Shi Su
shis

14-741 / PIT
11/20/2015

Problem #1 : Running Kerberos and Wireshark

Figure 1: Modules of Gravel

1. Why is the last step (Step 6) optional?
   aaa

2. kinit
(a) Which version of Kerberos are you running?
   aaaa

(b) What is the server name? (AS))

   The buffer fills used in the exploit:

(c) What is the client name? (C)
   aaaaa

(d) What encryption method is being used?
   aaaaa

(e) What is the encrypted value of the ticket TicketTGS in the lecture notes (use only the first 8 hexadecimal digits)?

3. Provide the output of klist. How many tickets are currently valid? For how long are they valid? Who are the principals involved?
   aaaaa

4. AFS
(a) Show the four Kerberos messages that preside over the establishment of the AFS connection.
   aaaaa

(b) What is the name of the AFS server? (V)
   aaaaa

(c) Show that the ticket(TicketTGS) the authentication server gave you is sent to the ticket granting server.

aaaaa

(d) Identify the ticket that the TGS returned to you (T icketV), and show that it is sent to the AFS server when you are trying to create the file 14741-test. Show only the first eight hexadecimal digits of the ticket.

aaaaa

5. Once again, provide the output of klist. How many tickets are currently valid? For how long are they valid? Who are the principals involved?

aaa

Problem #2 : TPM, PHP, and HTTP

1. Explain why this reasoning is completely flawed.

aaaaaa

2. Whether or not the TPM could prevent the attacks from succeeding. If the attacks can be foiled, explain how. If they cannot, state why:

aaaaaa

3. Is the update procedure secure? Justify your answer, by either proving its security, or giving an example of attack against it.

aaaaaa

Problem #3 : Alice and Bob getting married

1. Which security property/ies Bob?s protocol enforces?

aaaaaa

2. Show that Alice?s father is wrong ? in that one of the security properties Bob?s protocol enforces is not maintained anymore.

aaaaaa

3. Bob?s protocol unfortunately has a major problem: It is vulnerable to a replay attack in case the same message X is repeated over time. Enhance the protocol proposed by Bob to prevent this attack.

aaaaaa

4. Enhance the protocol proposed by Bob to provide the freshness property.

aaaaaa

Problem #4 : Finding open ports and bypassing firewalls

1. Suggest a technique to exhaustively determine all the open TCP ports on a given host you want to attack.

Assume that we know the target's ip address and it is not behind a firewall.

1. Craft a TCP packet with destination port set to target port and only SYN flag set.
2. Send it to the target host
   - If host replies SYN-ACK, mark the target port as open, and send a RST packet to host to close the half-open connection and avoid SYN flooding.
   - If host replies RST, then the target port is closed.
3. Repeat previous steps for all 65535 ports.

2. Harry Bovik claims the attack consumes a lot of memory on the attacker?s side. Is he right or not? Why?

No, with SYN scan attacker doesn't need to maintain any open or half open connection, it only sent a SYN packets, which is lightweight, to each port on target server and check the responses, so the memory consumption should be low.

3. Suggest an alternative method to determine all the open TCP ports on the host you want to attack.

Assume that we know the target's ip address and it is not behind a firewall.

1. Craft a TCP packet with destination port set to target port and only FIN flag set.
2. Send it to the target host
   - If no reply from host for a certain amount of time, send the packet again. Repeat the process for several time, if no reply ever come back, then mark the port as open.
   - If host reply RST, then the target port is closed.
3. Repeat previous steps for all 65535 ports.

4. Harry Bovik tells you that neither of these attacks work to determine all open ports on a packet filtering layer-3 firewall. Why is he right?

Packet filtering firewalls have filter rules to determine which packet is allowed to pass, based on the information about packet protocol, ip address, port number and packet type. It checks every packet trying to pass through it against those filter rules, the offending packet will be dropped. For example if an attacker trying to send a packet to a filtered port, while the source ip address, port and protocol is not specified in the firewall's ACL, then the probe packet will be denied and dropped. So if some ports are filtered by the firewall, we can know they are filtered but cannot tell whether they are open or not.

5. Suggest an extension to either of the above attacks that allows to figure out open ports on a firewall.

Assume that we know the target's ip address and the firewall will not queue and reassemble ip fragments. Based on SYN scan, we can break the probe packet into small ip fragments, so that the TCP header will be split into different packets, so make it will make it harder for firewall to apply filter rules on them.