Fundamentals Cracking the Perimeter

PROF. JOAS ANTONIO

SOBRE O EBOOK

- Aprender a identificar vulnerabilidades
- Configurações incorretas
- Ver casos de estudos sobre algumas vulnerabilidades
- Esse livro tem com base o curso CTP da Offensive Security, mas vou trazer não só para especialistas na área, mas também para os novos, aqueles que estão começando como PenTesters

SOBRE O AUTOR

- Pesquisador de segurança da informação pela Experience Security
- Autodidata na área
- Palestrante
- Instrutor de informática
- Fundador da Cyber Security UP
- Escritor

INTRODUCTION

Advanced PenTest

- Quando falamos em PenTest avançado, não estamos só citando o uso de ferramentas mais profissionais para quebrar a segurança de um sistema
- Mas sim, utilizar de técnicas que vai além de ferramentas comuns, usar técnicas avançadas de penetração
- Por exemplo: Engenharia reversa, Buffer Overflow, Desenvolvimento de exploits, criação de shellcodes, bypass em erros de configurações e por ai vai.

CTP (OFFENSIVE SECURITY)

- Cracking the Perimeter (CTP) é um curso on-line e autônomo que está entre os cursos de hacking e penetração éticos mais desafiadores disponíveis na indústria. Além do guia de curso tradicional e palestras em vídeo, cada aluno recebe acesso a um laboratório de testes de penetração virtual, no qual as técnicas aprendidas no curso podem ser praticadas em um ambiente seguro e legal. Você aprenderá como identificar vulnerabilidades difíceis de encontrar e configurações incorretas em vários sistemas operacionais e realizar ataques organizados de maneira controlada e focada. Após a conclusão bem-sucedida do curso e do exame de certificação, você se tornará oficialmente um Especialista Certificado em Segurança Ofensiva, o que prova que você não apenas domina as habilidades avançadas de testes de penetração, mas também tem a capacidade de pensar lateralmente e agir sob pressão.
- https://www.offensive-security.com/information-security-training/cracking-the-perimeter/

CTP (OFFENSIVE SECURITY)

- Cracking the Perimeter (CTP) é um curso on-line e autônomo que está entre os cursos de hacking e penetração éticos mais desafiadores disponíveis na indústria. Além do guia de curso tradicional e palestras em vídeo, cada aluno recebe acesso a um laboratório de testes de penetração virtual, no qual as técnicas aprendidas no curso podem ser praticadas em um ambiente seguro e legal. Você aprenderá como identificar vulnerabilidades difíceis de encontrar e configurações incorretas em vários sistemas operacionais e realizar ataques organizados de maneira controlada e focada. Após a conclusão bem-sucedida do curso e do exame de certificação, você se tornará oficialmente um Especialista Certificado em Segurança Ofensiva, o que prova que você não apenas domina as habilidades avançadas de testes de penetração, mas também tem a capacidade de pensar lateralmente e agir sob pressão.
- https://www.offensive-security.com/information-security-training/cracking-the-perimeter/

PRATICA

WEB APPLICATION

INTRODUCTION

APLICAÇÃO WEB

- Em computação, **aplicação web** designa, de forma geral, sistemas de informática projetados para utilização através de um navegador, através da internet ou aplicativos desenvolvidos utilizando tecnologias web HTML, JavaScript e CSS. Pode ser executado a partir de um servidor HTTP (*Web Host*) ou localmente, no dispositivo do usuário.
- Uma aplicação web também é definida em tudo que se é processado em algum servidor, exemplo: quando você entra em um e-commerce a página que você acessa antes de vir até seu navegador é processada em um computador ligado a internet que retorna o processamento das regras de negócio nele contido. Por isso se chama aplicação e não simplesmente site web.
- A função do servidor web é receber uma solicitação (requisição) e devolver (resposta) algo para o cliente.O browser permite ao usuário solicitar um recurso e quando o servidor responde a uma solicitação são encontrados recursos como: páginas HTML, figuras e documento PDF que são exibidas depois para o usuário. Geralmente os servidores enviam instruções para o browser escritas em HTML. O HTML diz ao browser como apresentar conteúdo ao usuário web.
- O servidor em si tem alguns recursos, mas por algumas deficiências não consegue processar tudo sozinho como: criações de páginas dinâmicas e o armazenamento de dados em um banco de dados.

