Teste de Invasão: O segredo por trás de como funciona uma invasão hacker, a metodologia de invasão utilizada por hackers

João Victor Alves Vasconcelos[1]

[1]Instituto de Ciências Exatas e Tecnologia – Universidade Federal do Amazonas(ICET/UFAM)
Itacoatiara – AM – Brasil

victorvicky045@gmail.com

Resumo. *Ataques cibernéticos ao passar dos anos tem se tornado muito mais comum, estima-se que ao dia 30 mil sites são vítimas de ataques cibernéticos por dia e a cada 39 segundos ocorre algum ataque na internet. Embora sabendo desses fatos ainda há uma enorme desinformação e mistério de como ocorrem estes ataques e também de que tipo de pessoas estão por trás destes ataques e seus motivos para eles, fazendo com que muitos mitos e preconceitos sejam criados ao redor da figura do hacker, fazendo muitos acreditarem que todos os hackers são criminosos ou que são capazes de feitos considerados fantasiosos. Através desta pesquisa, busca-se conscientizar o público geral da figura do hacker, mencionando técnicas, ferramentas e conhecimento teórico de como essas invasões são feitas, além de demonstrar a metodologia para invasão utilizada por todos os hackers, tanto cibercriminosos como hackers éticos. Este artigo tem como objeto educar o público leigo sobre o assunto, a fim de gerar uma maior compreensão sobre as etapas de uma invasão hacker.*

1. Introdução

No mundo da cibersegurança, mais especificamente falando, na área ofensiva da cibersegurança, assim como em qualquer área de tecnologia de informação, é abordada uma metodologia para realizar testes de invasão contra um alvo. Esta metodologia de ataque é aplicada para todos os tipos de invasões e também aplicada por todos os tipos de invasores, como por exemplo: cibercriminosos, hackers éticos, bug bounty hunters, hacktivistas e também até mesmo por nações estados em programas de espionagem.

2. Metodologia

A metodologia utilizada por todos os tipos de hackers é conhecida como teste de invasão: uma abordagem clara e metódica que busca dividir em partes as principais etapas de como um invasor invade sua vítima. Ela consiste em coletar informações importantes sobre um alvo, descobrir as vulnerabilidades de um alvo, explorar as vulnerabilidades de um alvo, adentrar no sistema do alvo, persistir dentro do sistema do alvo e limpar os rastros do ataque ou reportar relatórios.

3. Teste de Invasão

O teste de invasão se aplica para todas as categorias de invasão, seja ela a invasão de redes, dispositivos IoTs, computadores, dispositivos móveis, websites e hardware. A metodologia do teste de invasão é essencial no arsenal de um hacker e é indispensável para todos os tipos de invasores. Ela é dividida em reconhecimento, enumeração, exploração, pós-exploração, limpeza de rastros e relatórios.

3.1. Reconhecimento

Também referida como “footprinting” em inglês, a fase de reconhecimento é a primeira e mais importante etapa de uma invasão. Nesta fase, o invasor começa a buscar informações sobre o alvo utilizando OSINT (Open Source Intelligence), uma técnica que consiste em buscar informações que estão publicamente disponíveis sobre o alvo, como e-mails, domínios, números de telefone, endereços IP, etc. Esta etapa é dividida em coleta de informações passiva e coleta de informações ativa.

Na coleta de informações passiva, o atacante não interage diretamente com o alvo; ele busca, através do uso de ferramentas e técnicas de OSINT, coletar informações de forma passiva em relação ao alvo, usufruindo de informações publicamente disponíveis na internet e em outros meios. A coleta de informações ativa, diferente da passiva, interage diretamente com a vítima, possuindo um maior risco de o invasor ser detectado. Esta etapa consiste em fazer uma varredura nos serviços de portas abertas no alvo para saber quais portas estão abertas e fechadas, para se ter uma noção de planejamento de ataque.

