9.2.4 Anti-Malware Software Facts

Malware programs are one of the tools and methods attackers use to gain access to systems. Utilizing anti-malware software is one of the more important steps you can take to protect a system.

This lesson covers the following topics:

- Anti-malware software
- Malware detection methods
- Penetration testing malware
- Malware removal

Anti-Malware Software

Anti-malware is an umbrella term that encompasses several types of programs that prevent malicious software from infecting a system. Anti-malware includes anti-Trojan and antivirus software. Anti-Trojan software is designed specifically to counterattack Trojan horse programs. Anti-Trojan programs utilize scanning methods specifically designed to detect and clear a system of Trojans, rootkits, backdoors, and similar types of damaging software.

Antivirus software is designed specifically to counterattack viruses and worms. Antivirus programs usually have a live monitoring system to immediately detect and stop viruses and worms from running.

Often, the antivirus and anti-Trojan software is combined into a single anti-malware program. Some of the more popular anti-malware programs include:

- Bitdefender
- McAfee
- Webroot
- Symantec Norton 360
- Kaspersky
- AVG
- Avira
- ClamAV (Open Source Program)

The development of an anti-malware program typically follows these steps:

1. Identify unique characteristics of malicious software. Malware programs have unique signatures or characteristics.
2. Write the scanning process. Developers write the program that scans for the identified signatures and characteristics.
3. Update the anti-malware program. Anti-malware software typically stores the signatures and characteristics of known threats in a database that is part of the anti-malware program. Anti-malware software installed at client sites is typically automatically updated to include the database changes to detect and deal with the latest threats.
4. Scan the system. The anti-malware scans the system and identifies any malware found in the system. Anti-malware typically either quarantines or deletes the malware.

Malware databases must be updated regularly. They cannot detect unknown threats.

Malware Detection Methods

Anti-malware software uses a variety of methods to detect malware. Some of the best methods for detecting are described in the following table:

Method	Description
Scanning	A malware scanner is a vital piece of the anti-malware software. The scanner should have live system monitoring to immediately detect malware. The anti-malware database should be updated on a regular basis to ensure that it can protect systems from newly devised threats. If not, the system is vulnerable to attack by new malware.
Integrity checking	Integrity checking establishes a baseline of the system and will alert the user if any suspicious system changes occur. Integrity checkers cannot determine if the change is from malware, a system failure, or some other cause.
Interception	Interception is mainly used against logic bombs and Trojans. If a request for network access or any request that could damage the system is made, the interceptor will notify the user and ask if they wish to approve and continue.
Code emulation	The anti-malware software opens a virtual environment to mimic CPU and RAM activity. Malware code is executed in this environment instead of the physical processor. This method works well against polymorphic and metamorphic viruses.
Heuristic analysis	Heuristic analysis aids in detecting new or unknown malware. The heuristic analysis is based on other known malware. Every malware program has a fingerprint, or signature. If an anti-malware program detects similar code, it marks it as malware and alerts

	the user.

Penetration Testing Malware

Part of a penetration test is checking for malware vulnerabilities. When performing a penetration test, the penetration tester follows a set of steps:

1. Scan for open ports.
2. Scan for running processes.
3. Check for suspicious or unknown registry entries.
4. Verify all running Windows services.
5. Check startup programs.
6. Look through event log for suspicious events.
7. Verify all installed programs.
8. Scan files and folders for manipulation.
9. Verify device drivers are legitimate.
10. Check all network and DNS settings and activity.
11. Scan for suspicious API calls.
12. Run anti-malware scans.

All results and finding must be documented. The anti-malware program documentation should help you determine the next steps if malware is detected.

Malware Removal

If malware is found on a system, follow these steps:

1. Isolate the system from the network immediately.
2. Verify that the anti-malware software is updated and running. If its not, update it and scan the system.
3. Sanitize the system using updated anti-malware software and appropriate techniques.