**☎️ War Dialing Challenge Lab — Beginner Notes**

**🔍 What is War Dialing?**

**War Dialing** is the act of automatically dialing a list/range of phone numbers to find **modems, fax machines, voicemail boxes, PBX systems**, or other systems that answer calls.

🧠 *Old-school hackers used it to find weak points in corporate phone systems.*

**🎯 Why Should You Learn This?**

* To **understand how attackers find hidden systems** connected via phone lines.
* Helps in **testing legacy systems**, especially in **VoIP/telecom security**.
* Still relevant in some **critical infrastructure**, **PBX hacking**, and **acoustic intrusion** scenarios.

**🔊 Acoustic Intrusion (What’s That?)**

This is when **audio signals (like from speakers or phones)** are used to carry data, leak information, or even exfiltrate files.

🧠 Example:  
An attacker sends data over **high-frequency sound** that humans can’t hear but a microphone can record.

**🔁 War Dialers (Tools)**

| **Tool** | **Description** |
| --- | --- |
| **WarVOX** | Modern tool that works over VoIP. Dials numbers, analyzes audio. |
| **ToneLoc (T00NY)** | Classic MS-DOS war dialer (1990s tool). |
| **iWar** | GUI-based war dialer. Still used in some environments. |
| **Modem utilities** | Like minicom, used to manually connect. |

**🎯 What Can Be Found?**

1. **Modem lines**
2. **PBX systems** (Private Branch Exchange)
3. **Voicemail systems**
4. **IVR menus** (Press 1 for Sales...)
5. **Fax machines**
6. **Remote access devices**

**💻 WarVOX (Modern VoIP War Dialing)**

**🛠 What it Does:**

* Uses VoIP instead of analog lines.
* Dials numbers and records the audio.
* Analyzes waveforms to detect modems, fax, voicemail, etc.

**🚀 Steps:**

1. Install WarVOX (works on Linux).
2. Configure with SIP provider (VoIP).
3. Load list of numbers to call.
4. Start dialing.
5. Analyze responses (tones, silence, patterns).

**🔐 Voice Mail Boxes – Vulnerable Points**

Attackers often:

* Guess default PINs (like 1234, 0000)
* Access saved voicemails.
* Record new outgoing messages.
* Leave malicious payloads or phishing messages.

**🛡️ Preventive Controls**

| **Threat** | **Prevention** |
| --- | --- |
| **Unauthorized Modem** | Scan & remove all old modem lines |
| **Voicemail Hacking** | Use strong PINs, lockout on failed attempts |
| **PBX abuse** | Firewall VoIP, disable unused extensions |
| **War Dialing** | Monitor call logs, detect high call volume |
| **VoIP exposure** | Use SIP hardening, encryption, VLAN separation |
| **Acoustic data leak** | Disable unnecessary mics/speakers in secure zones |

**⚔️ Fun Real-World Scenario**

Company ABC still has some old fax lines open. You run WarVOX against their number range and find a modem tone on +92-51-555-0123. You connect, and discover it’s a forgotten **remote access server** using admin/admin.

This is a **real attack surface** in legacy and even modern infrastructure.

**🔄 Challenge Task Ideas**

1. Simulate a number range using VoIP tools like SIP trunk & Asterisk.
2. Run WarVOX in a test environment.
3. Record responses (voicemail vs modem).
4. Attempt to brute-force voicemail box with weak PINs (on a lab setup).
5. Identify which numbers return data tones vs humans.

**🧠 Final Thoughts**

* War Dialing is like **network scanning**, but for **phone systems**.
* Still used in **pen testing**, especially for companies with legacy systems.
* Ties into **VoIP hacking**, **telecom security**, and **acoustic attack research**.
* WarVOX gives a modern twist by using **internet-based calls** (cheap + fast).

L