Secure Network architect

29 mrt

* New Kali template
* WiFi adapter

Network separation and zones/Classification

Bok Security Engineer

White Heads

31 mrt

Kamil:

Cyber offensive
High tech campus
White box security assesment
Cert: OSCP, OSWE, OSWP and OSEP

Stan vander Vleuten
Cyber consultant
Web, mobile, Desktop, Embeded
eWPTX

White Box source code
General overview of the APP
Test Protocol per item:
- Identify Hot spot
- Validate Hypothesis
- or other way

Web application and Infra

Burp Suite

From Zero To Hero
Juice Shop
  Back end: Node-JS
  Frontend: Angular

Obtain foot
Read Local

Container Sec

31 Mrt

Note: Hacking is illegal

Containers vs Vm
- Container uses same kernel as the kernel
- Containers are modulaire
- Container can run multiple software on one os

SeLinux
- Limiting File acces
- Restrict syscall
- Isolate UID, PID, hostname

Container security: what can go wrong?
- Containers can break out
- Docker runs on Root Privelage
- Back Doors
- Unpatched containers
- Config mistake

Docker Daemon Attack Surface

Mitigation
- Use trusted Base images
- Update the container
- Use secure config
- Perform securityscans (Dock Bench for security)
- Have tight controls

Principle of Least Privilege
- Do not run as Root if you don't need it
- Limit the amount of user/processes
- Don't give extra permission

Hutten

Meeting

Nick Buvnen
Styn Veld Paus

* Security is HIGH Topic RN

Update Security Policy

* Segmentation will start in June

Two Buildings Same Setup

Azure is No go

ONLY it Social Engineering

Digital NDA

Time on a day 6 Hours a day

Wifi and Lan are welcome

Spare Laptops can be used

Discus 2 Hours

Wifi Intercept is ok

Get Laptop of their to acces AD

SSID is Hidden

Intune Device Reserved for us

Last week of april (27 of April) to start

Location: Hutten: Serice

Port exclude: Cameras, Alarms
Cameras: no Cracking Pass or any other sec

Network Intrusion Detection and Prevention

5 Apr

NIDS 2023

Tools:
- SNort
- Suricata

IDS
NIDS Patern matching
HIDS Anomaly detection

PFSense + Suricata

ALReady DiD Snort in Sem 3

It monitoring

6 APR

Traditional monitoring (operational)

What needs to be logged
- Event
  - Software Dev
  - Users
  - System manager
- Logging Data
  - performance
  - Usability
  - Confidentiality

What to take care of?
- Amount of logging and logs
- Log file truncation
- Cyclic log files
- Time sync
- Acces to logging
- Log level

Where to log
- Disk based
- Network based

How will be logged
- Poll
  - Monitoring system connects
  - E.g. Service as HTTPS, POP3, SSH
- PUSH
  - Host push data
  - E.g. Service CPU, memory
- Hybrid
  - Combination of Poll and PUSH

Simple network management protocol (SNMP)
- OLD
- Not safe

Nagios: monitoris
- Nagios Xi is non free
- Nagios open source version

Prometheus

IT Security Monitoring

6 APR

IT monitoring VS security monitoring
Availibility VS Confidiality, integ, compliance
SLA Req VS Sec Policy Req
Traditional oldsystem VS New Tech and Process

Siem For SoC
- Detect Report
- Collecting Report
- Correlation Report
- Report Incident
- Manage Incident
- Quality assurance

NSM: What data are Relavant
- ALOT OF Things

Password Cracking

Password Length:

Brute Force Strength

Have i been Pwned?: 11 Times

Threads To Passwords
- Default Pass
- Brute Force
- Shoulder Surfing
- Key Loggers
- Dumpster Diving
- Leaked Pass

  etc....

Hydra
- Use Burp

Owasp Zap

  Its Free unlike Burp

Application Pentest

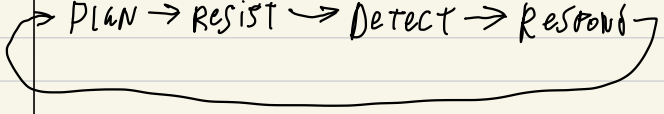
  Swipping

  Social Engineering

Security Incident management

13 Feb

INCIDENT management



Phases in sec handeling
- Prep
- IDentify
- Containment
- Eradication
- Recovery
- Lessons Learned

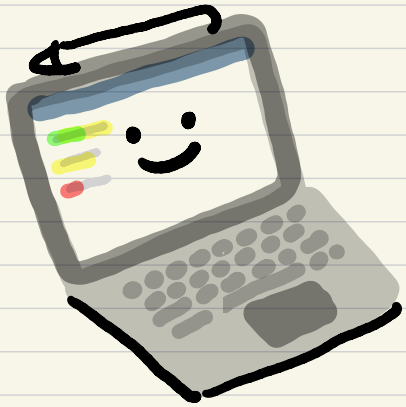
PRepare and Prevent
- Alert Reception
  - Ongoing alert
  - CUSTomers report
- Triage
- Response
  - Technical response
  - Management Response
- Review

MSSP

AUthentiCation workShop

IGAPr

What is AUth : To Prove you are you OR Prove something is true
RBAC : Role Based acces



SHared Secret
- Pass
- PIN
- Symmetric Keys
- Api Key

Biometric auth

MULTI Factor AUThenTicatioN (MFA)

DigiID infrastructure

1. Choose between ID or a passport check
2. SMS authentication
3. Wait for confimation (3 days)
4. Choose your own PIN (5 digits)
5. MFA/2FA upon every login?
6. You can log in your account
7. Put in your code
8. „You are logged in"!

CVE SysDefence

20TH April

Application Hardening
Operation Hardening
Server Hardening
Database Hardening
Network Hardening

CVE
- Dictionary
- Standard
- Linking pin
  - The Number

CVE is not:
- a virus Negate

OT Security

21 April

It is for the industry
Probably for IOT

VDL got Hacked

SANS
Arnaud Soullie : Senior Cyber

Software :
PLC
Eco structure
ICS Simulation platform
IGSS
machine expert
Simulation RII
Revolution pi

Brucon 0x0

Advanced Pass Crack

21 April

Why are we using password
- Usability & Deployability

Smith Attack

Does your password matter?

Hacker use after pass complex rules
- Known characteristics of password
- Guess
- Password stuffing
- Use context information

Ethical Consideration
- Use breached passwords
- Validate researches on hashes