UNIVERSIDADE DE SANTO AMARO

CURSO DE GRADUAÇÃO TECNOLOGICA EM ANALISE E DESENVOLVIMENTO DE SISTEMAS

SEGURANÇA DE COMPUTADOR E REDES:VOCÊ ESTÁ SENDO ATACADO POR ADOLESCENTES?

KAIO GABRIEL DE OLIVEIRA AZEVEDO

UNIVERSIDADE SANTO AMARO - POLO REGISTRO-SP

2021

KAIO GABRIEL DE OLIVEIRA AZEVEDO

Aspectos da Segurança da Informação: Sua Importância para as Organizações

Trabalho de Projeto Integrador do Curso de Graduação em Analise e Desenvolvimento. Área de concentração: Segurança de Redes. Orientador: Luis Fernando dos Santos Pires.

Universidade Santo Amaro – Polo Registro-SP

2021

RESUMO

Esse trabalho tem como finalidade introduzir pessoas e empresas a saberem alguns dos possíveis ataques que poderão ocorrer no local de trabalho. Explicarei como funciona um dos ataques e porque está se tornando tão frequente as invasões nas empresas por meios de alguns métodos. Classificarei as categorias “hacker” para entendimento de saber com o que estamos lidando nas empresas e como a mídia os chamam hoje em dia. Citarei alguns tipos de ataques mais famosos para que fique claro que nem sempre o meio tecnológico é o culpado e sim o fator humano. Irei citar uma serie e um filme em especifico que engrandecem adolescentes e adultos a praticarem as invasões tanto beneficamente quanto maleficamente. Apresentarei um simples ataque em um servidor para testes de vulnerabilidades para provar o quanto um servidor desatualizado pode ser um risco para a empresa ou comercio.

Palavras-Chaves: Invasões; Hackers; Empresas;

SUMÁRIO

1. INTRODUÇÃO

Esse trabalho tem como finalidade orientar as pessoas, Microempresas e Empresas de pequeno a médio porte a fim de identificar a causa e finalidade dos ataques que ocorrem no setor tecnológico dessa empresa ou negócio, centralizando nos serviços de Web e banco de dados. Nesse presente trabalho citaremos as famosas “Categorias Hackers”, e iremos analisar os ataques mais frequentes e ver o fator que incentiva esses ataques e como os adolescentes se sentem incentivados a fazer esses ataques por meio das mídias. Para entendimento desses ataques usaremos alguns exemplos de invasão dentro de um ambiente controlado.

2. Nomeando inimigos

Na Internet, há uma grande disputa de conhecimento, onde há o lado que diz que tudo que é crime informático é associado aos “hackers” e nada mais, porém há aqueles que digam que há classificações para distinguir quem é quem. Citarei algumas:

2.1 White Hat (Hacker ético): Um exemplo deles podem ser os Analistas de Segurança da Informação (pentesters), eles encontram as vulnerabilidades e avisam a empresa como contornar isso. Geralmente são as empresas que chamam os pentesters para testar seus negócios sendo ele de servidores de Web até programas, às vezes a empresa contrata um Analista de segurança da informação para estar sempre presente na empresa.

2.2 Black Hat (“Hackers do mal”): Eles e os White Hat são como inimigos pré-definidos nesse mundo tecnológico que nos engloba. Black hat buscam apenas dados e informações nas vulnerabilidades que os próprios encontram e assim tentam capturar senhas de bancos, dados pessoais, dados bancários.

2.3 Script-Kiddies: Os famosos “Crianças do script” são hackers inexperientes que buscam fama e fins lucrativos, eles realizam tal feito através de scripts prontos distribuídos na internet e os alvos deles sempre existirá uma falha fácil de ser explorada.

2.4 Lammers: Os lammers são os mais completos inexperientes, ou seja, vivem em fórum falando coisas sem sentido como criar um super-virus pelo bloco de notas mais não ter nenhuma experiencia ou ser o criador do mais poderoso ransomware que o mundo já viu. Os lammers são o termo antigo de script kiddie e mesmo assim os scripts kiddies ainda usam scripts prontos já os lammers só falam e nada faz.

2.5 Crackers: O mal em pessoa, os crackers possuem um alto conhecimento por meio do mundo digital, os alvos deles começam desde softwares (com a quebra de "serial key") a fraudes bancárias.

3. Ataques mais importantes

Segundo OWASP (Open Web Application Security Project), ou Projeto Aberto de Segurança em Aplicações Web eles concentram em 10 falhas, mas vou me concentrar nas mais comuns. Vou citar três falhas que um Lammer e Script-Kiddies conseguiriam atacar em um servidor desatualizado e mais usado por adolescentes no início de sua carreira "Hacker".

