COURSE: SECURITY+ SY0-401

MODULE 3: THREATS AND VULNERABILITIES

Overview

- Explain types of malware
- Summarize various types of attacks

Malware

Virus: A virus is a program or piece of code that runs on your computer without your knowledge. It is designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched. It then attaches to other files, adds its code to the application’s code, and continues to spread.

Types of viruses:

- Boot sector
- Polymorphic
- Macro
- Program
- Stealth
- Multipartite

Malware

Adware: *Advertising-supported software, or adware, is another form of spyware. It is an online way for advertisers to make a sale.*

Spyware: *Undesirable code sometimes arrives with commercial software distributions. Spyware is associated with behaviors such as advertising, collecting personal information, or changing your computer configuration without appropriately obtaining prior consent.*

Malware

Trojan: *Trojans are programs disguised as useful applications. Trojans do not replicate themselves like viruses, but they can be just as destructive. Code hidden inside the application can attack your system directly or allow the system to be com- promised by the code's originator.*

Rootkits: *Rootkits were first documented in the early 1990s. Today, rootkits are more widely used and are increasingly difficult to detect on networks. A rootkit is a piece of software that can be installed and hidden on a computer mainly for the purpose of compromising the system and getting escalated privileges, such as administrative rights.*

Malware

Backdoors: *Backdoors are application code functions created intentionally or unintentionally that enable unauthorized access to networked resources. Many times during application development, software designers put in shortcut entry points to allow rapid code evaluation and testing.*

Logic bomb: *A logic bomb is a virus or Trojan horse designed to execute malicious actions when a certain event occurs or a period of time goes by. For a virus to be considered a logic bomb, the user of the software must be unaware of the payload*.

Attacks

Man-in-the-middle

The man-in-the-middle attack takes place when an attacker intercepts traffic and then tricks the parties at both ends into believing that they are communicating with each other. This type of attack is possible because of the nature of the three-way TCP handshake process using SYN and ACK packets. Because TCP is a connection-oriented protocol, a three-way handshake takes place when establishing a connection and when closing a session.

Attacks

Replay: *In a replay attack, packets are captured by using sniffers. After the pertinent information is extracted, the packets are placed back on the network. This type of attack can be used to replay bank transactions or other similar types of data transfer in the hopes of replicating or changing activities, such as deposits or transfers.*

Spoofing: *Spoofing is a method of providing false identity information to gain unauthorized access. This is accomplished by modifying the source address of traffic or source of information.*

Attacks

Denial-of-Service

The purpose of a denial-of-service (DoS) attack is to disrupt the resources or services that a user would expect to have access to. These types of attacks are executed by manipulating protocols and can happen without the need to be validated by the network.

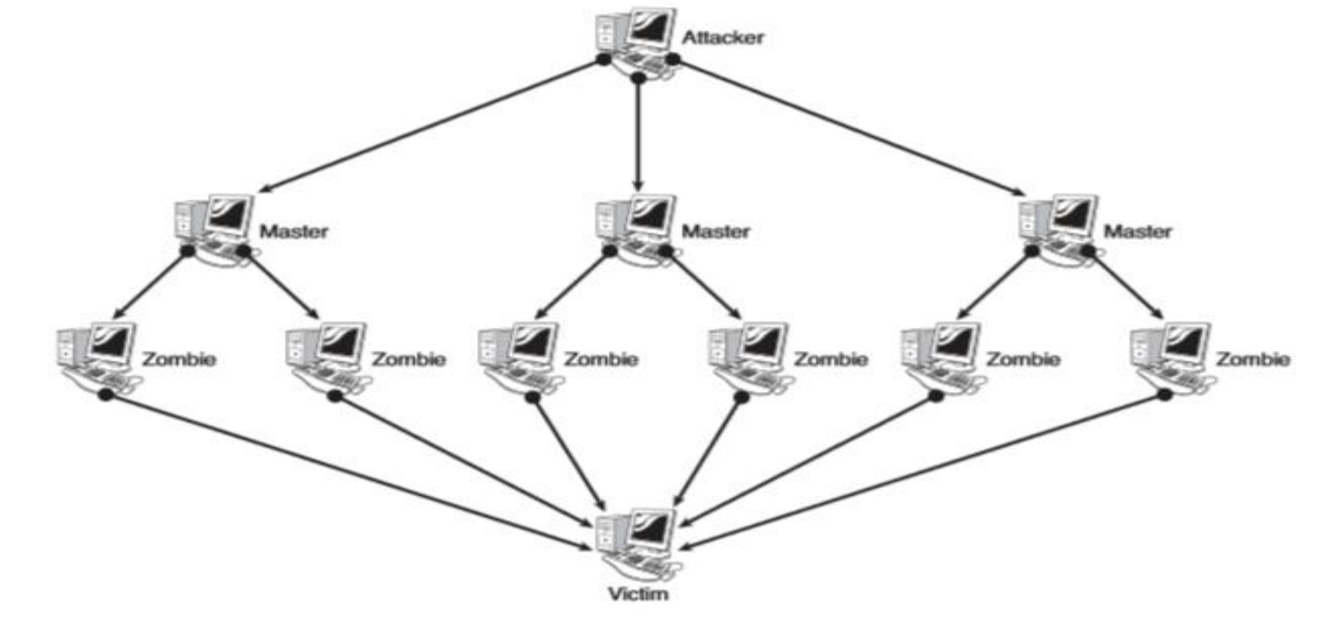
Types of DoS:

