

Data Loss Prevention

5. Database and Web Loss

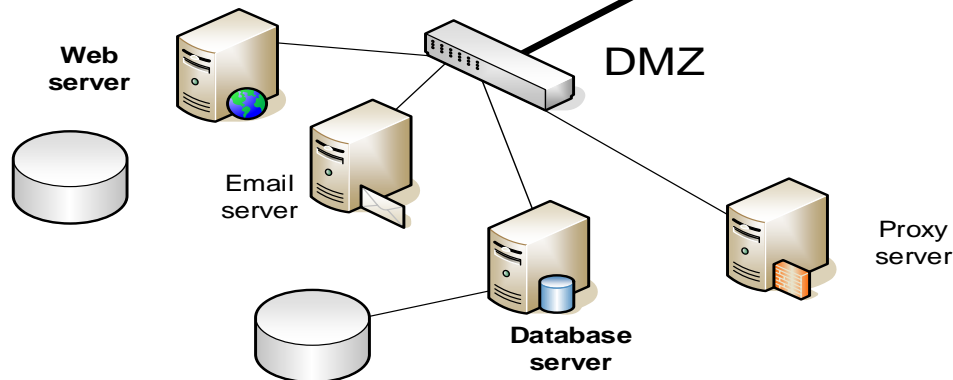
- SQL Misuse.
- Cross-site Scripting (XSS).
- Web scanning.
- Honeypots.



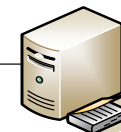
<http://asecuritysite.com/dlp>

OWASP Top 10

- A1-Injection
- A2-Broken Authentication and Session Man
- A3-Cross-Site Scripting (XSS)
- A4-Insecure Direct Object References
- A5-Security Misconfiguration
- A6-Sensitive Data Exposure
- A7-Missing Function Level Access Control
- A8-Cross-Site Request Forgery (CSRF)
- A9-Using Components with Known Vulnerabilities
- A10-Unvalidated Redirects and Forwards