APLICAÇÃO WEB

- Páginas dinâmicas – Quando a aplicação roda no servidor, este disponibiliza somente páginas estáticas. Porém, para efetuar essa comunicação é necessário o auxílio de uma outra aplicação de ajuda que é passada através de Servlet.
- Armazenar dados no servidor – Para efetuar essa ação o servidor precisa de uma aplicação de apoio (Servlet), fazendo com que o servidor envie esses parâmetros para o Servlet.
- As falhas de segurança podem surgir em diferentes etapas, tais como: análise de requisito; especificação; Implementação. Os riscos de aplicação na vulnerabilidade de uma empresa pode causar impactos.
- O HTTP usa um modelo de solicitações e respostas. Uma solicitação ocorre quando o usuário faz uma solicitação HTTP e o servidor web devolve uma resposta HTTP, sendo que o browser verifica como tratar esse conteúdo. Se a resposta que vem do servidor for uma página HTML, então é inserido na resposta HTTP.
- As diferenças entre as solicitações GET e POST são que enquanto o GET anexa dados do formulário no final da URL o POST inclui dados do formulário no corpo da solicitação.

SaaS

- **Software como serviço**, do inglês ***Software as a service (SaaS)***, é uma forma de distribuição e comercialização de *software*. No modelo *SaaS*, o fornecedor do software se responsabiliza por toda a estrutura necessária à disponibilização do sistema (servidores, conectividade, cuidados com segurança da informação), e o cliente utiliza o software via internet, pagando um valor pelo serviço.
- O modelo SaaS oferece software como serviço com propósitos específicos que estão disponíveis para os usuários na Internet. Os sistemas de software são acessíveis a partir de vários dispositivos por meio de uma interface cliente em uma rede de modelo cliente-servidor como um navegador Web. No SaaS, o usuário não administra as características individuais da aplicação, exceto configurações específicas. Sendo assim, os desenvolvedores se concentram em atualização e não na infraestrutura, levando ao desenvolvimento rápido de sistemas de software.
- A tecnologia utilizada não determina o modelo. O software utilizado pode ser inteiramente pela internet (utilizado via navegador) ou pode ter alguma instalação local (como no caso de softwares antivírus ou de backup). A característica principal é a não aquisição das licenças vitalícias, mas sim o direito pelo uso da licença a partir de pagamentos recorrentes, normalmente mensal ou anual.
- O modelo de serviço SaaS (Software as a Service) a receita gerada por um cliente vem ao longo de um período extenso. A maioria gera receita a partir de uma mensalidade (ou até mesmo anuidade). Caso o cliente fique insatisfeito por algum motivo ou perca o interesse pelo serviço, vai descontinuar o uso, fazendo com que a empresa incorra na perda dos recursos gastos para trazer e conquistá-lo.

CLIENT AND SERVER

- O **modelo cliente-servidor** (em inglês *client/server model*), em computação, é uma estrutura de aplicação distribuída que distribui as tarefas e cargas de trabalho entre os fornecedores de um recurso ou serviço, designados como servidores, e os requerentes dos serviços, designados como clientes.
- Geralmente os clientes e servidores comunicam através de uma rede de computadores em computadores distintos, mas tanto o cliente quanto o servidor podem residir no mesmo computador.
- Um servidor é um *host* que está executando um ou mais serviços ou programas que compartilham recursos com os clientes. Um cliente não compartilha qualquer de seus recursos, mas solicita um conteúdo ou função do servidor. Os clientes iniciam sessões de comunicação com os servidores que aguardam requisições de entrada.
- O modelo cliente-servidor foi desenvolvido na Xerox PARC durante os anos 70. Este modelo é atualmente o predominante nas redes informáticas. Email, a World Wide Web e redes de impressão são exemplos comuns deste modelo.

