**Narration Script – Kali Linux Network Security Tools Video**

**0:00 – 0:30 | Intro**

**[On screen: Title card + agenda]**  
\*"Welcome! In this video, we’ll explore some of the most important Kali Linux tools for network security. Everything you’ll see is performed safely inside an isolated lab environment. Please, never scan or test systems without permission.

Here’s our roadmap: Nmap for discovery, Wireshark and tcpdump for traffic analysis, Nikto for web checks, OpenVAS for vulnerability scanning, and Metasploit for safe validation."\*

**0:30 – 2:00 | Discovery with Nmap**

**[On screen: Terminal running Nmap]**  
\*"Let’s start with **Nmap**, one of the most widely used network discovery tools. Here, we’re scanning a target host in our lab.

The results show open ports and the services running on them—for example, SSH on port 22 and HTTP on port 80.

Why does this matter? Every open port is a potential entry point for attackers. By running Nmap, defenders can quickly understand what’s exposed and reduce unnecessary services."\*

**2:00 – 3:30 | Traffic Insight with Wireshark and tcpdump**

**[On screen: Wireshark window + capture]**  
\*"Next, let’s look at **network traffic analysis** using Wireshark.

Here, I’ve captured a simple HTTP login request. Notice how the username and password are visible in plain text. Compare that to HTTPS, where the credentials are encrypted and hidden.

Wireshark allows us to filter traffic—for example, typing http or tcp.port==80 focuses on just web traffic.

For quick command-line captures, we can also use **tcpdump**. With one command, we can capture packets and save them for later review in Wireshark."\*

**3:30 – 4:30 | Web Checks with Nikto**

**[On screen: Nikto terminal output]**  
\*"Now let’s move on to **Nikto**, a web vulnerability scanner.

Here we’re scanning a deliberately vulnerable web app called DVWA. Nikto quickly reports issues like outdated headers or exposed directories.

Not every finding is critical—many are low risk in a lab environment. But in production, even small misconfigurations can become stepping stones for attackers."\*

**4:30 – 5:15 | Vulnerability Scan Snapshot with OpenVAS**

**[On screen: OpenVAS dashboard/report]**  
\*"For a more comprehensive scan, we can use **OpenVAS**, a vulnerability management tool.

This dashboard shows detected vulnerabilities. Here’s one example: a service with a known CVE, or Common Vulnerability and Exposure identifier.

The key takeaway? These scans help organizations map weaknesses to patching and updates, reducing real-world risk."\*

**5:15 – 6:00 | Validation with Metasploit**

**[On screen: Metasploit console]**  
\*"Finally, let’s look at **Metasploit**. While often seen as an exploitation tool, it can also be used safely for validation.

Here we’re using a benign module to grab a service banner. Notice that we confirm the service is exposed, but we stop short of any exploitation.

This approach helps security teams verify whether a vulnerability is truly accessible without causing harm."\*

**6:00 – 6:30 | Wrap-Up**

**[On screen: End card – “Practice only in labs” + resources]**  
\*"To wrap up: Nmap helps us discover hosts and services, Wireshark and tcpdump reveal traffic details, Nikto and OpenVAS highlight weaknesses, and Metasploit validates exposures.

Together, these tools give defenders a clearer picture of their networks, guiding hardening steps like patching, encryption, and service reduction.

If you’d like to learn more, check out resources like the Kali Linux documentation, OWASP, and free lab environments like DVWA.

And remember: always practice safely in isolated labs. Thanks for watching!"\*