Funded by the European Union

CYBER4Dev

Vulnerability assessment Estonian CIIP methodology

Priit Kaup

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Approach

Funded by the European Union
CYBER4Dev

- We are mainly using “white-box” approach during vulnerability assessments.
- While the “black-box” approach is more realistic…
- We believe that “white-box” approach gives a better picture of the IT security situation of the target company.
- “White-box” method is also considerably cheaper and faster since it is less time consuming.
- Evaluation is done using best practices i.e CIS18.
- “Risk Based Time Limited” prioritization is also used depending of the discovered situation during On-Site testing.

Methodology

Initial meeting

- Introduction of the testing Methodology will be presented to the target organization.
- Detailed planning of the testing targets (services, subnets, physical locations).
- Actual dates of on-site testing will be decided.
- Requirements for on-site testing will be addressed to the target organization.
- Reporting schedule will be agreed and a date of the final project meeting will be scheduled.
- In case of 3-party testers the confidentiality agreement between the tester company and target organization will be prepared.

Preparation

Information gathering

- Usually done before the onsite testing (black-box)
- Collecting relevant information about the target company from the internet:
  - Employees
  - Contractors
  - Public IP ranges used
  - Devices used
  - Internet facing services
  - Public leaks that could include information about target related user accounts.
  - Domain security configuration
- Tools used for information collection:
  - Google
  - Shodan
  - search.censys.io
  - PassiveDNS services
  - Different CLI tools (dig, openssl, wget)

On-Site testing

- **Team size depends of the target network. Usually:**
  - Team-lead who will be responsible for the arrangement of the testing and will be doing assessments of the documentation and procedures.
  - 1 or 2 technical experts.
- **Requirements for on-site testing**
  - Office space for on-site testing.
  - Network access to the required networks (wired connection)
  - User accounts for testing (domain admin rights)
  - Assigning local contact person(s) who's main responsibility during the testing is to support the testing and who knows about services/network setup.
    Usually a sysadmin and a network admin.

Information gathering

Network Perimeter

- We consider the internal network security design as important as securing the external perimeter.
- External network perimeter protection is widely understood and usually pretty well implemented.
- End-user networks are the foothold for the attackers.
- Network design is evaluated against best practices.
- The network segmentation is tested against the initial design. Meaning that the services/servers in network should be accessed only from the networks it was initially intended to.

Network Perimeter testing

M

Network Perimeter

Testing includes:

- Interviewing the local administrators
- Analyzing Network Schemas (if they exist)
- Analyzing Firewall rules + logs
- Analyzing Firewall IPS/IDS configuration if available.
- External perimeter testing is done from the Internet and is targeting all target organization's IP ranges on all 65535 ports.
- The end-user networks (office, wifi etc) are considered as the external networks when testing the isolated internal network segments (ICS/SCADA).

Network Perimeter testing

M

Critical Networks

It is crucial to perform the testing of the critical (ICS, SCADA) network perimeters with extreme care, as the operation of the processes may require constant and undisturbed operation of the network.

Testing includes:

- Auditing firewall traffic logs that are related to critical networks.
- Capturing and analyzing the critical network perimeter traffic.
- Testing network segmentation using existing tools available in workstations located in critical networks.

Network Perimeter testing

M

Service Discovery

1. Make a list of critical services/hosts that can break during port scanning.
2. Discover available services in target IP range:

a) External - SYN scan for all ports (0-65535).

b) Internal - SYN scan using NMAP 1000 common ports and custom port ranges based on host profiles (excluding critical).

3. Create target lists based on discovery scans.
4. Do a Version Scan based on target lists.

Vulnerability Detection

1. Use automated tools to discover vulnerabilities:

– Nessus, Open-VAS, etc

2. Acunetix, OWASP ZAP, Burp Suit, WPScan, DroopeScan, Joomscan

– Manual vulnerability assessment using common testing tools: web browser, netcat, curl, openssl.

3. Testing vulnerabilities with known exploits (ExploitDB, Github), if required.

Vulnerable Configurations

- Directory listing
- Public .git folders
- Public configuration files (config.php, database dumps etc)
- Testing IP spoofing (X-Forwarded) to bypass HTTP services IP based ACL-s
- Missing authentication
- Default passwords
- Smart Card Authentication misconfigurations
- etc ...