Domain name
server



Internet

Firewall

Router

Intrusion
Detection
System

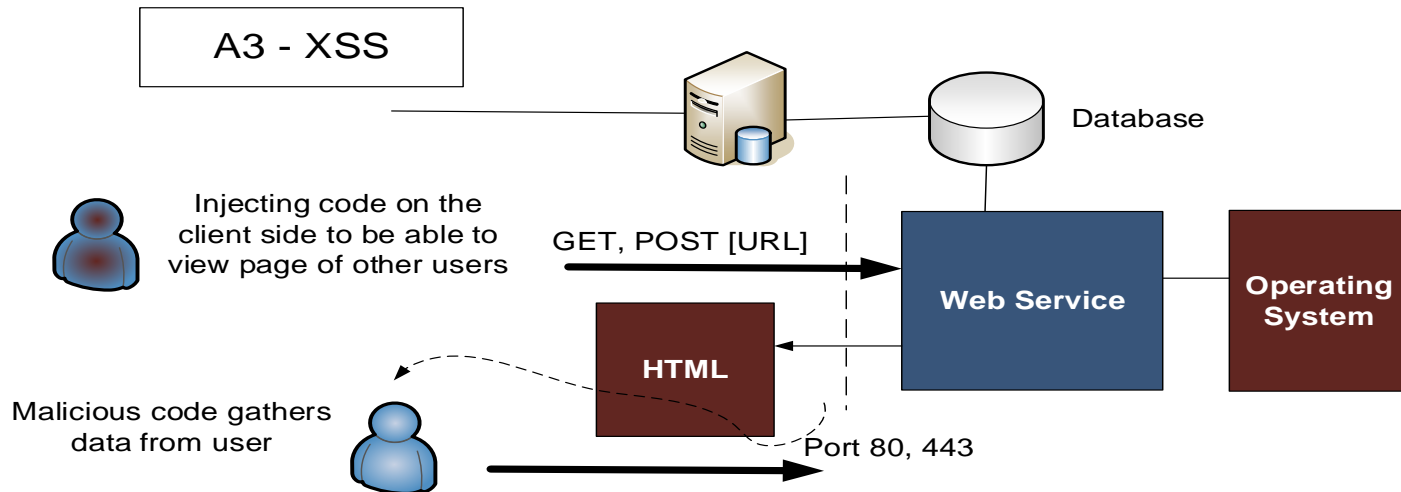
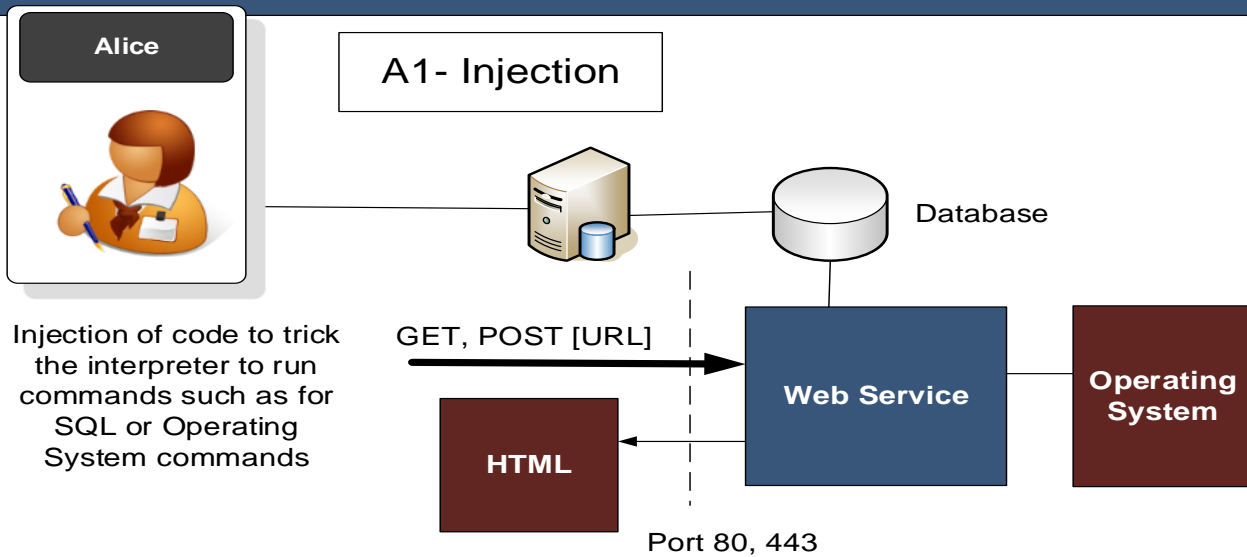
Proxy
server



Alice



SQL and Web

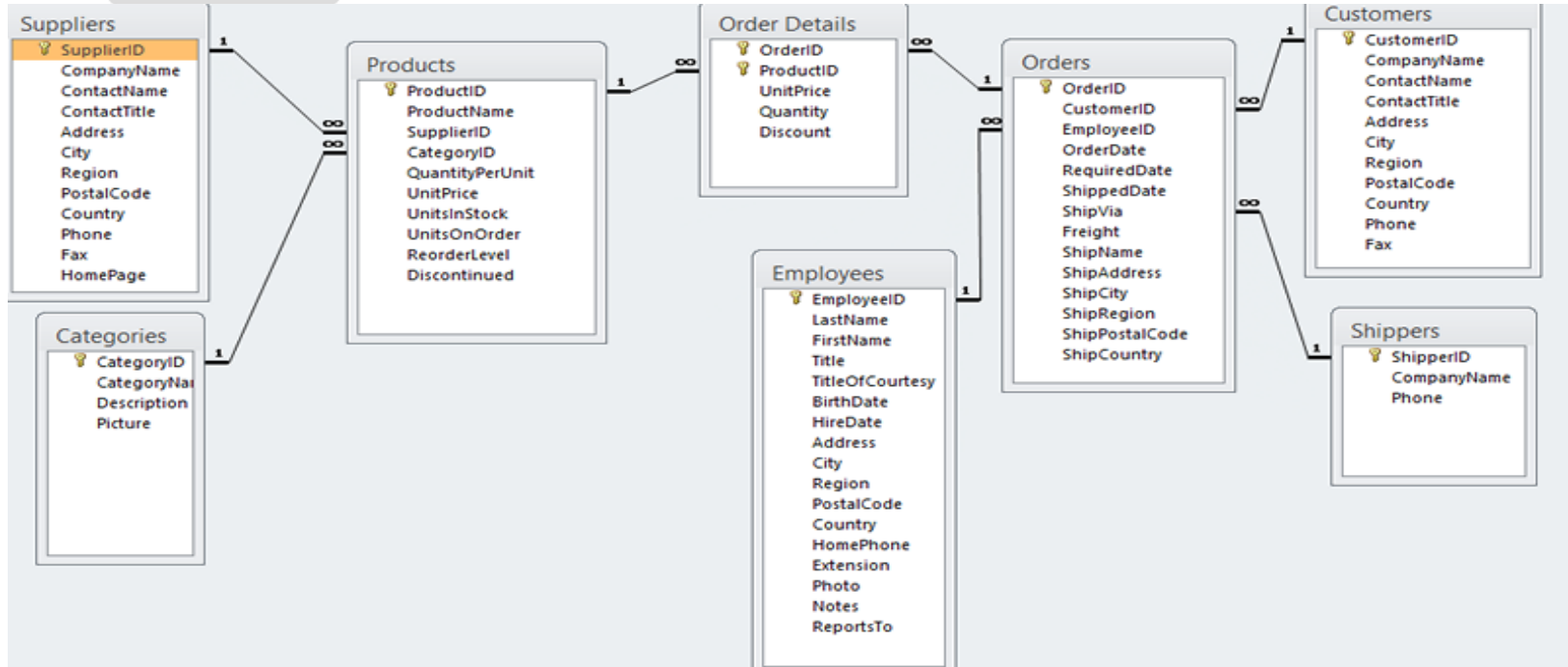
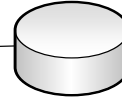