ADVANCED EXPLOIT

CROSS SITE SCRIPTING

CROSS SITE SCRIPTING

- Os ataques de Cross-Site Scripting (XSS) são um tipo de injeção, na qual scripts maliciosos são injetados em sites de outra forma benignos e confiáveis. Ataques XSS ocorrem quando um invasor usa um aplicativo da Web para enviar código mal-intencionado, geralmente na forma de um script do lado do navegador, para um usuário final diferente. As falhas que permitem que esses ataques sejam bem-sucedidos são bastante difundidas e ocorrem em qualquer lugar em que um aplicativo da Web use a entrada de um usuário na saída gerada sem validá-lo ou codificá-lo.
- Um invasor pode usar o XSS para enviar um script mal-intencionado a um usuário desavisado. O navegador do usuário final não tem como saber que o script não deve ser confiável e irá executar o script. Como ele acredita que o script veio de uma fonte confiável, o script mal-intencionado pode acessar cookies, tokens de sessão ou outras informações confidenciais retidas pelo navegador e usadas com esse site. Esses scripts podem até reescrever o conteúdo da página HTML.

CROSS SITE SCRIPTING

- Ataques Cross-Site Scripting (XSS) ocorrem quando:

Os dados entram em um aplicativo da Web por meio de uma fonte não confiável, com mais frequência uma solicitação da web.

Os dados são incluídos no conteúdo dinâmico que é enviado a um usuário da web sem ser validado para conteúdo malicioso.

- O conteúdo mal-intencionado enviado ao navegador da Web geralmente assume a forma de um segmento de JavaScript, mas também pode incluir HTML, Flash ou qualquer outro tipo de código que o navegador possa executar. A variedade de ataques baseados em XSS é quase ilimitada, mas eles geralmente incluem a transmissão de dados privados, como cookies ou outras informações da sessão, ao invasor, redirecionando a vítima ao conteúdo da Web controlado pelo invasor ou realizando outras operações maliciosas na máquina do usuário. sob o disfarce do site vulnerável.

CROSS SITE SCRIPTING: TIPOS

- Os ataques XSS geralmente podem ser categorizados em duas categorias: armazenados e refletidos. Há um terceiro tipo de ataque XSS, muito menos conhecido, chamado XSS baseado em DOM.

CROSS SITE SCRIPTING: TIPOS

Ataques XSS armazenados

- Ataques armazenados são aqueles em que o script injetado é permanentemente armazenado nos servidores de destino, como em um banco de dados, em um fórum de mensagens, registro de visitantes, campo de comentários etc. A vítima recupera o script mal-intencionado do servidor quando solicita o armazenamento armazenado. em formação. O XSS armazenado também é conhecido como XSS Persistente ou Tipo-I.

Ataques XSS Refletidos

- Os ataques refletidos são aqueles em que o script injetado é refletido no servidor da Web, como em uma mensagem de erro, resultado da pesquisa ou qualquer outra resposta que inclua parte ou a totalidade da entrada enviada ao servidor como parte da solicitação. Os ataques refletidos são entregues às vítimas por meio de outra rota, como em uma mensagem de email ou em outro site. Quando um usuário é levado a clicar em um link mal-intencionado, enviando um formulário especialmente criado ou até mesmo navegando em um site malicioso, o código injetado viaja para o site vulnerável, que reflete o ataque de volta ao navegador do usuário. O navegador então executa o código porque veio de um servidor "confiável". O XSS refletido também é conhecido como XSS Não Persistente ou Tipo II.

