The Rules of Engagement

Tyler Chotikamars

University of Arizona Global Campus

CYB 302 Secure Web Applications and Social Networking

Carl Marquez

December 5th, 2021

Within our world of ever-evolving technology, there come risks involved with using the sophisticated tools that we utilize daily. It's a common belief that if an exploit exists, someone will always come along to take advantage of it. Within this paper, besides the rules of engagement, we will outline multiple attack-defend scenarios on resources that we use on our own Windows and Linux servers and applications. We will also be looking at how web applications and social networking play a role in the company's security, as well as how to conduct payment card industry compliance.

As previously mentioned, as technology advances and evolves, so do the tactics used by attackers. A common type of security flaw that attackers look for is coding errors within Linux and Windows computers that are associated with web applications and social networking. This can involve cross-site scripting, SQL injection, cross-site request forgery, and the failure to preserve OS commands. These kinds of attacks can be prevented by mitigating coding errors to prevent them from happening. Other threats that we may face as a company could include e-mail and social networking threats. This can include pictures embedded with scripts, phishing, social engineering, and many other types of malicious attacks. To defend from all these types of attacks it is important to create a security culture within the company so that all employees know the dangers that come with using the internet. Increasing user awareness, implementing encryption, using plaintext e-mail and antiviruses are all ways to prevent these types of attacks.

Another important thing to consider as a company is how we handle the rules and regulations set by the payment card industry. Without following their regulations, we can be subject to fines and unable to process card payments. The main principles they cover include maintaining a secure network, protecting cardholder data, maintaining a vulnerability

management program, implementing access control measures, monitoring/testing networks, and maintaining an information security policy. The PCI DSS assessment entails network systems that include firewalls, switches, routers, (WAPs), network appliances, and other security applications. The PCI council also audits the servers that are used to process card payments. The best way to be compliant with PCI DSS requirements is to apply security measures properly, document, simplify complex rules, and document policies and systems.

Protecting employee and customer data is crucial for operating a successful business that is not susceptible to outside attacks. It is important that within company culture there is an emphasis on security and that we create an environment where employees feel safe and secure. As technology constantly changes it is important for us as a company to be aware of the type of threats that exist so that we can protect ourselves from them. Web applications and social networking play an important part in conducting business within e-commerce, and that is why online security, as well as compliance with PCI standards, are important to us as a company.

Rules of Engagement Worksheet:

Penetration Testing Team Contact Information:

Primary Contact: Will Broshire

Mobile Phone: (531)531-6136

Pager: 12351856

Secondary Contact: Sarah Willingham

Mobile Phone: (702)812-9481

Pager: 76498478

Target Organization Contact Information:

Primary Contact: John Smith

Mobile Phone: (702) 984-1928

Pager:132462878

Secondary Contact: Lily Scott

Mobile Phone: (702)-123-5215

Pager:56835734

"Daily Debriefing" Frequency: Twice a day

"Daily Debriefing" Time/Location: 4 PM, held in the pen test conference room.

Start Date of Penetration Test: 1/1/2022

End Date of Penetration Test: 5/1/2022

Testing Occurs at Following Times: 1:00 PM, 2:45 PM, 3:15 PM

Will test be announced to target personnel: No

Will target organization shun IP addresses of attack systems: Yes

Does target organization's network have automatic shunning capabilities that might disrupt access in unforeseen ways (i.e. create a denial-of-service condition), and if so, what steps will be taken to mitigate the risk: No.

Would the shunning of attack systems conclude the test: Yes.

If not, what steps will be taken to continue if systems get shunned and what approval (if any) will be required: N/A

IP addresses of penetration testing team's attack systems:

170.0.30.1 – 170.0.30.2 - 170.0.30.80 -170.0.30.20 -170.0.30.21 - 170.0.30.0

Is this a "black box" test: Yes.

What is the policy regarding viewing data (including potentially sensitive/confidential data) on compromised hosts: Data that is sensitive to individuals will be disregarded and discarded. Confidential data concerning the company will be given back to the company so that they can estimate the damage that could have been done.

Will target personnel observe the testing team: Yes

Signature of Primary Contact representing Target Organization

Brian Oversee

Date

12/6/2021

Signature of Head of Penetration Testing Team

Rick Handler

Date

12/6/2021

If necessary, signatures of individual testers:

Signature

Lucy Malik

Date

12/6/2021

Signature

Ty Wilshire

Date

12/6/2021

References:

Harwood, M. (2016). *Internet security: How to defend against attackers on the web* (2nd ed.).

Retrieved from https://content.uagc.edu

Gibb, T. (2017, July 11). Geek school: Writing your first full PowerShell script (Links to an external site.). Retrieved from https://www.howtogeek.com/141495/

Leonhard, W. (2016, October 16). How to use Windows PowerShell: A beginner's guide (Links to an external site.). Retrieved from https://www.pcworld.com/article/3131611/windows/how-to-use-windows-powershell-a-beginners-guide.amp.html

Payment Card Industry Security Standards Council. (2010, October). Getting started with PCI data security standard (Links to an external site.). Retrieved from https://www.pcisecuritystandards.org/documents/PCI_SSC_Getting_Started_with_PCI_DSS.pdf?agreement=true&time=1489613277483

Testing Brain. (n.d.). Penetration testing tutorial, types, steps and PDF guide (Links to an external site.). Retrieved from https://www.testingbrain.com/tutorials/penetration-testing-tutorial.html