Data Loss Detection/ Prevention



SQL

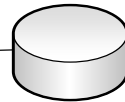
Supplier ID	Company Name	Contact Name	Contact Title	Address	City	Region	Postal Code	Country
1	Exotic Liquids	Charlotte Cooper	Purchasing Manager	49 Gilbert St.	London		EC1 4SD	UK
2	New Orleans	Cajun Delights	Order Administrator	P.O. Box 78934	New Orleans	LA	70117	USA



Alice



ID	FirstName	Surname	FullAddress	Test 1	Test 2	Gender	Age
1	Fred	Smith	10 Fake Street	10	20	M	30
2	Bert	Smith	1 Round Lane	30	40	M	40
3	Bob	Malcolm	5 Square Road	100	30	M	22
4	Eve	Almond	11 Full Lane	45	40	F	56
5	Freddy	Smith	111 Edinburgh	50	50	M	43



```
SELECT * FROM db1
SELECT * FROM db1 ORDER BY Surname
SELECT * FROM db1 ORDER BY Surname DESC
SELECT * FROM db1 ORDER BY Age
SELECT * FROM db1 ORDER BY Gender
SELECT FirstName FROM db1 WHERE (Gender='M')
SELECT Surname FROM db1 WHERE (Gender='M')
SELECT TOP 1 (Surname) FROM db1 WHERE (Gender='M')
SELECT Top 1 (Surname) FROM db1 WHERE (Gender='M') ORDER BY Surname DESC
SELECT Max(Age) FROM db1
SELECT Min(Age) FROM db1
SELECT FirstName FROM db1 WHERE (Surname='Smith' OR Surname='Almond')
SELECT Avg([Test 1]) FROM db1
SELECT Avg([Test 1]) FROM db1 WHERE (Age>30)
SELECT Sum([Test 1]) FROM db1
SELECT Sum([Test 1]) FROM db1 WHERE (Age>30)
SELECT Count(FirstName ) FROM db1 WHERE (Age<30)
SELECT Count(FirstName ) FROM db1 WHERE (Age=30)
SELECT FirstName,Surname FROM db1
SELECT DISTINCT Surname FROM db1
SELECT FirstName,Surname,Age,[Test 1] FROM db1 WHERE (Gender='M')
SELECT FirstName,Surname,[Test 1],[Test 2] FROM db1 WHERE (Gender<>'M')
SELECT FirstName,Surname,[Test 1],Age FROM db1 WHERE Age BETWEEN 10 AND 50
SELECT FirstName,Surname,[Test 1],Age FROM db1 WHERE Age IN (22,56,33)
SELECT FirstName,Surname,[Test 1],Age FROM db1 WHERE Surname LIKE 'Sm%'
SELECT FirstName,Surname,[Test 1],Age FROM db1 WHERE Surname LIKE '[AaSsUu]%'
SELECT FirstName,Surname,[Test 1],Age FROM db1 WHERE Surname NOT LIKE 'Sm%'
SELECT Gender,AVG([Test 1]) FROM db1 GROUP BY Gender
SELECT FirstName,Surname,[Test 1] from db1 where Surname in ( 'Smith', 'Almond') ORDER BY Surname
```