3.1 SQL Injection: Utilizado mais por quem está no início da carreira de "hacker", ou seja, seriam os Script-Kiddies ou Lammers, esse ataque permite a o atacante inserir uma instrução SQL personalizada e não esperada dentro de uma consulta conhecida como SQL Query no banco de dados.

3.2 Phishing: Esse é um dos ataques mais comuns dentro de uma empresa que não tem uma boa política de segurança, ele consiste mais em persuadir os funcionários da empresa de modo a darem acesso a conteúdo internos da empresa. O phishing usa mais o fator humano para atacar suas vítimas através de sites falsos mais idênticos aos originais ou fingindo ser uma pessoa de alto escalão na empresa que nenhum dos funcionários negaria acesso. O termo Phishing se compara a palavra inglesa fishing que significa pescar ou pescaria, então os atacantes "pesca" os alvos pegando suas informações com "anzol" que mordem as iscas em sites falsos enviados por mensagens de e-mail para a vítima (muitas vezes fingindo ser quem não é).

3.3 Defacement: É o nome dado à técnica de explorar erros de aplicações web e realizar operações no conteúdo e na estética dos elementos que compõem o site. Deface a palavra de origem inglesa é utilizada em segurança da informação para categorizar ataques realizados por Defacers que são usuários de computador que na maioria das vezes possui pouco conhecimento técnico sobre servidores web (muito usado por lammers e script kiddies, porém hacktivistas como o grupo"Anonymous"utilizam também em forma de protesto).Defacement é mais como uma pichação eletrônica para brincar ou insultar.

4. Demonstrações de ataques

Demonstraremos os ataques sendo realizados em ambientes totalmente desenvolvidos para a situação em questão. Testamos a vulnerabilidade SQL Injection no site da empresa Acunetix designado para esses tipos de testes, assim não estaremos infringindo nenhuma lei e usarei uma ferramenta que automatiza o ataque para mostrar como é fácil explorar uma falha dessas num site despreparado.

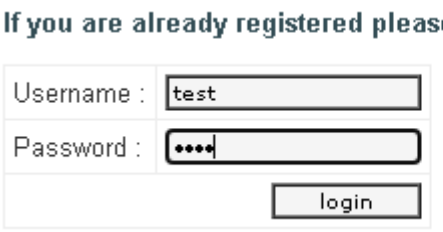
4.1– Entrando em um ambiente com essa falha.

OBS:O site testphp.vulnweb.com.

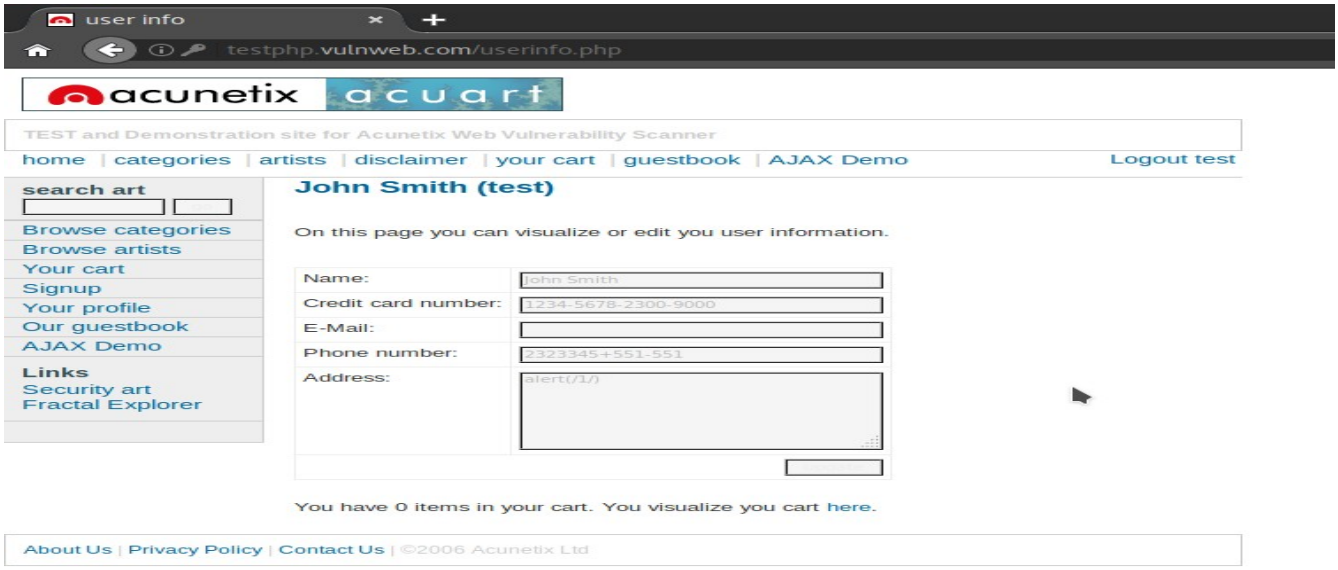
4.2 – Ferramenta de código aberto: SQLMAP.