- Smurf/smurfing
- Fraggle
- Ping flood
- SYN flood
- Land
- Teardrops
- Xmas Tree

Attacks

Distributed Denial-of-Service

Another form of attack is a simple expansion of a DoS attack, referred to as a distributed DoS (DDoS) attack. Masters are computers that run the client software, and zombies run software. The attacker creates masters, which in turn create a large number of zombies or recruits..

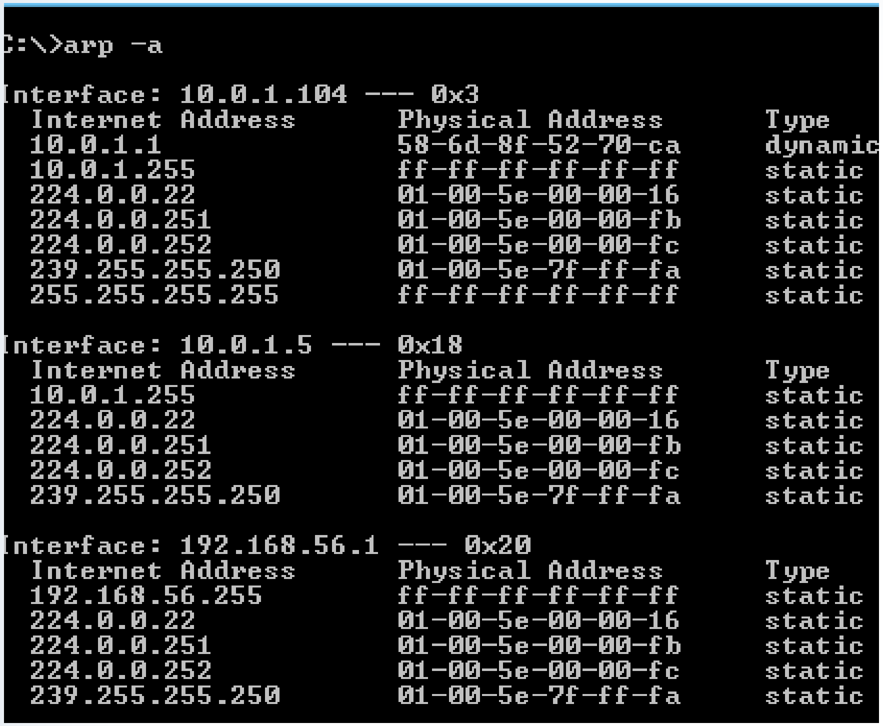


Attacks

DNS Poisoning: DNS poisoning enables a perpetrator to redirect traffic by changing the IP record for a specific domain, thus permitting the attacker to send legitimate traffic anywhere he chooses. This not only sends a requestor to a different website, but also caches this information for a short period, distributing the attack's effect to the server users.

ARP Poisoning: *All network cards have a unique 48-bit address that is hard-coded into the network card. For network communications to occur, this hardware address must be associated with an IP address. Address Resolution Protocol (ARP), which operates at Layer 2 (data link layer) of the OSI model, associates MAC addresses to IP addresses.*