Basic commands:

- SQL SELECT
- SQL DISTINCT
- SQL WHERE
- SQL AND OR
- SQL IN
- SQL BETWEEN
- SQL Wildcard
- SQL LIKE
- SQL ORDER BY
- SQL GROUP BY
- SQL HAVING
- SQL ALIAS
- SQL AS
- SQL SELECT UNIQUE
- SQL INSERT INTO
- SQL INSERT INTO SELECT
- SQL UPDATE
- SQL DELETE FROM

Functions:

- AVG: Average of the column.
- COUNT: Number of records.
- MAX: Maximum of the column.
- MIN: Minimum of the column.
- SUM: Sum of the column.

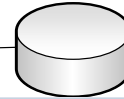
String:

- SQL CAST
- SQL CONVERT
- SQL CONCATENATE
- SQL SUBSTRING
- SQL INSTR
- SQL TRIM
- SQL LENGTH
- SQL REPLACE
- SQL TO_DATE

Alice



TCP Port 3306



mysql01.pcap [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 0 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.254	192.168.0.254	TCP	74	56162 > mysql [SYN] Seq=0 Win=32792 Len=0 MSS=16396 SACK_PERM
2	0.000046	192.168.0.254	192.168.0.254	TCP	74	mysql > 56162 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=16396
3	0.000077	192.168.0.254	192.168.0.254	TCP	66	56162 > mysql [ACK] Seq=1 Ack=1 Win=32832 Len=0 TSval=1578561
4	0.000265	192.168.0.254	192.168.0.254	MySQL		
5	0.000286	192.168.0.254	192.168.0.254	TCP		
6	0.000559	192.168.0.254	192.168.0.254	MySQL		
7	0.000583	192.168.0.254	192.168.0.254	TCP		
8	0.000695	192.168.0.254	192.168.0.254	MySQL		
9	0.000893	192.168.0.254	192.168.0.254	MySQL		
10	0.001051	192.168.0.254	192.168.0.254	MySQL		

Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 192.168.0.254 (192.168.0.254), Dst: 192.168.0.254 (192.168.0.254)
Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 56162

0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 3c 00 00 40 00 40 06 b7 6f c0 a8 00 fe c0 a8
0020 00 fe 0c ea db 62 cd 34 95 d7 cc d8 bb 4e a0 12
0030 80 00 77 cd 00 00 02 04 40 0c 04 02 08 0a 00 f0
0040 4d e8 00 00 00 00 00 00 00 00 00 00 00 00 00

Ready to load or capture Packets: 57 · Display... Profile: Default

Follow TCP Stream

Stream Content

```
4...  
5.0.54.A...>  
$4uth...!>612IWZ>fhwx.  
>.....!.....tfoerste...mub....j.A#j..1A....  
select @@version_comment limit  
1.....def....@@version_comment..!K.....Gentoo  
Linux mysql-5.0.54.....SELECT DATABASE().....def...  
DATABASE  
(...!f.....def...test.....show  
databases.....1.....def...SCHEMATA..Database.SCHEMA_NAM  
E..!.....information_schema.....test.....  
show tables.....9.....def...TABLE_NAMES..Tables_in_test  
TABLE_NAME..!.....def...agent.....agent.*.....de  
f.test.agent.agent.id.id.?......B.....0.....def.test.agent.agent.cust  
om_data1.custom_data1..!h.....def.test.agent.agent.custom_d  
ata2.custom_data2..!h.....def.test.agent.agent.custom_data  
3.custom_data3..!h.....create table foo (id BIGINT  
(10 ) UNSIGNED NOT NULL AUTO_INCREMENT PRIMARY KEY, animal VARCHAR  
(64) NOT NULL, name VARCHAR(64) NULL DEFAULT NULL) ENGINE =  
MYISAM.....7.....insert into foo (animal, name) values ("dog",  
"Goofy").....insert into foo (animal, name) values  
("cat", "Garfield").....select * from foo.....  
$.....def.test.foo.foo.id.id.?.  
.....#B.....def.test.foo.foo.animal.animal..!  
.....def.test.foo.foo.name.name..!.....1.dog.Goof  
y.....2.cat.Garfield.....delete from foo where name like '%  
00%'.....delete from foo where id =  
1.....select count(*) from foo.....def....count  
(*)
```

