/ Network Threats / Threat Actor Tools

Threat Actor Tools

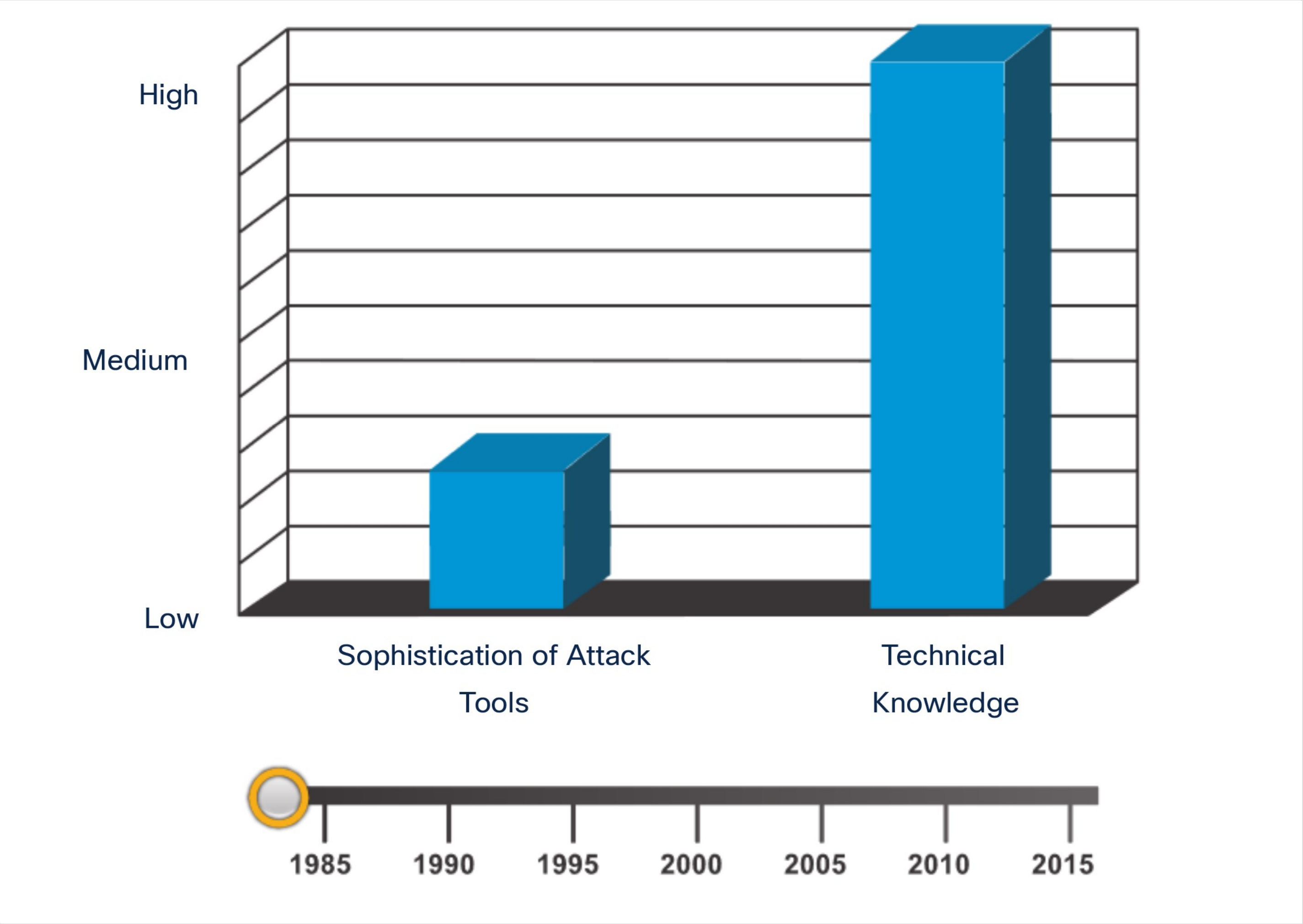
2.2.1

Introduction of 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



2.2.2

Evolution of Security Tools

Ethical hacking involves using many different types of tools to test the network and end devices. To validate the security of a network and its systems, many network penetration testing tools have been developed. However, many of these tools can also

Network Security

be used by threat actors for exploitation.