A ferramenta mais utilizada para coleta de informações ativa é o nmap, enquanto através de várias ferramentas como whois, recon-ng e maltego, o invasor pode coletar um número considerável de informações sobre a vítima de forma passiva.

3.2. Enumeração

Após coletar um número considerável de informações valiosas sobre a vítima, é hora de descobrir como ela pode ser vulnerável. Esta fase consiste em procurar por vulnerabilidades, tanto na parte humana, como por exemplo, nomes de usuários e suas senhas, quanto na parte do sistema, através da procura de versões de softwares vulneráveis a exploits. A enumeração é a etapa principal que determina se um ataque poderá ser bem-sucedido ou não. Caso seja negligenciada ou não realizada da forma correta, as chances do ataque falhar serão grandes.

Um exemplo prático da fase de enumeração seria um ataque a um sistema operacional Windows 10 que talvez fosse vulnerável à vulnerabilidade EternalBlue (CVE-2017-144). Alguém inexperiente tentaria invadir o sistema sem ao menos enumerá-lo antes para descobrir se é vulnerável ou não. Em contrapartida, uma pessoa mais experiente, antes de ao menos tentar invadir o sistema, usufruiria de scripts para descobrir se o Windows 10 da vítima é vulnerável ou não à EternalBlue e procuraria a versão apresentada no software para descobrir qual o melhor exploit para utilizar na