Entire conversation (1853 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Filter Out This Stream Close

MySQL

mysql01.pcap [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `frame matches /^(%27)(\")(\\-)(%23)(#)/ix` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
10	0.001051	192.168.0.254	192.168.0.254	MySQL	162	Response
36	47.16829	192.168.0.254	192.168.0.254	MySQL	109	Request Query

Frame 10: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)

- Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
- Internet Protocol Version 4, Src: 192.168.0.254 (192.168.0.254), Dst: 192.168.0.254 (192.168.0.254)
- Transmission Control Protocol, Src Port: mysql (3306), Dst Port: 56162 (56162), Seq: 68, Ack: 104, Len: 96
- MySQL Protocol
 - Packet Length: 1
 - Packet Number: 1
 - Number of fields: 1
- MySQL Protocol
 - Packet Length: 39
 - Packet Number: 2
 - Catalog: def
 - Database:
 - Table:
 - Original table:
 - Name: @@version_comment
 - Original name:
 - Charset number: utf8 COLLATE utf8_general_ci (33)
 - Length: 75
 - Type: FIELD_TYPE_VAR_STRING (253)
 - Flags: 0x0001

0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 08E.
0010 00 94 4b 59 40 00 40 06 6b b6 c0 a8 00 fe c0 a8 ..kY@. k.....
0020 00 fe 0c ea db 62 cd 34 96 1b cc d8 bb b5 80 18b.4.....
0030 02 00 83 d3 00 00 01 01 08 0a 00 f0 de 8f 00 f0t.....
0040 4a 8f 01 00 00 01 01 77 00 00 02 02 64 65 66 00def.....

Ready to load or capture Packets: 57 · Display... Profile: Default

Data Loss Detection/ Prevention



Code Injection

Alice



http://asecuritysite.com/database/db?word=SELECT%20*%20FROM%20db1

GET

```
GET /mutillidae/index.php?page=user-info.php&username=bill&password=fred&user-info-php-submit-button=View+Account+Details HTTP/1.1
Host: 10.200.0.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Icedweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=2; PHPSESSID=2858f079ae6ead4f60e4d2c8ec4e7a2
Connection: keep-alive
If-Modified-Since: Sun, 25 May 2014 22:32:38 GMT
```

