging circuit + inverter to generate AC voltage from DC from batteries

placed on system level for data availability

generators - converts one form of energy to another

ex: fuel & batteries → power

network forward traffic from 1 node to another with router/switch

PDU is for management & monitoring but <u>does not</u> store power for backups

main function is distribution

dual power supply - two or more elec inputs
that supply power to single circuit

DNS Amplification attack - app attack
that targets vulns in headers/payloads
of app protocol
triggers short request for long response
at victim network

Secure cookies = session hijack & data leak

malicious code client-side attacks

- session replay

SOAR can be used to validate ML
data before giving to model

how to circumvent attackers using decoys?

how to circumvent attackers using decoys?

Use a **defensive maneuver** - use passive discovery techniques so threat actor dont know theyre been made

intelligence fusion - combine threat anal platforms w/ threat feeds to determine if active threat

ISAC = info sharing and Analysis center

rights management - data owner exert control over info and provides access to users

r/w/e

SSRF - exploits lack of auth between internal servers (implicit trust) and weak input valid

valid

Active Directory Domain Services AD DS

- "Enforce password history"

  how many previous pwords are blocked

- "passwords must meet complex reqs"

- "logon hours"

  time of day restrictions

has no password reuse policy

using work pword somewhere else

these can only be enforced w/ soft policies

IPsec = IP traffic

RADIUS

- AAA server
- NAC/RADIUS client
- Supplicant = any device trying to access remotely

802.1x - Port based NAC proto provides means of using EAP method when device connects to switch port, WAP, or VPN

fingerprinting - topology discovery tech
- scans for hosts
  - IP ranges
  - routes
- WiFi scanner for AP

enterprise workspace - corpo apps bundled in container

netcat - reads/writes data across net connections

can be used for port scanning

directory traversal = request info from server not w/ directory path

XML injection = take advantage of data w/ no encryption to inject code

honeyfile = track misusage/exploit

honeypot = analyze attack strats

honeynet = decoy to provide false rep of net topology

SNMPv1 & v2c = no encryption and send community names in plaintext

SNMPv3 = encryption (DES ; AES) and
strong user based auth
Unames + access perms

Management info base MIB - database
that agent within SNMP uses
agent = process that runs on net device

SSL/TLS = proto between app and
transport layer to encrypt TCP
connection

Mimikatz - widely used Windows
tool to retrieve passwords, NTLM
hashes, and conduct Kerberos attacks

admin = brute force first?
mentions SQL injection

hashcat = password recovery tool

Hybrid password attacks - combo. of dict and brute force

weak/reused passwds

ex: have i been pwned + exec account

John the ripper - not as intense as hashcat but effective at smaller-scale pword cracking