Exam Network Security

(192654000 & 201000086)

9 November 2012

- This is an open-book exam: you are allowed to use the book ("Network Security Essentials" by Stallings), the papers that were distributed through Blackboard, and copies of the lecture slides. Furthermore, you are allowed to use a (paper) dictionary.
- Use of electronic devices, such as calculators, laptops, notebook computers, PDAs, mobile phones, iPads, e-readers, etc. is not allowed. ***Please remove any such devices from your desk, now!***
- Although the questions are only written in English, you are allowed to answer in either English or Dutch.
- This exam consists of 8 problems on 6 pages (including this page).
- Because different lecturers will grade your answers, you should write your answers on three different sheets of paper. Label these sheets with an 'A', 'B' and 'C' , and write the answer to each problem on the right sheet.

Continued on next page...

WRITE ANSWERS ON SHEET A

1. WLAN security [A]

(a) Draw a diagram to illustrate TKIP (WEP2) receiving (decryption) that matches the diagram on TKIP (WEP2) sending (encryption) given on slide 43 (from slides used for Lecture 2)!

Consider: (i) Wireless Local Access (IEEE 802.11) network, (ii) an attacker can receive many cipher texts of packets.

(b) Assuming WEP is used:
- Describe at least one attack that can be implemented by an attacker to calculate at least one plaintext.
- List and describe all the assumptions needed to successfully perform this attack.

(c) Assuming WPA is used:
- Describe at least one attack that can be implemented by an attacker to calculate at least one plaintext.
- List and describe all the assumptions needed to successfully perform this attack.

(d) Assuming WPA2 is used:
- Describe at least one attack that can be implemented by an attacker to calculate at least one plaintext.
- List and describe all the assumptions needed to successfully perform this attack.

2. RADIUS/DIAMETER [A]

(a) Give and explain at least three advantages of using RADIUS in the IEEE 802.11i RSN mode instead of using DIAMETER!

(b) Give and explain at least three advantages of using DIAMETER in the IEEE 802.11i RSN mode instead of using RADIUS!

(c) Give at least one reason of why the DIAMETER server is able to initiate DIAMETER protocol messages to request a session termination. Explain and motivate your answer.

(d) List at least two differences and at least two similarities between the use of proxies in RADIUS and DIAMETER! Motivate/explain these similarities and differences.

Continued on next page...

WRITE ANSWERS ON SHEET B

3. IPSec

B

(a) Assume a company has multiple branches, which are connected via the Internet. Since communication must be secure, the company uses IPSec gateways to connect all branches to the Internet. Between the gateways, IPSec is used in tunnel mode. In such scenario IPSec can be used for authentication. The question is now what is being authenticated in this scenario. Is it the end user (person)? Is it the computer that is used by the end user? Is it the security gateway that connects a specific branch to the Internet? Is it the company itself? Or is it something else? Explain!

(b) Explain the mechanism IPSec is using to detect replay attempts.

(c) An interesting difference between IPSec-AH and IPSec-ESP is that for IPSec-AH the Message Authentication Code (MAC) algorithm includes the source and destination IP addresses, whereas the MAC algorithm for IPSec-ESP does not cover both IP addresses. Still IPSec-AH as well as IPSec-ESP claim to ensure authentication. How is this possible?

4. SSL/TLS and SSH

B

(a) Is it possible that, at a certain moment, a SSH channel exist, although there is no SSH transport connection? Explain!

(b) The TLS handshake protocol uses a key exchange algorithm such as Diffie-Hellman. Is it necessary to run such algorithm before every new TLS connection? Explain!

(c) Assume a company defines as policy that all keys used within the SSL/TLS protocol should have a minimum key-length of 512 bits. What do you think of such a policy?

Continued on next page...

WRITE ANSWERS ON SHEET C

5. Web attacks

C

(a) Consider a web page that allows the user to select his/her preferred language. It's a great web page! You can provide a default language in the URL:

```
...
Select your language:

<select><script>

document.write("<OPTION value=1>"
+document.location.href.substring(document.location.href.indexOf("default="
)+8)+"</OPTION>");
document.write("<OPTION value=2>English</OPTION>");
document.write("<OPTION value=3>French</OPTION>");

</script></select>
...
```

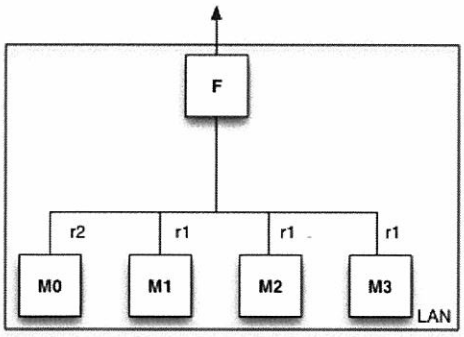
Show how to perform an XSS attack on this page (`document.location.href` contains the current URL).

