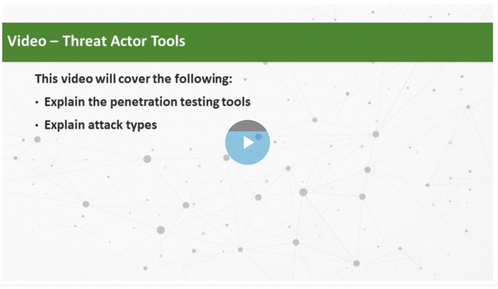
Threat Actor Tools

3.3.1

Video - Threat Actor Tools

As you learned in the previous topic, there are different types of hackers with different motivations for what they do. In this topic, you will learn about some of the tools these individuals use.

Click Play in the figure to view a video about threat actor tools.



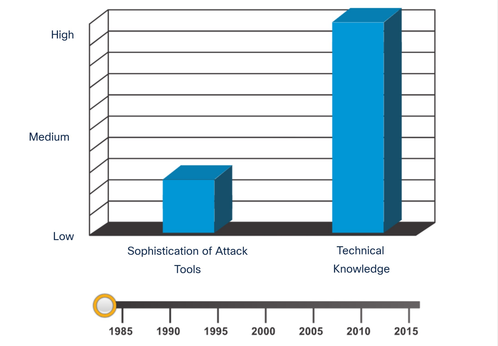
3.3.2

Introduction to Attack Tools

To exploit a vulnerability, a threat actor must have a technique or tool. Over the years, attack tools have become more sophisticated, and highly automated. These new tools require less technical knowledge to implement.

In the figure, drag the white circle across the timeline to view the relationship between the sophistication of attack tools versus the technical knowledge required to use them.

Sophistication of Attack Tools vs. Technical Knowledge



3.3.3

Evolution of Security Tools

Ethical hacking involves many different types of tools used to test the network and keep its data secure. To validate the security of a network and its systems, many network penetration testing tools have been developed. It is unfortunate that many of these tools can be used by black hat hackers for exploitation.

Black hat hackers have also created many hacking tools. These tools are created explicitly for nefarious reasons. White hat hackers must also know how to use these tools when performing network penetration tests.

The table highlights categories of common penetration testing tools. Notice how some tools are used by white hats and black hats. Keep in mind that the list is not exhaustive as new tools are always being developed.

Penetration Testing Tool	Description
Password Crackers	Password cracking tools are often referred to as password recovery tools and can be used to crack or recover a password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
Wireless Hacking Tools	Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, inSSIDer, KisMAC, Firesheep, and NetStumbler.
Network Scanning and Hacking Tools	Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Packet Crafting Tools	These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
Packet Sniffers	These tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.
Rootkit Detectors	This is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.
Fuzzers to Search Vulnerabilities	Fuzzers are tools used by threat actors to discover a computer's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
Forensic Tools	These tools are used by white hat hackers to sniff out any trace of evidence existing in a computer. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.
Debuggers	These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.
Hacking Operating Systems	These are specially designed operating systems preloaded with tools optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, Knoppix, BackBox Linux.
Encryption Tools	Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data. Examples of these tools include VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN, and Stunnel.
Vulnerability Exploitation Tools	These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.
Vulnerability Scanners	These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Examples of tools include Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, and Open VAS.

Note: Many of these tools are UNIX or Linux based; therefore, a security professional should have a strong UNIX and Linux background.

3.3.4

Attack Types

Threat actors can use the previously mentioned attack tools, or a combination of tools, to create attacks. The table displays common types of attacks. However, the list of attacks is not exhaustive as new attack vulnerabilities are constantly being discovered.

Attack Type	Description
Eavesdropping Attack	This is when a threat actor captures and "listens" to network traffic. This attack is also referred to as sniffing or snooping.
Data Modification Attack	If threat actors have captured enterprise traffic, they can alter the data in the packet without the knowledge of the sender or receiver.
IP Address Spoofing Attack	A threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.
Password-Based Attacks	If threat actors discover a valid user account, the threat actors have the same rights as the real user. Threat actors could use that valid account to obtain lists of other users, network information, change server and network configurations, and modify, reroute, or delete data.
Denial of Service Attack	A DoS attack prevents normal use of a computer or network by valid users. A DoS attack can flood a computer or the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.
Man-in-the-Middle Attack	This attack occurs when threat actors have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.
Compromised-Key Attack	If a threat actor obtains a secret key, that key is referred to as a compromised key. A compromised key can be used to gain access to a secured communication without the sender or receiver being aware of the attack.
Sniffer Attack	A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

3.3.5

Check Your Understanding - Threat Actor Tools

Check your understanding of threat actor tools by choosing the BEST answer to the following questions.

1. Which penetration testing tool uses algorithm schemes to encode the data, which then prevents access to the data?

- Packet Sniffers
- (•) Encryption Tools
- Vulnerability Exploitation Tools
- Forensic Tools
- Debuggers

2. Which penetration testing tool is used by black hats to reverse engineer binary files when writing exploits? They are also used by white hats when analyzing malware.

- Packet Crafting Tools
- Rootkit Detectors
- Vulnerability Exploitation Tools
- Forensic Tools
- (•) Debuggers

3. Which penetration testing tool is used to probe and test a firewall's robustness?

- (•) Packet Crafting Tools
- Encryption Tools
- Rootkit Detectors
- Forensic Tools
- Debuggers

4. Which penetration testing tool is used by white hat hackers to sniff out any trace of evidence existing in a computer?

- Fuzzers to Search Vulnerabilities
- Encryption Tools
- Packet Sniffers
- (•) Forensic Tools
- Debuggers

5. Which penetration testing tool identifies whether a remote host is susceptible to a security attack?

- Packet Sniffers
- Encryption Tools
- (•) Vulnerability Exploitation Tools
- Forensic Tools
- Debuggers

Check | Show Me | Reset