Data Loss Prevention
5. Database and Web Loss

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

http://asecuritysite.com/dlp

Author: Prof Bill Buchanan

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

OWASP
Open Web Application Security Project

Web server

DMZ

Intrusion Detection System

Alice

Email server

Proxy server

Database server

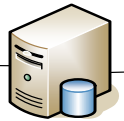
Data in-motion

DLP

Alice

Injection of code to trick the interpreter to run commands such as for SQL or Operating System commands

A1- Injection



Database

GET, POST [URL]

Web Service

Operating System

HTML

Port 80, 443

A3 - XSS

Database

Injecting code on the client side to be able to view page of other users

GET, POST [URL]

Web Service

Operating System

HTML

Malicious code gathers data from user

Port 80, 443

Data in-motion

DLP

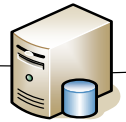
MySQL

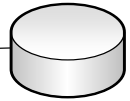
Data Loss Detection/ Prevention

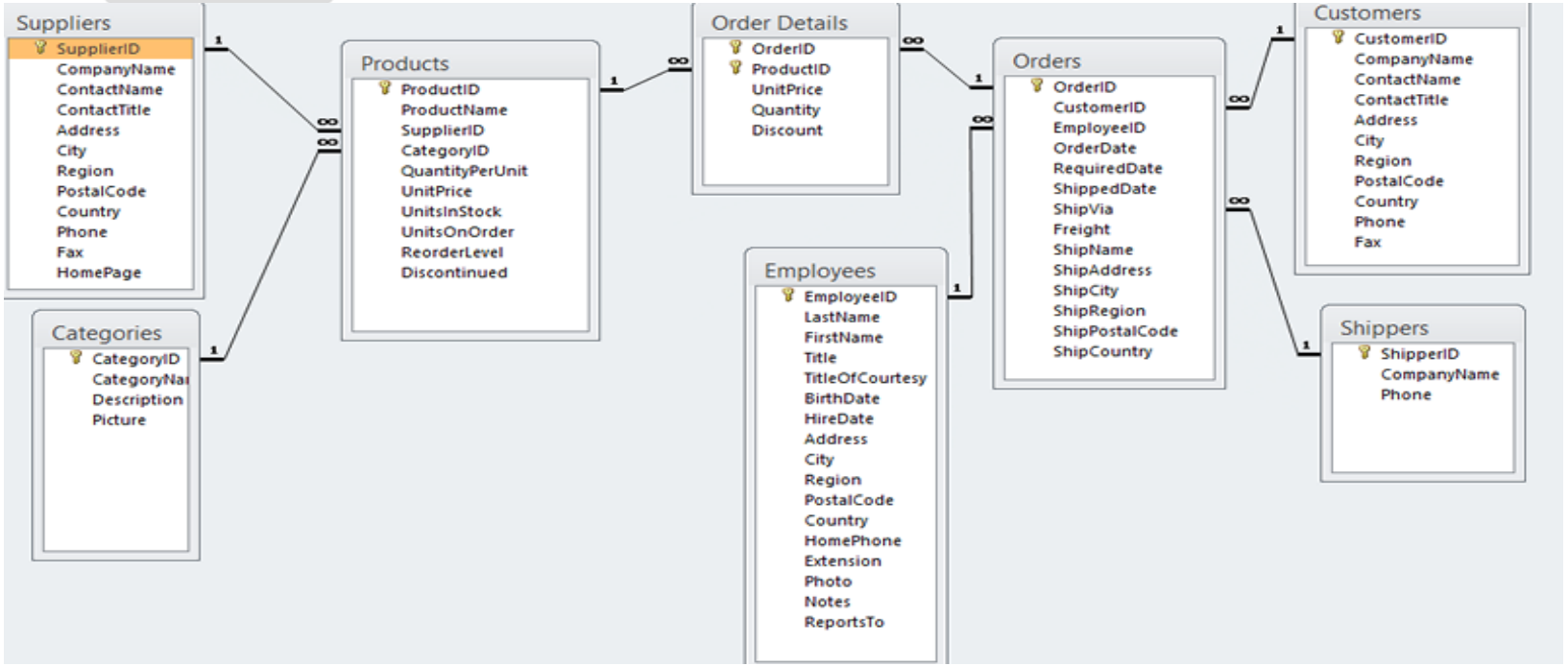
SQL

Author: Prof Bill Buchanan

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







Data in-motion

DLP

Relational Databases

Data in-motion

DLP

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

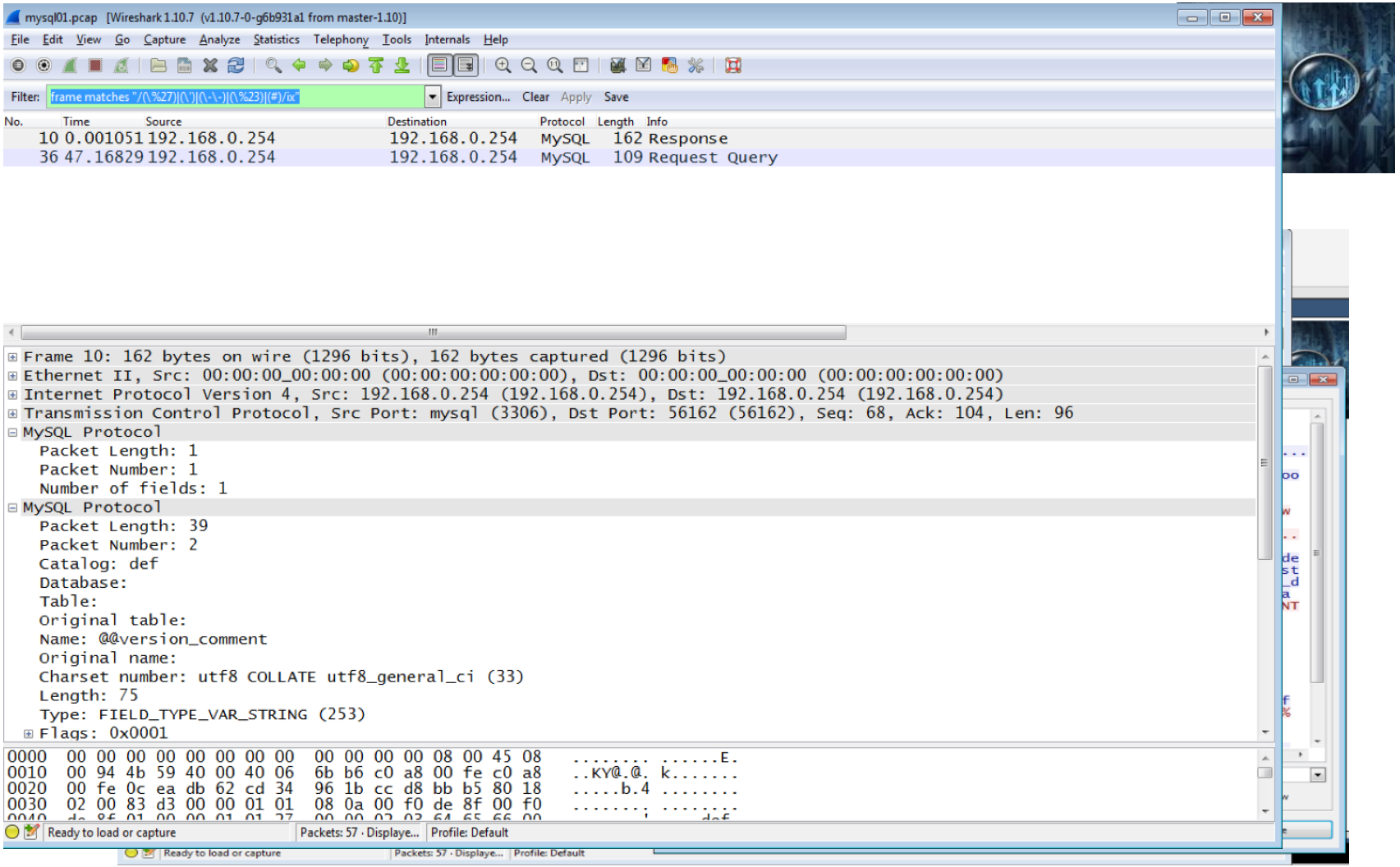
Alice

TCP Port 3306

Data in-motion

DLP

MySQL



Data in-motion

DLP

MySQL

Data Loss Detection/ Prevention

Code Injection

Author: Prof Bill Buchanan

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 Iceweasel/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=2858f079ae6eaad4f60e4d2c8ec4e7a2
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 Iceweasel/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=2858f079ae6eaad4f60e4d2c8ec4e7a2
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 62
target_host=google.com&dns-lookup-php-submit-button=Lookup+DNS
```

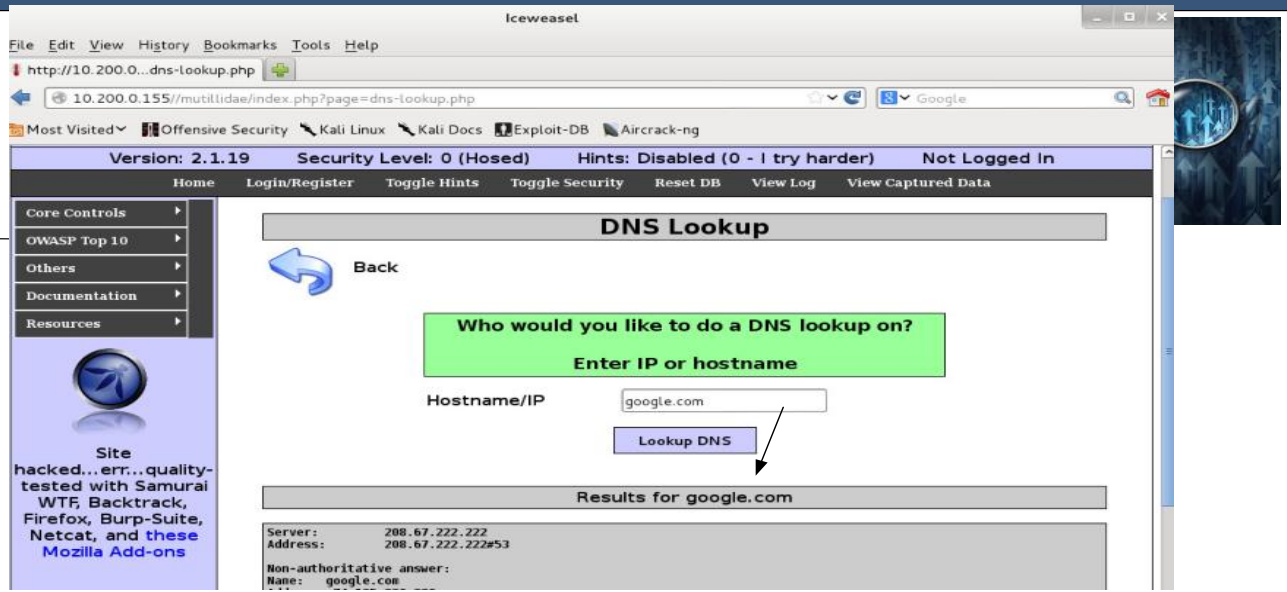
```
<form>