Vulnerability Detection

M

Inspection of IT governance

- Documentation
  - Network Topology
  - IP management (vlans, subnets)
  - Disaster recovery plan
  - Other IT governance documentation.
- Procedures/Tools/Services
  - Hardware + Software Inventory
  - User Account management
  - Configuration management
  - Centrally managed: logging, patching, antivirus, backup, authentication.

IT management

Vulnerability Assessment of Devices

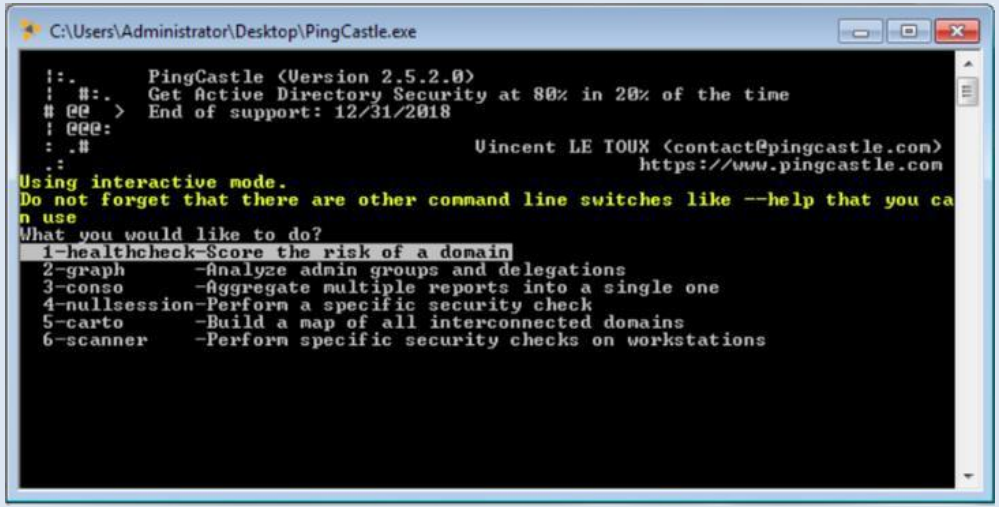
- The objective of this phase is to verify whether the configuration of **workstations, servers,** and **network devices** are in compliance with recommended best practices and the information security policies established in the organization.
- This includes testing for the presence of:
  - Outdated and forbidden software
  - Presence of Antivirus and up to date AV signatures
  - Unsecure use of an administration profile.
  - Vulnerable configuration
- Nessus Vulnerability Scanner is used for automated scans of workstations and servers.
- Evaluation for other devices is done manually.

Assessment of Devices

M

Vulnerability Assessment of Devices

PingCastle is an excellent tool to verify domain security.
https://www.pingcastle.com/



Servers and Workstations

test.mysmartlogon.com

Date: 2018-07-25 - Engine version: 2.5.1.0

Active Directory Indicators

Indicators

Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Stale Object : 46 /100 — 5 rules matched

It is about operations related to user or computer objects

Privileged Accounts : 45 /100 — 3 rules matched

It is about administrators of the Active Directory

Trusts : 100 /100 — 3 rules matched

It is about links between two Active Directories

Anomalies : 100 /100 — 9 rules matched

It is about specific security control points

Risk model

Remote Connections

- **Mapping all remote connections in use**
  (ipsec, vpn, rdesktop, vnc, ssh, ftp etc…)
  - Interviewing administrators, users
  - Using results of service discovery scans done previously
- **Analyzing security configuration of remote connections.**
  - Authentication methods (password, certificate, MFA usage)
  - Encryption methods/ciphers used.
  - Protections against password attacks
  - Analyzing remote connection access logs
- **Review of remote connection user accounts.**

Wireless networks

- Mapping wireless networks available in the area
- Networks are identified based on the name, approximate location and signal strength. The goal of this task is to identify and locate rogue/undocumented wireless access points.
- Analyzing wireless access point configuration, client isolation, authentication and encryption methods.
- Wireless attacks will be carried out if necessary. Attacks may include eavesdropping, MAC-spoofing, pre-shared key guessing and breaking passwords from captured data.