POST

<http://asecuritysite.com/database>

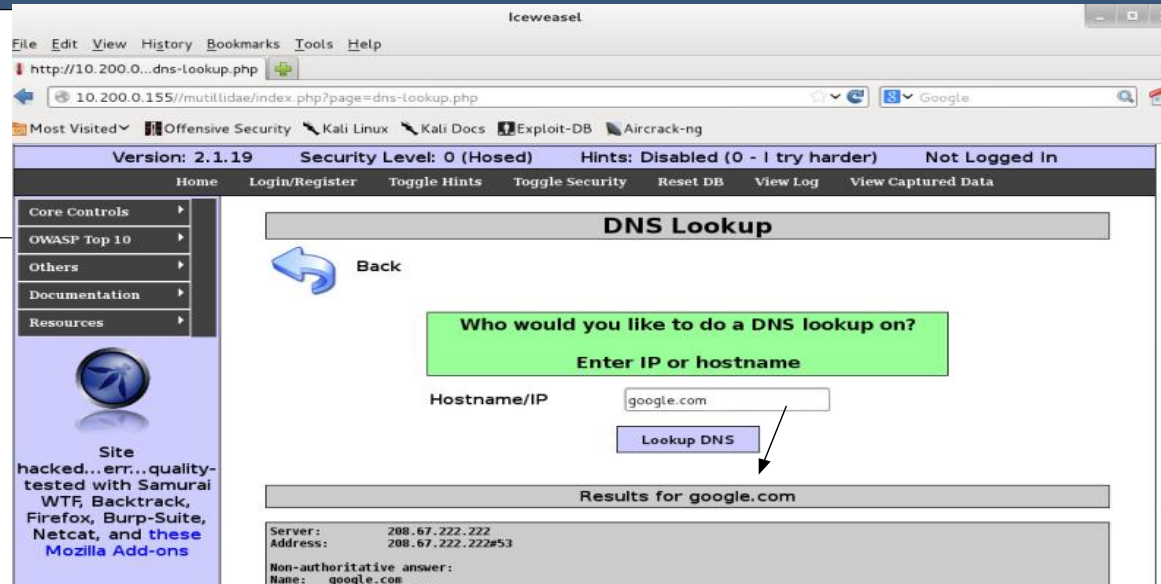
```
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 10.200.0.47
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:18.0) Gecko/20100101 Firefox/18.0 Icedweasel/18.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.200.0.47/mutillidae/index.php?page=dns-lookup.php
Cookie: PHPSESSID=2858f079ae6ead4f60e4d2c8ec4e7a2
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
target_host=google.com&dns-lookup-php-submit-button=Lookup+DNS
```

<form>

</form>

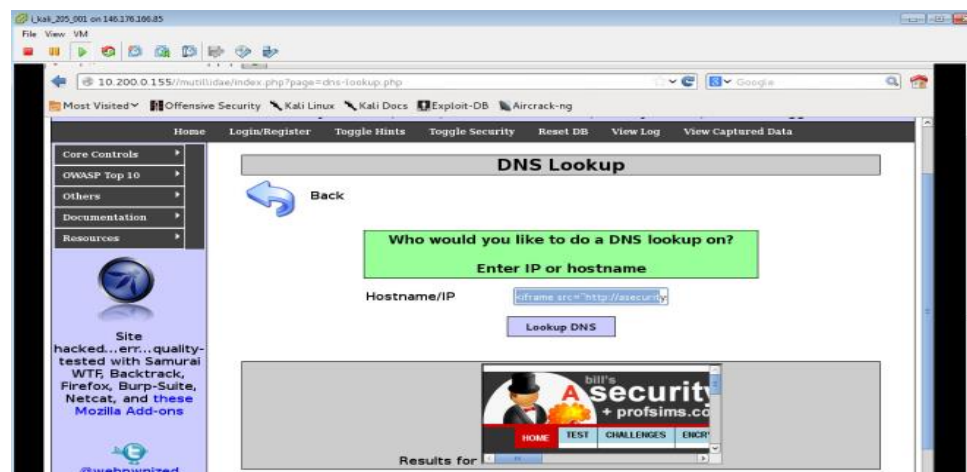
URL Posting

Alice



Code Injection

<iframe> Injection



Code Injection

Data Loss Detection/ Prevention



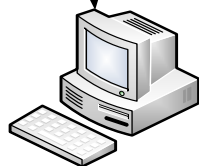
Honeypots

This device has all the required weaknesses, such as:

- Default administrator/password.
- Dummy users with weak passwords.
- Ports open for connection.
- React to virus/worm systems (but simulate conditions).

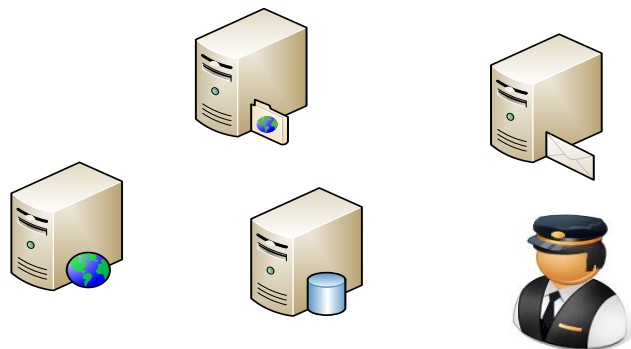


Intruder



Honeypot

**Servers/
systems**



Author: Prof Bill Buchanan



Open ports: 110 (POP-3), 80 (HTTP), 21 (FTP), 22 (SSH)



High-interaction honeypot. This simulates all the aspects of the operating system



Low-interaction honeypot. This simulates only part of the network stack (such as for **Honeyd**)
- can be virtual (from a virtual machine) or simulated by another machine.