(b) Describe how you could use XSS on a server X to perform a Distributed DoS attack against a machine Y hosting a database. Assume that there are no bugs on Y that can be exploited.

6. Firewalls

C

The hosts M0, M1, M2, and M3 are placed behind a (bridging) firewall F, as indicated in the figure. F is an IP packet filtering firewall. The firewall limits the rate of the hosts M1, M2 and M3 to r1 Mbps, and the rate of M0 to r2 Mbps. Suppose r2 > r1.



(a) Assume M3 starts crafting IP packets with source IP the IP of M0. Check the following claims (for each claim a simple true/false answer is sufficient):

1) M3 can send with rate r2.
2) M3 can launch a SYN Flooding DoS attack towards an external server.
3) M3 can download a rootkit from an external server F.
4) M3 can receive the traffic destined to M0.

Continued on next page...

(b) Assuming that the MAC addresses are not stolen, how can you prevent spoofed IP packets to leave your network through F? Check the following claims (for each claim a simple true/false answer is sufficient):

1) You cannot prevent it.
2) You must extend the firewall rules to include MAC addresses.
3) You must use static ARP tables on the firewall.
4) You must extend the firewall rules to include MAC addresses AND you must use static ARP tables on the firewall.

7. Intrusion Detection

C

(a) A security administrator is looking to set-up an especially secure network. To this end, he wants to deploy both an Intrusion Detection System and a Firewall. He is considering the following deployment schemes: i) Deploy the IDS behind the edge firewall; ii) Deploy the IDS in front of the edge firewall;
Can you name the pros and cons of both setups?

(b) For each of the 6 options shown in the table below, give one example of attack that can be detected with the considered type of IDS. For each attack, briefly explain how and/or why.

	Host-based IDS	**Network-based IDS (packet-based)**	**Network-based IDS (flow-based)**
Signature-based IDS	Option A1	Option A2	Option A3
Anomaly-based IDS	Option B1	Option B2	Option B3

(c) Suppose that you have been hired to design an IDS.

- The given requirements are that i) the IDS will detect widely spread Botnets, and ii) the IDS is flow-based.
  How would your solution look like and why?
- Can you name a different monitoring technique that would allow observing botnets activities? Explain why.

8. SQL Injection

C

Consider an "Active Server Pages" (ASP) login page that accesses a SQL Server database. The page displays a form to retrieve the following information from a user:

```
Username:
Password:
```


Continued on next page...

The code for "process_login.asp" is:

```
[some previous code]

<%@LANGUAGE = JScript %>
<%

function trace( str )
{
  if( Request.form("debug") == "true" )
    Response.write( str );
}

function Login( cn )
{
  var username; var password;

  username = Request.form("username");
  password = Request.form("password");
  var rso = Server.CreateObject("ADODB.Recordset");
  var sql = "select * from users where username = '" +
      username + "' and password = '" + password + "'";
  trace( "query: " + sql );
  rso.open( sql, cn );
  if (rso.EOF)
  {
    rso.close();
%>
<FONT Face='tahoma' color='cc0000'>
<H1>
<BR><BR>
<CENTER>ACCESS DENIED</CENTER>
</H1>
</BODY>
</HTML>
<%
   Response.end
   return;
}
else {
  Session("username") = "" + rso("username");
%>
<FONT Face='tahoma' color='00cc00'>
<H1>
<CENTER>ACCESS GRANTED</CENTER>
<BR> <BR>
Welcome,
<%
  Response.write(rso("Username"));
  Response.write( "</BODY></HTML>" );
  Response.end
  }

[some other code]
```

Answer the following questions:

(a) Which is the critical code for SQL injection?

(b) What happens if the attacker injects the following code in the `Username` form field?

```
Username: ' or 1=1--
```

(c) List two examples of mitigation techniques that can secure the considered application.

End of this exam!