Attacks

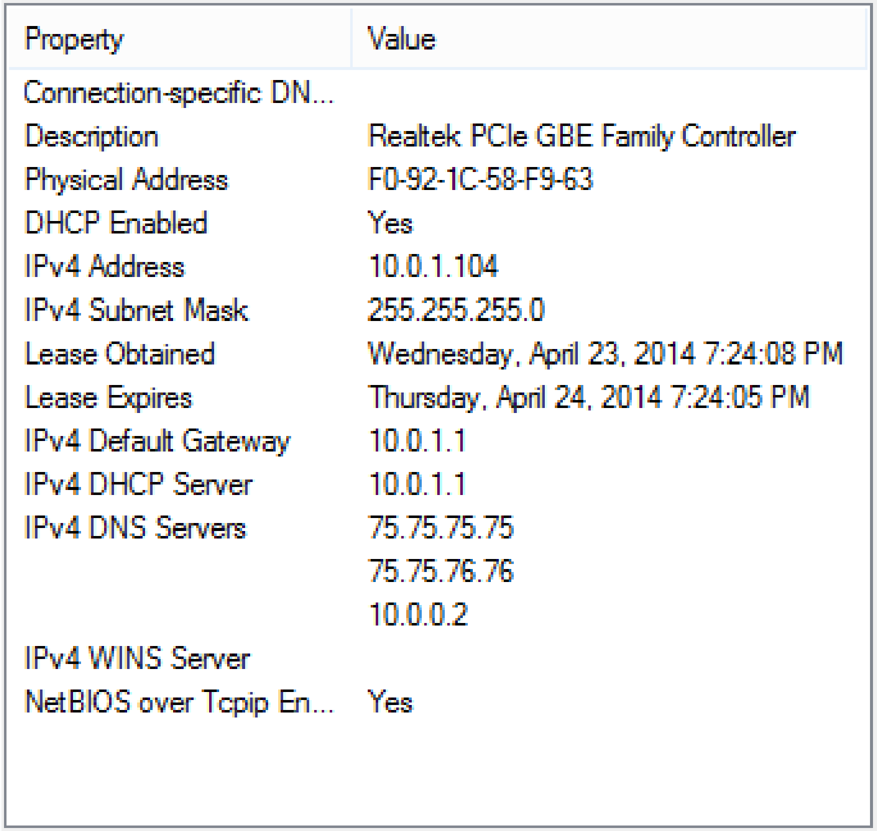


```
C:\>arp -a

Interface: 10.0.1.104 --- 0x3
  Internet Address      Physical Address      Type
  10.0.1.1              58-6d-8f-52-70-ca     dynamic
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.0.1.5 --- 0x18
  Internet Address      Physical Address      Type
  10.0.1.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.56.1 --- 0x20
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```



Property	Value
Connection-specific DN...	
Description	Realtek PCIe GBE Family Controller
Physical Address	F0-92-1C-58-F9-63
DHCP Enabled	Yes
IPv4 Address	10.0.1.104
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, April 23, 2014 7:24:08 PM
Lease Expires	Thursday, April 24, 2014 7:24:05 PM
IPv4 Default Gateway	10.0.1.1
IPv4 DHCP Server	10.0.1.1
IPv4 DNS Servers	75.75.75.75 75.75.76.76 10.0.0.2
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes

Attacks

Privilege Escalation: *Programming errors can result in system compromise, allowing someone to gain unauthorized privileges. Software exploitation takes advantage of a pro- gram's flawed code, which then crashes the system and leaves it in a state where arbitrary code can be executed, or an intruder can function as an administrator.*

Malicious Insider Threat: *Attacks are often thought to be a result of the outside malicious hacker; however, insider threats are a source of many breaches. In many cases, this*

includes employees who have the right intentions but are unaware of or ignore an organization's security policy

Attacks

Spear phishing: *This is a targeted version of phishing. Whereas phishing often involves mass email, spear phishing might go after a specific individual.*

Whaling: *Whaling is identical to spear phishing except for the "size of the fish." Whaling employs spear phishing tactics but is intended to go after high-profile targets such as an executive within a company.*

Vishing: *Also known as voice phishing, the attacker often uses fake caller ID to appear as a trusted organization and attempts to get the individual to enter account details via the phone.*

Attacks

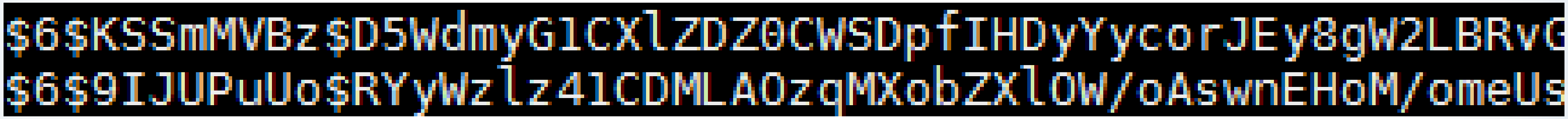
Privilege Escalation: *Programming errors can result in system compromise, allowing someone to gain unauthorized privileges. Software exploitation takes advantage of a pro- gram's flawed code, which then crashes the system and leaves it in a state where arbitrary code can be executed, or an intruder can function as an administrator.*

Spam: *Just like junk mail clogs our regular mailboxes, spam clogs our email boxes. Spam is a term that refers to the sending of unsolicited commercial email. Email spam targets individual users with direct mail messages.*

Attacks

Password Attacks

- Brute force
- Dictionary attacks
- Hybrid
- Birthday attacks
- Rainbow tables



```
$6$KSSmMVBz$D5WdmyG1CXlZDZ0CWSDpfIHDyYycorJEy8gW2LBRvG
$6$9IJUPuUo$RYyWzlz41CDMLA0zqMXobZXl0W/oAswnEHoM/omeUs
```

Attacks

Demonstration

Password Cracking
with
Cain and Able

THANK YOU