

Intro to Web Application Exploitation

whoami

- Whoami
 - Matt Fiely
 - Titan on slack
- What do I do?
 - Student
 - Intern in the security realm

Disclaimer

- Hacking without written consent is illegal
 - DO NOT practice on systems you don't own!!!!
- I am not a lawyer
 - I can't help you if you use this knowledge for evil
- What I'm going over today is for educational purposes only!

What we will be going over

- Setting up DVWA with Metasploitable
- Setting up Burp Suite
 - How to use Burp Suite
- Going over some vulnerabilities
 - XSS
 - SQLi
 - Command Injection

DVWA / Metasploitable

- Setting up a local environment to practice in
- Metasploitable is a vulnerable VM
 - DO NOT EXPOSE TO YOUR NETWORK
- Web environments:
 - DVWA
 - Mutillidae

Setting up Metasploitable

- Download
 - <https://sourceforge.net/projects/metasploitable/>
- Unzip
- Create new machine in virtualbox
 - Name Metasploitable
 - Allocate 1 gb
 - Import Metasploitable.vmdk
- **BEFORE STARTING VM**
 - Go to Settings -> Network -> Host Only Adapter

metasploitable - Settings



General



System



Display



Storage



Audio



Network



Serial Ports



USB



Shared Folders



User Interface

Network

Adapter 1

Adapter 2

Adapter 3

Adapter 4

☒ Enable Network Adapter

Attached to: Host-only Adapter ▼

Name: VirtualBox Host-Only Ethernet Adapter #3 ▼

▼ Advanced

Adapter Type: Intel PRO/1000 MT Desktop (82540EM) ▼

Promiscuous Mode: Deny ▼

MAC Address: 080027B8FAD0 

☒ Cable Connected

Port Forwarding

OK

Cancel

Metasploitable Continued

- Start VM
- Login with
 - UN: msfadmin
 - PW: msfadmin
- Ifconfig
 - Note the IP Address

Burp Suite

- Man in the Middle proxy
- Used to analyze and manipulate requests
- We will be using the free version
- Comes with features such as
 - Spidering
 - Repeater
 - Decoder
- Available on Windows, Linux, OSX

Setting up Proxy

- Going to be using Kali
 - Before starting change Kali to Host Only Adapter (same on metasploitable)
- Start Kali
- Launch Firefox
 - Preferences -> Advanced -> Network -> Settings
- Manual Proxy Configuration
 - 127.0.0.1 PORT: 8080
 - Use this proxy for all protocols
 - No Proxy for:
 - Clear out

Setting up Burp Suite

- Launch Burp Suite
- Accept Agreement
- Temporary Project -> Use Default -> Start Burp
- Proxy -> Intercept off
 - For now
- Proxy -> options -> Intercept Server Response
 - My preference

Damn Vulnerable Web App

- Navigate to the IP in firefox
- Select DVWA
 - UN: admin
 - PW: password
- DVWA Security -> Low -> Submit

Add to scope

- Go back to Burp Suite
- Target -> right click -> add to scope
 - Accept pop up
- Click Filter -> Show only in-scope items
 - We don't want to log outside traffic

Exploits

- Cross-Site Scripting
- Command Execution
- SQL Injection

Cross Site Scripting (XSS)

- Injection attack
 - Malicious scripts are injected into trusting websites
- Three main types
 - Reflected
 - Stored
 - Dom Based

Navigate to XSS Reflected

- Follow along with me

XSS

- Scenario
 - Send malicious link to a user
 - User visits page
 - Their session ID is stolen and sent to the attacker
- Example
 - `<script> alert(document.cookie); </script>`

Command Execution

- Rare but extremely powerful
- Navigate to Command Execution
 - Allows you to ping an ip address
 - Try typing an IP to see what happens

- How do you think we can attack this?

Command Execution

- Utilizes Bash, so ; will allow us to break out
- Try executing some commands
 - ; cat /etc/passwd
 - ; echo "test"

SQL Injection

- Placement of malicious code in SQL statements
- Common attack
 - Occurs when an application doesn't sanitize inputs
 - Application just trusts data

SQL Injection

- Go to SQL Injection
 - Observe what happens when you input 1
-
- Thoughts on breaking out of statement?

SQL Injection

- Php statement we are exploiting:
 - `$query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";`
- Exploit string injects like this
- Attack String
 - `x' OR 'a'='a`
- `"SELECT first_name, last_name FROM users WHERE user_id = 'x' OR 'a'='a';"`

What now?

- Now it's your turn
 - Raise the difficulty
 - Mutillidae
 - Webgoat
 - The Web Application Hacker's Handbook 2nd Edition
- The only way to get better at this is practice
- Are there any questions?