



Social Engineering, SQL Injection, and DOS

By Anthony Stidham
Glenda Torres
Kevin Hernandez

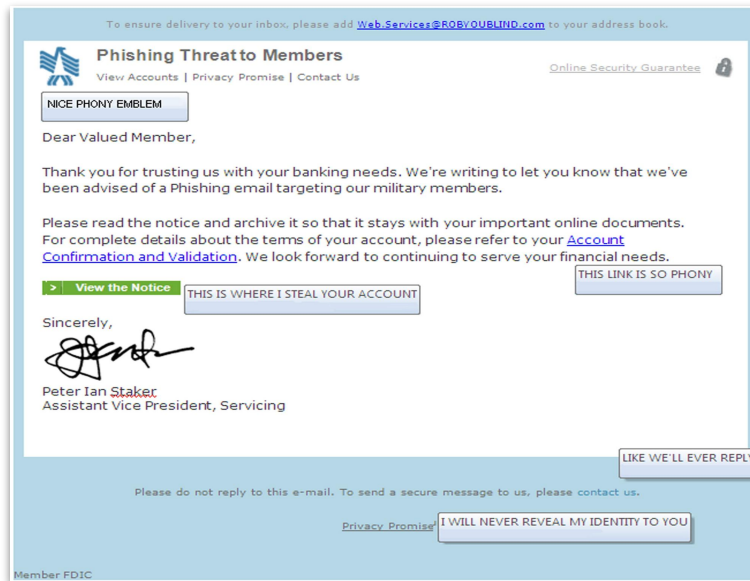


Script Kiddies and Their Impact With Easy Tools

- In this presentation, we will be showing how easily a new hacker can be dangerous with the many tools available to them.
- We will go over an attack we carried out using social engineering, sql injection, and DOS, as well as the tools used to carry out this attack.
- We will also be sharing various mitigation strategies to help reduce these attacks on yourself.

What is Social Engineering?

- A term used for a broad range of malicious activities accomplished through human interaction. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive data
- 98% of cyber attacks involve some form of Social Engineering
 - Source: Firewall Times



What is SQL Injection

- Consists of insertion or “injection” of a SQL query via the input data from the client to the application
- Part of OWASP Top 10

Example of SQL injection

SQL Injection.

User-Id :

Password :

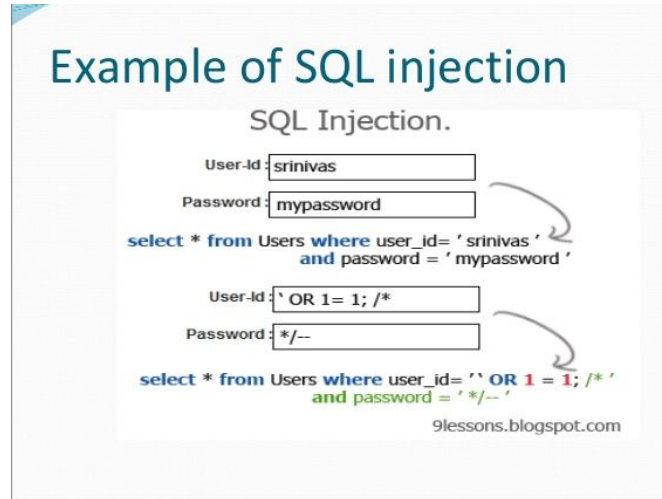
`select * from Users where user_id= 'srinivas' and password = 'mypassword '`

User-Id :

Password :

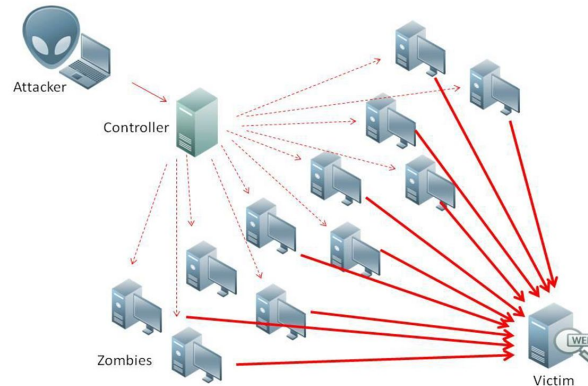
`select * from Users where user_id= '' OR 1 = 1; /* ' and password = '*/-- '`

9lessons.blogspot.com



What is DOS (Denial of Service)

- A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.



Tools Used For Today

- Linux VirtualBox Machine
- SET (Social Engineering Toolkits)
- SQLMAP
- DVWA (Damn Vulnerable Web Application)
- Burp Suite
- Goldeneye

Installing and Using SET (Social Engineering Toolkits)

- SET does not come with Linux by default, so the following command should be run:

```
sudo apt-get install git
git clone https://github.com/trustedsec/social-engineer-toolkit/ set/

cd set
pip install -r requirements.txt
```

- To open a graphical interface version of SET, you must type the following:

```
sudo ./settoolkit
history
```

SET Demo

Social Engineering Mitigation Strategies

- 2-step authentication.
- Clean up public information.
- Social Engineering training.

SQLMap and Installation

- SQLMap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers
- SQLMap can be installed from github using:

```
git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
```

SQLMap Demo

Mitigating SQL Injections

- Input Validation: A programming technique that ensures only properly formatted data may enter a software system component
- Parameterized Queries: A technique that aims to separate the SQL query from the user input values. The user input values are passed as parameters. They can no longer contain an executable code since the parameter is treated as a literal value and checked for the type and length

GoldenEye Installation

- From github GoldenEye can be installed

```
git clone https://github.com/jseidl/GoldenEye.git
```

- To use this tool it's as simple as adding the URL you want to attack

```
sysadmin@UbuntuDesktop:~$ goldeneye http://192.168.13.25/vulnerabilities/sqli/  
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>  
Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel.
```

GoldenEye (DOS) Demo

Mitigating Denial of Service (DOS)

- Detection - methods to identify normal traffic from high volume traffic. IP reputation, common attack patterns, etc.
- Response - Web Application Firewall (WAF) page rule updates for the application layer attacks or other filtration process rules that target L3/L4 layer attacks.
- Routing - Improvements on routing traffic into manageable chunks. (load balancers)
- Adaptation - Good network analysis allows for improved recognition of repeat attacks and patterns. This information allows for improved hardening of the system and prevention of future attacks.

Any Questions?