invasão. As ferramentas mais comuns da fase de enumeração utilizadas por invasores podem ser resumidas ao próprio nmap, ao Metasploit Framework e à utilização de técnicas avançadas de pesquisa, como o Google dorking.

```
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Figura 1. Uso da ferramenta nmap na fase de enumeração, utilizando script para descobrir vulnerabilidade EternalBlue no sistema.

3.3. Exploração

A fase de exploração é aquela em que ocorre o ataque de fato. Após obter todas as informações necessárias da vítima na fase de reconhecimento e descobrir todas as possíveis vulnerabilidades dela com a enumeração, é aplicado o ataque contra a vítima. O ataque pode consistir na utilização de exploits: programas ou códigos projetados para encontrar e explorar falhas de segurança ou vulnerabilidades dentro do sistema para poder adentrar ao sistema da vítima ou de técnicas avançadas de invasão, como man-in-the-middle e buffer overflows.

Várias ferramentas podem ser utilizadas na fase de exploração: Metasploit Framework para poder injetar exploits dentro do sistema, Msfvenom para criação de exploits personalizados, Ettercap para ataques man-in-the-middle, Netcat para escuta de portas e injeção de reverse shells, John the Ripper e Hydra para quebra de senhas, e o Social Engineering Toolkit para ataques de phishing e engenharia social.

Figura 2. Metasploit Framework, a ferramenta de exploração e pós-exploração mais famosa dentro do universo da cibersegurança, muito utilizada em diversos ataques.

3.4. Pós-Exploração

Finalmente, o sistema é explorado com sucesso. Porém, ainda não está acabado. Apenas conseguir adentrar dentro do sistema não é suficiente; é preciso escalar privilégios dentro do sistema. Através do uso de payloads (códigos que são executados quando um ataque é bem-sucedido), o hacker consegue realizar, de fato, o seu ataque desejado.

O uso de payloads pode variar muito dentro de uma invasão. Porém, o uso mais comum deles é através da injeção de malwares dentro do sistema. Malwares podem ser classificados como softwares maliciosos projetados para prejudicar um computador ou sistema de computador. Eles possuem vários tipos diferentes de funções, como vírus, cavalos de tróia, rootkits, spywares, keyloggers e ransomwares. Um dos tipos de malware mais famosos para o público geral são os ransomwares: softwares maliciosos capazes de criptografar todos os arquivos de um sistema de computador. É um dos ataques mais utilizados por cibercriminosos, e nele a vítima precisa pagar um valor monetário aos cibercriminosos para descriptografar os arquivos dentro do ou dos seus sistemas de computadores.

Outra técnica, além do uso de payloads na pós-exploração, trata-se da escala de privilégios: uma forma na qual o invasor eleva seus privilégios dentro do sistema até alcançar o superusuário do sistema, permitindo ao invasor obter nível administrativo dentro do sistema. A escala de privilégio se divide basicamente em dois tipos: escala de privilégio horizontal e escala de privilégio vertical. Na escala de privilégio horizontal, são escalados gradualmente os privilégios através do acesso de contas com menor privilégio até finalmente chegar na conta com maior privilégio, basicamente pulando de conta em conta para, no fim, conseguir alcançar a conta com maior privilégio administrativo. Já na escala de privilégio vertical, é utilizado algum payload ou falha no sistema para conseguir rapidamente acesso à maior conta com privilégios administrativos dentro do sistema que está sendo invadido.

Figura 3.Representação do ataque de ransomware mais famoso: Wannacry, responsável pela infecção de mais de 230 mil computadores em mais de 150 países.

3.5. Limpeza de rastros e relatórios

Esta é a última fase de uma invasão. Finalmente, depois de todas essas etapas, o atacante conseguiu realizar seu objetivo. Agora, para não levantar suspeitas, ele precisa limpar sua atividade do ataque para permanecer oculto. São utilizadas diversas técnicas para limpar seus rastros e permanecer oculto. Isso inclui alterar valores de registro, desinstalar todos os aplicativos que foram usados, excluir todas as pastas, alterar valores dentro do registro e também modificar, corromper e excluir os valores desses registros, tornando assim muito difícil identificar se ocorreu um ataque hacker ou não.

A limpeza de rastros é utilizada tanto por cibercriminosos, com o objetivo de ficarem totalmente ocultos dentro do sistema, como também por hackers éticos, para simular por completo a invasão de um cibercriminoso dentro do sistema para uma maior legitimidade no ataque, tornando-se uma etapa indispensável dentro de um ataque.

No final, o que difere a invasão de um cibercriminoso ou usuário malicioso de um hacker ético são seus motivos pelo ataque. Enquanto um cibercriminoso (também chamado de “Black Hat”) procura ganhos financeiros ou maliciosos invadindo um sistema, o hacker ético (também chamado de “White Hat”) busca encontrar falhas de segurança dentro do sistema para melhorar a segurança de seus clientes. É nessa etapa que entra a criação de relatórios: a fase na qual o hacker ético irá reportar todas as

vulnerabilidades encontradas dentro do sistema por ele(a) em formato de um documento detalhado sobre suas descobertas para seus clientes, para que os mesmos possam consertar essas falhas de segurança, sendo a fase final e mais importante do hacking ético.

4. Conclusão

Através desta análise, foi possível obter uma visão geral sobre as etapas de uma invasão cibernética, mencionando técnicas, ferramentas e metodologias utilizadas para realizar ataques. Ao compreender como os ataques cibernéticos são realizados, é possível tomar medidas para a proteção geral contra os mesmos. É de extrema importância para estudantes de cibersegurança que compreendam cada etapa dita neste artigo para uma maior compreensão sobre o assunto.

Referências

PRAVEEN. What are Privilege Escalations? Attacks, Understanding its Types & Mitigating Them. Disponível em: <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/privilege-escalations-attacks/>. Acesso em: 22 jan. 2024.

GRAHAM, D. Ethical hacking: A hands-on introduction to breaking in. São Francisco, CA, USA: No Starch Press, 2021. p.49-424.

SCHELDT, A. 7 most common types of malware. Disponível em: <https://www.comptia.org/blog/7-most-common-types-of-malware>. Acesso em: 22 jan. 2024.

Phases of hacking. Disponível em: <https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking>. Acesso em: 22 jan. 2024.

YAWORSKI, P. Real-world bug hunting: A field guide to web hacking. São Francisco, CA, USA: No Starch Press, 2019. p.268-313.