Phishing Tests

We are also performing a Phishing Tests to evaluate cyber security awareness of employees of the target organization.

- It is important not to spread the knowledge about the phishing test inside the organization. The less people know about is better.
- When conducting the phishing test it is also very important to notify local CERT/CSIRT or other organizations who are dealing with the cyber security issues.
- Notify the owner of the domain that you are impersonating so they know about it / ask for permission.

Phishing Tests

Preparing the infrastructure:

- Choose an attack vector - some website that is commonly used by the employees of the target organization.
- Register an internet domain name that is similar to the actual domain name of the website that will be used for the Phishing attack.
- Clone the original website using wget, GoPhish or other tools.
- Configure the phishing domain SPF, DMARC, DKIM, HTTPS so that it will not get stuck to the Spamfilters and Web browsers would not block the content when accessing the website.

– If the email security configuration is missing we will spoof the original domain for sending a phishing email.

– Or just ask the local admin to whitelist the phishing domain.

Phishing Tests

Preparing the content:

- The website should be hosted by a trusted hosting provider and use HTTPS to not leak credential or other confidential data that users could enter.
- It is important to prepare a very authentic email content, because the first impression is most important if you want to get a click. The sender must also be trust worthy.
- The email should be in HTML format and contain some hidden content that will be accessed when email is opened and contain also a clickable url. The urls must be unique to be able to track which user opened and clicked the link on an email.
- To make it less suspicious the cloned website must be edited very little and use already existing authentication forms that are also available on actual website.

Physical Security

The objective is to see **whether it is possible to gain unauthorized physical access** to network switchboards, server rooms, other off-limits IT systems, device racks etc.

- Physical security assessment is performed by doing visual observation on selected locations.
- Physical force is not used to gain access to locations or devices.
- Checking the design and presence of the security system, physical access controls (physical keys, PIN codes, keycard system management)
- It also includes **assessing the availability risks** to the hardware components like presence of **air conditioning, UPS, backup generators, readiness in case of emergency situations** (fire, water emergency, inflammable objects inside server room etc.) Also design of the server room.

Reporting

- Introduction that describes the assessment timeline, scope, methodology and participants.
- Summary of the general level of IT security and most critical problems discovered.
- Description of vulnerability scoring system used to prioritize the discovered vulnerabilities.
  - Risk of the vulnerability – High, Medium, Low, Info
  - Difficulty of remediation – High (difficult), Medium (relatively easy), Low (easy)

Reporting

- List of critical findings that include in depth description of the problem and recommended remediation.
- List of all findings as follows:

Description	Risk	Difficulty of remediation	Affected hosts	Remediation recommendations
Unsegmented internal network	**High**	**Difficult**	10.0.0.0/24	Implement network segmentation based on the need for data protection on servers and workstations, and establish access control between network segments. The computer network must be segmented into different security domains. Traffic between segments must be controlled by firewalls and the least privilege principle must be used. We suggest to start segmentation from most critical (SCADA) networks.

Reporting

- We are also considering adding CVSS scoring standard to be able to compare the results and make statistics.

Common Vulnerability Scoring System (CVSS-SIG)

- **Calculator**
- Specification Document
- User Guide
- Examples
- CVSS v3.1 Documentation & Resources
- CVSS v3.0 Archive
- CVSS v2 Archive
- CVSS v1 Archive
- JSON & XML Data Representations
- CVSS On-Line Training Course
- Identity & logo usage

CVSS

Common Vulnerability Scoring System Version 3.1 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.1 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.1).

Base Score

8.4 (High)

Attack Vector (AV)

Network (N) | Adjacent (A) | **Local (L)** | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | **High (H)**

Integrity (I)

None (N) | Low (L) | **High (H)**

Availability (A)

None (N) | Low (L) | **High (H)**

Hands-On training

- Your computer CPU must have Virtualization Support Enabled
- Insert USB key and
  - Install VirtualBox 6.1
  - Create a folder for VM-s on your computer
  - Copy VM-s (folders) from the USB key to the previously created folder.
  - Double Click every *.vbox file and make sure that it appears to VirtualBox Manager
  - Configure as many vCPu-s as available for both machines
  - Change Display video memory to max for Kali
  - Start VMs named: KALI and Metasploitable

Preparation