</form>
```

Data in-motion

DLP

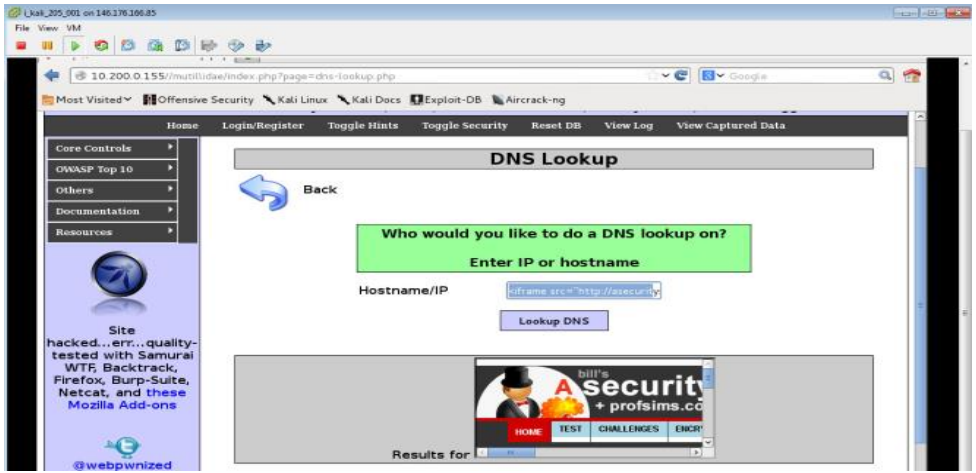
URL Posting

Alice



Code Injection

<iframe> Injection



Data in-motion

DLP

Data Loss Detection/ Prevention

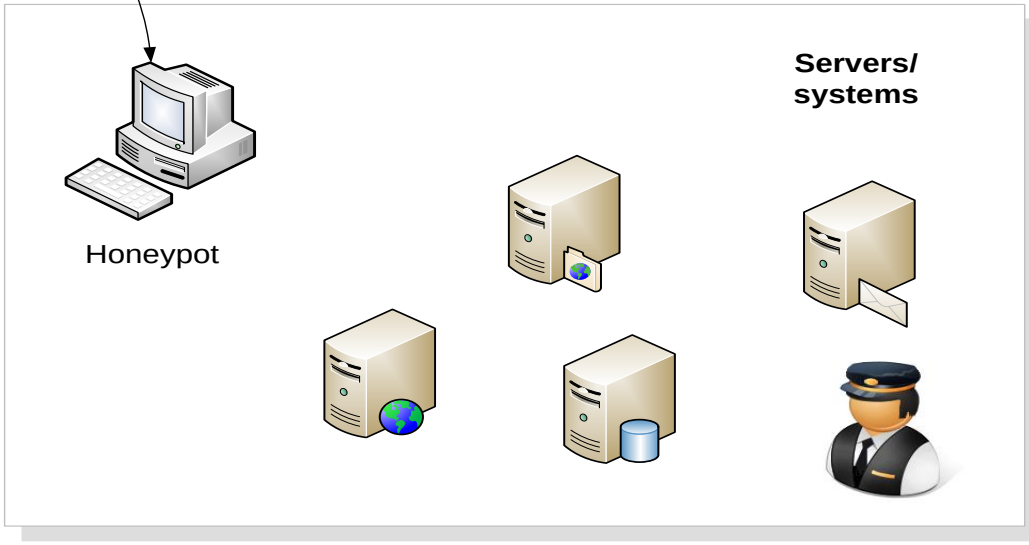
Honeypots

Author: Prof Bill Buchanan

Intruder

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).



Author: Prof Bill Buchanan

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

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

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
```

Author: Prof Bill Buchanan

```
#!/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 Surpress Go Ahead
$return = pack('ccccccccc', 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);
}
```

Example of router-telnet.pl

Data Loss Prevention
5. Database and Web Loss

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

http://asecuritysite.com/dlp

Author: Prof Bill Buchanan