Threat actors have also created various hacking tools. These tools are explicitly written for nefarious reasons. Cybersecurity personnel must also know how to use these tools when performing network penetration tests.

Explore the categories of common network 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 continually being developed.

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

Categories of Tools	Description
password crackers	Passwords are the most vulnerable security threat. Password cracking tools are often referred to as password recovery tools and can be used to crack or recover the 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 and access the system. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
wireless hacking tools	Wireless networks are more susceptible to network security threats. 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	Packet crafting tools are used to probe and test a firewall’s robustness using specially crafted forged packets. Examples of such tools include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
packet sniffers	Packet sniffers 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	A rootkit detector 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 when attempting to discover a computer system’s security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
forensic tools	White hat hackers use forensic tools to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.
debuggers	Debugger 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

Categories of Tools	Description
	Immunity Debugger.
hacking operating systems	Hacking operating systems are specially designed operating systems preloaded with tools and technologies optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, SELinux, Knoppix, Parrot OS, and BackBox Linux.
encryption tools	These tools safeguard the contents of an organization’s data when it is stored or transmitted. Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Examples of these tools include VeraCrypt, CipherShed, Open SSH, OpenSSL, 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 Tool Kit, 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 these tools include Nipper, Securia PSI, Core Impact, Nessus, SAINT, and Open VAS.

2.2.3

Categories of Attacks

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

It is important to understand that threat actors use a variety of security tools to carry out these attacks.

Category of Attack	Description
eavesdropping attack	An eavesdropping attack is when a threat actor captures and listens to network traffic. This attack is also referred to as sniffing or snooping.
data modification attack	Data modification attacks occur when a threat actor has captured enterprise traffic and has altered the data in the packets without the knowledge of the sender or receiver.
IP address spoofing attack	An IP address spoofing attack is when a threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

Category of Attack	Description
password-based attacks	Password-based attacks occur when a threat actor obtains the credentials for a valid user account. Threat actors then use that account to obtain lists of other users and network information. They could also change server and network configurations, and modify, reroute, or delete data.
denial-of-service (DoS) attack	A DoS attack prevents normal use of a computer or network by valid users. After gaining access to a network, a DoS attack can crash applications or network services. A DoS attack can also 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 (MiTM)	A MiTM 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	A compromised-key attack occurs when a threat actor obtains a secret key. This 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. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the threat actor does not have access to the key.

2.2.4

Check Your Understanding - Classify Cyber Attacks

Check your understanding of types of cyber attacks by answering the following questions.

1. Hackers have gained access to account information and can now login into a system with the same rights as authorized users. What type of attack is this?

○ compromised key

○ password-based

○ DoS

Network Security

○ social engineering

2. In what type of attack can threat actors change the data in packets without the knowledge of the sender or receiver?

○ eavesdropping
○ denial of service
○ data modification
○ IP address spoofing

3. Threat actors have positioned themselves between a source and destination to monitor, capture, and control communications without the knowledge of network users. What type of attack is this?

○ MiTM
○ eavesdropping
○ DoS
○ IP address spoofing

4. A threat actor has gained access to encryption keys that will permit them to read confidential information. What type of attack is this?

○ eavesdropping
○ man-in-the-middle
○ password-based
○ compromised key

5. In what type of attack does a threat attacker attach to the network and read communications from network users?

○ data modification
○ eavesdropping
○ denial of service

Network Security

○ password-based

6. A threat actor constructs IP packets that appear to come from a valid source within the corporate network. What type of attack is this?

○ eavesdropping

○ password-based

○ MiTM

○ IP address spoofing

7. What type of attack prevents the normal use of a computer or network by valid users?

○ DoS

○ password-based

○ MiTM

○ IP address spoofing

Check

Show Me

Reset

2.1 Who is Attacking Our Network?

2.3 Malware