CSE543/Fall 2006 - Quiz

Thursday, November 16, 2006 — Professor Trent Jaeger

Please read the instructions and questions carefully. You will be graded for clarity and correctness. You have 25 minutes to complete this quiz, so focus on those questions whose subject matter you know well. Write legibly and check your answers before handing it in.

Short Answer - some will be one or two words – no more than 3 sentences

1. (*3pts*) Why do *mutable fields* present problems for IPsec and *in which modes* do these problems manifest?

   answer: They are fields *in the IP header* that change on a *hop-by-hop basis* to *complicate integrity verification in AH.*

2. (*3pts*) What is a *client puzzle*? Why might a client puzzle help protect server processing from DDoS attacks?

   answer: A client puzzle is *a challenge provided by a server* upon a client request that is *much harder for clients to solve than for servers to verify.* If the *server request processing time is much greater than the puzzle verification time*, then client puzzles may be useful.

Long Answer - no more than 2 paragraphs

3. (*7pts*) What is the *most important reason* that Kerberos single signon provides better client authentication than the Passport single signon mechanism? Why is *this reason most important*?

   answer: Kerberos has an *authenticator* that contains a secret session key that both the client and server must know before a session with a new server is established, whereas the Passport only uses cookies (known by only the Passport server) and a secure communication channel between the Passport server and the application server.

   In Passport, the client need not prove knowledge of a secret prior to opening a session with a new server. Therefore, an attacker need only steal the Passport cookies of another user to signon to a new server as that user.

4. (*7pts*) DNS is a vulnerable network protocol. Identify one attack against DNS by an active network attacker. How does DNSSEC protect against this attack?

   answer: There are several attacks. An example is that an active attacker can submit a phony DNS response to a client's query if it knows the UDP port used by the client and the DNS sequence number. DNSSEC uses signed messages from a known root for these responses, so they cannot be forged by an active attacker.

Word Problems - take your time and answer clearly and completely.

5. (*10pts*) Suppose you have a network as defined above. Create stateless firewall policies for the following network firewalls FW1 and FW2. Create only as as many rules as you need (use the minimum) in the order they should be evaluated.

   (a) Unless otherwise specified, all traffic should be denied.

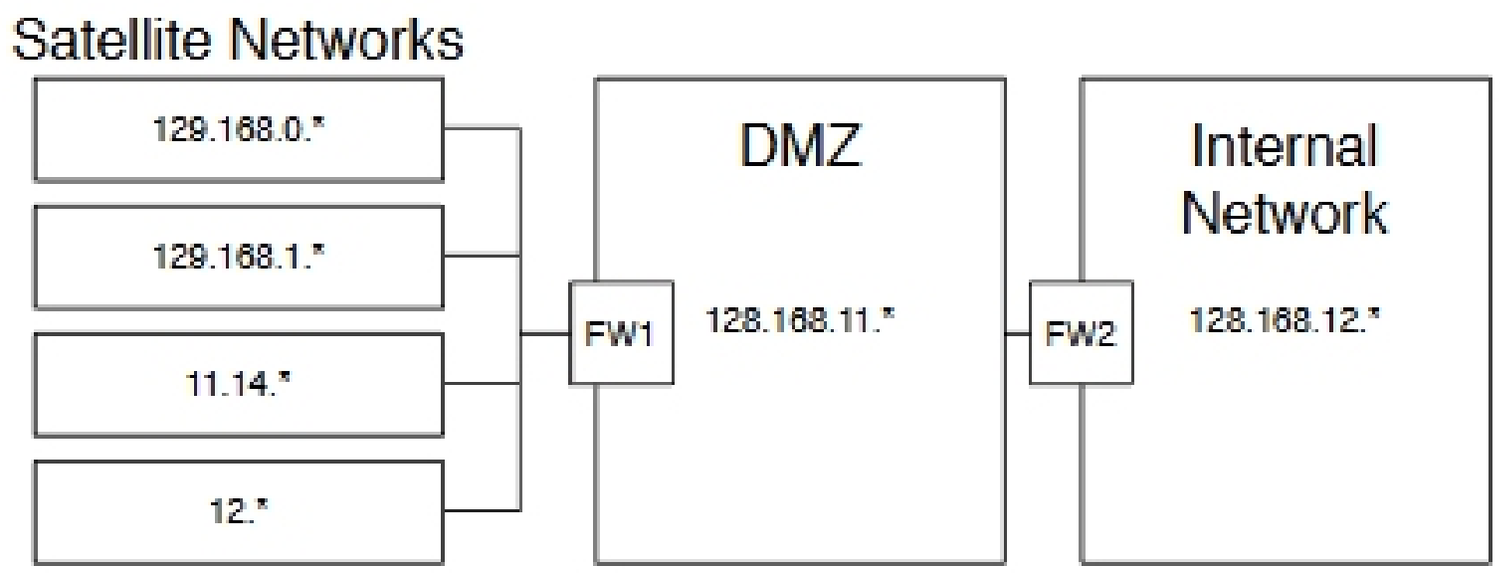
   (b) The satellite networks should be able to communicate with any DMZ host over http (port 80).

   (c) Satellite networks 11.14 should be able to speak with 128.168.11.4 over ssh (port 22).

   (d) Nobody outside the DMZ should be able to contact the internal network.

(e) Any host in the DMZ should be allowed to talk to the internal network to vsftp (port 21).

(f) Any host in the internal network should be allowed to talk to the DMZ to vsftp (port 21).



FW1				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny

FW2				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny

answer:

FW1				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny
129.168.0.*	*	128.168.11.*	80	A
129.168.1.*	*	128.168.11.*	80	A
11.14.*	*	128.168.11.*	80	A
12.*	*	128.168.11.*	80	A
128.168.11.*	80	129.168.0.*	*	A
128.168.11.*	80	129.168.1.*	*	A
128.168.11.*	80	11.14.*	*	A
128.168.11.*	80	12.*	*	A
11.14.*	*	128.168.11.4	22	A
128.168.11.4	22	11.14.*	*	A
*	*	*	*	D

FW2				
Src Addr	Src Port	Dest Addr	Dest Port	Accept/Deny
128.168.12.*	*	128.168.11.*	21	A
128.168.11.*	21	128.168.11.*	*	A
128.168.11.*	*	128.168.12.*	21	A
128.168.12.*	21	128.168.11.*	*	A
*	*	*	*	D