11.3.4 Evade Honeypots Facts

Honeypots are a security system set up to attract attackers in order to detect, deflect, counteract, or confine unauthorized intrusion attempts on a network. Attackers attempting to break into a target network perform honeypot detection methods using various tools and techniques.

This lesson covers the following topics:

- Honeypot detection techniques
- Honeypot detection

Honeypot Detection Techniques

Keep in mind that if the honeypot can be detected, it can be evaded. Ways to check for a honeypot include:

- Probing the services running on the system.
- Crafting malicious probe packets to scan for services such as HTTP over SSL, SMTP over SSL, and IMAP over SSL. Ports that show a particular service running but deny a three-way handshake connection indicate the potential presence of a honeypot.
- Analyzing network traffic for NetBIOS name server requests. A server without NetBIOS name server requests is usually a honeypot.

If all else fails, you may be able to reach out to the ethical hacking community and learn from the experience of others.

Honeypot Detection

Tools attackers can use to defeat honeypots include multi-proxies, Tors, encryption, and steganography. The following table lists additional detection methods.

Method	Description
Tarpits	Tarpits are an older honeypot technique that can operate at different levels of the OSI model depending on their function. Network tarpits typically use three primary mechanisms: ▪ A means to determine which IP addresses on a subnetwork are unused and, therefore, can be faked. ▪ A strategy to impersonate hosts by responding to TCP, UDP, or ICMP probes destined to fake IP addresses. ▪ A method to hold TCP connections open. Layer 7 tarpits act as security entities and are designed to respond to the incoming packet requests slowly. Layer 4 tarpits use the TCP/IP stack and are effectively employed to slow down the spread of worms, backdoors, and similar malware. Layer 2 tarpits can discover an attack from the same network and the same MAC address for multiple IP addresses.
VMWare	VMware is commercially available virtual machine software that is used to launch multiple instances of operating systems simultaneously on the same physical machine. The first step an attacker takes to detect VMware is to look for specific video cards, display adapters, and network cards because they are not configurable on some VMware. Another VMware detection method is to cause an illegal instruction. As the VMware's exceptions handler checks whether the instruction must be handled by VMware itself or by another handler, the attacker watches the time required to handle an illegal instruction. The time on a host OS system is usually 776mms; it increases to 2530mms when running on VMWare.
Honeyd	Honeyd is a widely used honeypot. It is used to create thousands of honeypots. Honeyd can act as a distraction to potential attackers. For instance, if a network has only three real servers, but one server is running Honeyd, the network will appear to the attacker to be running hundreds of servers. In order to avoid getting caught in the honeypot, the attacker will then have to do more research, possibly through social engineering, in order to determine which servers are real. Either way, the attacker will be slowed down or discovered.
User-Mode-Linux (UML)	User-Mode-Linux is an open-source tool used to create virtual machines and is efficient for deploying honeypots. UML does not use a real hard disk but a fake IDE device called /dev/ubd*. Attackers can detect the UML by examining the /etc/fstab file. Another sign of UML is the usage of the TUN/TAP backend for the network device 0, which is not common on a real system.
Sebek	Sebek is a server/client-based honeypot application that captures rootkits and other malicious malware that hijack read() system calls. An attacker can detect Sebek by measuring execution time of the read() system call. On a system without Sebek, minimal time is around 8225, and the physical is 0.776282.
Snort inline	Snort inline is a modified version of Snort IDS that is capable of packet manipulation. Snort rules must be contained on a single line because the parser does not handle rules on multiple lines. The packet manipulation capability might be spotted if the rule logic appears altered. The attacker would have to be highly knowledgeable of Snort inline and have the ability to sniff the IDS traffic.
Fake AP	Fake AP, or fake access points, are used to create fake 802.11b beacon frames with randomly generated ESSID and BSSID (MAC-address) assignments. Attackers can use many ESSID and BSSID validation tools to detect fake APs.
Bait and	

switch	Bait and switch technology works with IDS software, mainly Snort, to detour suspected malicious traffic into a honeypot that mirrors or closely resembles the real network without the attacker knowing. The attacker carries out their attacks against the honeypot. The attacker will have to be skilled enough to detect the detour or detect the honeypot.