Honeyd.conf

```
create default
set default personality "windows xp"
set default default tcp action reset
add default tcp port 110 "sh scripts/pop.sh"
add default tcp port 80 "perl scripts/iis-0.95/main.pl"
add default tcp port 25 block
add default tcp port 21 "sh scripts/ftp.sh"
add default tcp port 22 proxy $ipsrc:22
add default udp port 139 drop
set default uptime 3284460
```

```
### Cisco router
create router
set router personality "Cisco PIX Firewall (PixOS 5.2 - 6.1)"
add router tcp port 23 "/usr/bin/perl scripts/router-telnet.pl"
set router default tcp action reset
set router uid 32767 gid 32767
set router uptime 1327650
# Bind specific templates to specific IP address
# If not bound, default to windows template
bind 192.168.1.150 router
```

```

#!/usr/bin/perl
# Copyright 2002 Niels Provos <provos@citi.umich.edu>
# All rights reserved.
# For the license refer to the main source code of Honeyd.
# Don't echo Will Echo Will Suppress Go Ahead
$return = pack('cccccccc', 255, 254, 1, 255, 251, 1, 255, 251, 3);
syswrite STDOUT, $return, 9;

$string =
"Users (authorized or unauthorized) have no explicit or\r
implicit expectation of privacy. Any or all uses of this\r
system may be intercepted, monitored, recorded, copied,\r
audited, inspected, and disclosed to authorized site,\r
and law enforcement personnel, as well as to authorized\r
officials of other agencies, both domestic and foreign.\r
By using this system, the user consents to such\r
interception, monitoring, recording, copying, auditing,\r
inspection, and disclosure at the discretion of authorized\r
site.\r
\r
Unauthorized or improper use of this system may result in\r
administrative disciplinary action and civil and criminal\r
penalties. By continuing to use this system you indicate\r
your awareness of and consent to these terms and conditions\r
of use. LOG OFF IMMEDIATELY if you do not agree to the\r
conditions stated in this warning.\r
\r
\r
\r
User Access Verification\r
";

syswrite STDOUT, $string;
$count = 0;
while ($count < 3) {
    do {
        $count++;
        syswrite STDOUT, "\r\n";
        $word = read_word("Username: ", 1);
    } while (!$word && $count < 3);
    if ($count >= 3 && !$word) {
        exit;
    }
    $password = read_word("Password: ", 0);
    if (!$password) {
        syswrite STDOUT, "% Login invalid\r\n";
    } else {
        syswrite STDERR, "Attempted login: $word/$password";
        syswrite STDOUT, "% Access denied\r\n";
    }
}

exit;
sub read_word {
    local $prompt = shift;
    local $echo = shift;
    local $word;

    syswrite STDOUT, "$prompt";

    $word = "";
    $alarmed = 0;
    eval {
        local $$SIG{ALRM} = sub { $alarmed = 1; die; };
        alarm 30;
        $finished = 0;
        do {
            $nread = sysread STDIN, $buffer, 1;
            die unless $nread;
            if (ord($buffer) == 0) {
                ; #ignore
            } elsif (ord($buffer) == 255) {
                sysread STDIN, $buffer, 2;
            } elsif (ord($buffer) == 13 || ord($buffer) == 10) {
                syswrite STDOUT, "\r\n" if $echo;
                $finished = 1;
            } else {
                syswrite STDOUT, $buffer, 1 if $echo;
                $word = $word.$buffer;
            }
        } while (!$finished);
        alarm 0;
    };
    syswrite STDOUT, "\r\n" if $alarmed || !$echo;
    if ($alarmed) {
        syswrite STDOUT, "% $prompt timeout expired!\r\n";
        return (0);
    }

    return ($word);
}

```


Data Loss Prevention

5. Database and Web Loss

- SQL Misuse.
- Cross-site Scripting (XSS).
- Web scanning.
- Honeypots.



<http://asecuritysite.com/dlp>