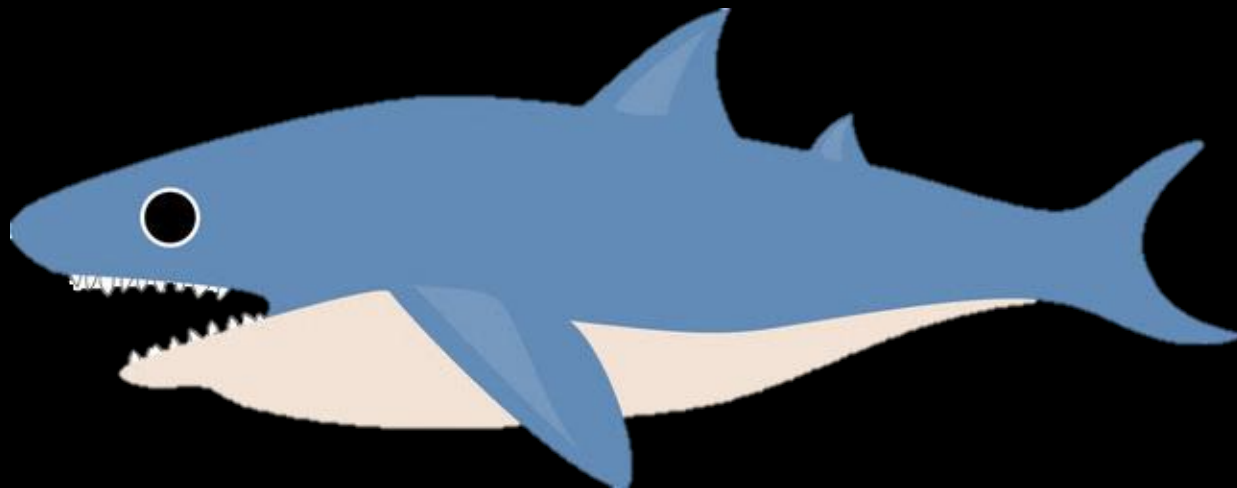
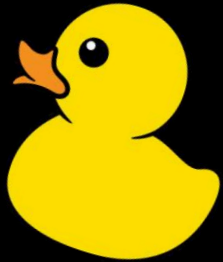


PAM and Penetration Testing (Hacking) Tools

By: Salman Youssef



Introduction to Privileged Access Management (PAM)

- **Definition:** Control over privileged devices in an organization, with the aim of containing such privilege to a small subset of all devices, thereby reducing the scope of potential attacks.
- **Importance:** Protects against internal and external threats by managing, monitoring, and auditing privileged access.
- **Penetration Testing tools** like the Rubber Ducky, Shark Jack, and WiFi Pineapple can exploit vulnerabilities in devices with privileged access.

Penetration Testing Tools and Privileged Access

- Tools that we will discuss are all **commercially-available** and can be **legally bought and utilized** by anyone.
- Learning about these penetration testing tools is a way to **understand potential vulnerabilities** and techniques that adversaries can utilize to exploit devices with privileged access.
- Helps us realize that PAM should be paired with security practices that **mitigate the risk** of such tools (as discussed in later slides).

Rubber Ducky

- **Tool Overview:** Designed by Hak5, the Rubber Ducky is a keystroke injection tool that can execute a wide variety of user-designed **scripts** when plugged into a device.
- **PAM Vulnerability:** If a threat actor gains physical access to a device with privileged access, the Rubber Ducky can inject commands to exploit the device's access.
- **Mitigation:** Enforcing MFA, logging and monitoring device activities via a SOC (Security Operations Centre), and blocking USB ports.

Rubber Ducky

Value: \$80

Time needed for first attack: 10 min.

Time needed to master: 50 hrs.



Shark Jack

- **Tool Overview:** An Ethernet-enabled network reconnaissance tool which also utilizes user configured **scripts** to exploit a target network.
- **PAM Vulnerability:** It can quickly map networks and find vulnerable privileged accounts or services.
- **Mitigation:** Implementing network segmentation, logging and monitoring device activities via a SOC, and blocking unused Ethernet ports.

Shark Jack

Value: **\$100**

Time needed for first attack: **20 min.**

Time needed to master: **50 hrs.**



WiFi Pineapple

- **Tool Overview:** Used to capture and analyze network traffic and can be used for a wide variety of attack, including Man-in-the-Middle.
- **PAM Vulnerability:** This tool can capture privileged session credentials if network traffic is not encrypted.
- **Mitigation:** Use of encrypted sessions (e.g., SSH, VPN), restricting privileged access over insecure networks, and logging/monitoring wireless traffic.

WiFi Pineapple

Value: \$140

Time needed for first attack: 30 min.

Time needed to master: 75 hrs.



Scripting

- **Scripting** is how most hacking tools accomplish their tasks. This can be done using a wide variety of scripting languages, **Bash** being amongst the most popular.
- **Notably**, the Rubber Ducky uses its own unique scripting language, **Ducky Script**, which can be used to run privileged commands via command-line tools such as PowerShell (Windows).
- **Logging and monitoring** of any script execution is a great way to ensure that any scripts being ran on devices are observed and can be analyzed.

My work at Canadian Nuclear Laboratories



- Created “**Attack Modules**” that were to be used for a set of IR (Incident Response) training exercises for Nuclear Energy Workers.
- The attack modules included
 - research about each tool’s capabilities
 - where it falls under **MITRE ATT&CK** (a knowledge base of adversary tactics and techniques)
 - its impact on each stage of the **NIST** framework
 - a step-by-step procedure to be used by trainees

My work at Canadian Nuclear Laboratories



The NIST Framework

"helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data...You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover."



My work at Canadian Nuclear Laboratories



« Rubber Ducky Attack »

*Utilizes privileged access of EWS
(Engineering Workstation) to run a
Man-in-the-Middle attack on the HMI
(Human-Machine interface) and PLC
(Programmable Logic Controller)*



My work at Canadian Nuclear Laboratories



« Shark Jack Attack »

Trainees are instructed on how to arm the shark jack,

Guided on how to perform the attack via a network switch,

Instructed for retrieving the information that has been collected

- Shows how easy it is to get started with one of these tools