Ela explora vulnerabilidades dentro de sites vulneráveis a falhas sql injection. Executamos para ter acesso a informações do banco de dados, assim sucessivamente conseguir acesso.

4.3 – Entrando no site com os dados capturados:



4.4 – Obtendo acesso.



5. A mídia na cabeça dos “hackers” ou os “hackers” na cabeça da midia.

A popularização da internet fez com que a mídia de massa começasse a abrir os olhos para o hackativismo e a cultura hacker, isso é, fez com que grandes produtoras de filmes e séries começassem a vender o hackativismo como “cool” (termo em inglês para legal), atraindo a atenção de público jovem, exemplo disso tem a série Mr.Robot que é vendida como uma série de hackers reais, já que a mesma tem roteiro auxiliados por hackers buscando a maior fidelidade nas ações da série, até mesmo em códigos, o roteiro da série baseia-se na história do engenheiro de segurança cibernética Elliot Alderson e seu envolvimento com o grupo de hackativismo fsociety que luta contra grandes corporações. A série tem forte inspiração nos grupos hackativistas Anonymous e LulzSec, eles colocam o grupo fsociety como revolucionário, de certa forma até heroico, inspirando muitos espectadores a procurarem e aprenderam sobre hacking como os protagonistas, exemplo disso temos o MrRobot (sessão do fórum Reddit sobre Mr. Robot) onde fãs debatem sobre os métodos de hacking utilizados pelos personagens, até mesmo replicando eles.

6 – CONCLUSÃO

Visto como os ataques funcionam e como é simples de explorar essa falha encontrada em muitos servidores, é possível contornar essa falha com o programador, fazendo com que os dados dos usuários não tenham efeito direto na consulta SQL, e para você ficar atualizado sobre seu sistema está livre dessas falhas é aconselhável automatizar para que o Sqlmap esteja verificando essas falhas diariamente ou a cada mudança no código fonte. Mantenha também os servidores com todos seus programas atualizados, visto que os desenvolvedores buscam contornar falhas de segurança com atualizações constantes. As atualizações servem tanto para o sistema operacional quanto para seus programas.

REFERÊNCIAS

BELCIC, Ivan. **Phishing**. Disponível em: <https://www.avast.com/pt-br/c-phishing>. Acesso em: 2 nov. 2021.

WINTERMEYER, WINNI**. How the Real Hackers Behind Mr. Robot Get It So Right**. Disponível em: <https://www.wired.com/2016/07/real-hackers-behind-mr-robot-get-right/>. Acesso em: 2 nov. 2021.

CANALTECH, Redação. **O que é Script Kiddie?**. Disponível em: <https://canaltech.com.br/produtos/O-que-e-Script-Kiddie/>. Acesso em: 2 nov. 2021.

LINHARES, H. M. et al. **SQL Injection, entenda o que é, aprenda a evitá-lo.** Disponível em: <http://re.granbery.edu.br/artigos/Mzk2.pdf>. Acesso em: 2 nov. 2021.

PANGBURN, Dj. **O Criador de 'Mr. Robot' Explica Suas Raízes Hacktivistas e Cults**. Disponível em: <https://motherboard.vice.com/pt_br/article/xyaewz/o-criador-de-mr-robot-explica-suas-razes-hacktivistas-e-cults>. Acesso em: 2 nov. 2021.

KOEBLER, Jason**. Where 'Mr. Robot' Gets Inspiration for its Hacks**. Disponível em: <https://motherboard.vice.com/en_us/article/8q85g4/where-mr-robot-gets-inspiration-for-its-hacks>. Acesso em: 2 nov. 2021.

OWASP. **OWASP Top 10 - 2021**. Disponível em: < https://owasp.org/Top10/>. Acesso em: 2 nov. 2021.

REDDIT. **R/MrRobot**. Disponível em: <https://www.reddit.com/r/MrRobot/>. Acesso em: 2 nov. 2021.

SQLMAP. **Sqlmap : automatic SQL injection and database takeover tool**. Disponível em: <http://sqlmap.org/>. Acesso em: 2 nov. 2021.