Penetration Test Agreement

For F4rmC0rp

By Joshua Main-Smith

Enterprise and Timeline	
Enterprise Name	F4rmC0rp
Authorized Personnel	Matt Mason
Emergency Contact Info	Slack Channel - @hachinijuku
Timeline	September 8th, 2020 – December 3rd, 2020
Locations	Remote – NetLab

Purpose

The purpose for F4rmC0rp (Company/Client) requesting a penetration test is to test the security posture of their new up and coming website. This penetration test is not to satisfy a compliance requirement. The permitted times given by the Company for testing are any time except during UFSIT meeting times (with a 30-minute buffer before and after said meetings).

Relevant IP addresses and their scope:

IP Addresses	Description
172.30.0.128	www.f4rmC0rp.com – Not a real network
172.30.0.0/24	ISP
172.30.0.1	Out of scope

Scope and Rules of Engagement

The Company has granted permission to

1. Scan for any vulnerabilities on potentially compromised machines.
2. Attempt to gain the highest root privileges on potentially compromised machines
3. Password attacks not including dictionary attacks
4. To assess
    a. Web applications – F4rmC0rp.com and a small number of pages
    b. Login systems – FTP
    c. Static pages – HT access files
    d. Wireless attacks against client
5. To use software engineering tactics to gain physical access – Phineas only

Devices within scope and their properties

1. Router providing access to a network disconnected from the internet
2. EAP network
3. Encryption – WPA2

4. Firewall

Communication and Potential Negative Outcomes

The Client has agreed to communicate sensitive information using encryption and that regular status meetings are not necessary before the final report. There should be no shunning and to contact Matt Mason if this is to occur. Under the event that there are any negative outcomes as a result of our testing, the Client has confirmed that a Virtual Machine is in place to reset the system and will not hold the tester liable so long as a best effort has been made to prevent or mitigate any possible negative outcomes resulting from testing. The Client has also informed us that their ISP has granted them permission in continuing with a penetration test.

_____ _____

Signature Date

Brief Explanation

I chose these elements to include into the contract agreement between me and F4rmC0rp to

1. Explicitly make it clear that I have permission to engage in using ethical hacking techniques on their network/software/hardware in exchange for a detailed report in my findings and suggestions on how to move forward.
2. Outline what is and is not in scope when conducting tests so that if there is a dispute in the future, we can refer to the agreement.
3. A timeline for when an appropriate time to test is as well as a hard deadline
4. Know the best way to communicate sensitive information that I may find with the company
5. And, basically to cover my @$$ in the event of any legal dispute

I felt that one of the best things to make clear is the IP range needed to test. As was mentioned in one of the lectures, I don't want to find myself in a situation where I'm performing hacking tests on a Sherriff department's network. Even when given an IP range, I would want to double and triple check that the IP range I've been given permission to test on actually belongs to the company in question.

Also, of significant importance is to make clear on what it is that I'm allowed to test on, including devices and humans. With humans being, well… human, we're prone to taking offense in being tricked or manipulated. So, it's important to make it clear that social engineering is an option in the testing cycle. Devices being devoid of emotion, it's not as big of a deal. But it's important to note that critical servers could be at risk for a potentially negative, albeit unintended, outcome if subject to testing.