CROSS SITE SCRIPTING: TIPOS

Ataques XSS baseado em DOM

- A vulnerabilidade DOM (*Document Object Model*) Based XSS executa todos os códigos Java Script maliciosos localmente no browser da vítima, sem ter contato direto com o servidor. Esse tipo de ataque é menos comum pois depende que a página alvo tenha componentes específicos que permitam que a ativação dos códigos aconteça em tempo de execução, ao invés de ficar atrelado a página como os ataques anteriores.

CROSS SITE SCRIPTING: ATAQUES

Vamos ver como funciona o ataque?

https://www.youtube.com/watch?v=nTvWqtYc5WY&t=361s

https://www.youtube.com/watch?v=D--gCvOS59g

https://www.youtube.com/watch?v=kh30ylrpU68

https://www.youtube.com/watch?v=QTS9jxaiHzw

https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)

https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)

https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)

https://www.youtube.com/watch?v=gkMI1suyj3M

CROSS SITE SCRIPTING: CENÁRIO REAL

Vamos ver alguns cenários reais?

https://medium.com/@rohanchavan/a-unique-xss-scenario-1000-bounty-347f8f92fcc6

https://www.youtube.com/watch?v=dVkDbmY8_wo

https://omespino.com/write-up-1000-usd-in-5-minutes-xss-stored-in-outlook-com-ios-browsers/

https://www.youtube.com/watch?v=IG7U3fuNw3A

https://www.youtube.com/watch?v=YdXkw3DwDd4

https://www.youtube.com/watch?v=gVrdE6g_fa8

https://medium.com/bugbountywriteup/900-xss-in-yahoo-recon-wins-65ee6d4bfcbd?source=false--------1

https://medium.com/bugbountywriteup/file-upload-xss-patched-83ea55bb9a55?source=false--------8

CROSS SITE SCRIPTING: DICAS

- Utilize diferentes payloads
- Estude os tipos de XSS, o conceito é o mesmo, mas o que muda é a forma de exploração
- Então procure Write-ups sobre xss
- Bounty relacionados a falha de XSS
- Métodos para burlar um WAF
- Estudar JavaScript e APIs

ADVANCED EXPLOIT

Path Traversal

PATH TRAVERSAL

- **Path traversal** é uma das vulnerabilidades (erro de software) mais perigosas segundo o CWE/SANS Top 25. É um ataque utilizado por atacantes para obter acesso não autorizado a arquivos e diretórios, e através da sua exploração é possível comprometer completamente o servidor onde a aplicação se encontra.

PATH TRAVERSAL: ATAQUES

- **Vamos ver alguns ataques**
- https://www.infosec.com.br/path-traversal/
- https://www.youtube.com/watch?v=jJ0ijQ5pADE
- https://www.youtube.com/watch?v=ZYbU9_cksUs
- https://www.youtube.com/watch?v=DmGVipmtTS8

PATH TRAVERSAL: ATAQUES

- **Vamos ver alguns cenários**
- https://bugbountyforum.com/blog/security/exploiting-directory-traversal-on-yahoo/
- https://shahmeeramir.com/traversing-the-path-to-5000-in-help-33750808704d
- https://medium.com/bugbountywriteup/find-path-traversal-cve-2005-3299-with-nmap-bada0eb72947
- https://en.internetwache.org/paypal-fixes-a-path-traversal-vulnerability-18-09-2013/
- https://twitter.com/0x01alka/status/826520689595265026

ADVANCED EXPLOIT

Backdoor

BACKDOOR

- Um backdoor é um meio de acessar um sistema de computador ou dados criptografados que ignoram os mecanismos de segurança habituais do sistema.
- Um desenvolvedor pode criar um backdoor para que um aplicativo ou sistema operacional possa ser acessado para solução de problemas ou outros fins. No entanto, os invasores geralmente usam backdoors que detectam ou instalam-se como parte de uma exploração . Em alguns casos, um worm ou vírus é projetado para tirar proveito de um backdoor criado por um ataque anterior.
- Seja instalado como uma ferramenta administrativa, um meio de ataque ou como um mecanismo que permite ao governo acessar dados criptografados, um backdoor é um risco de segurança, pois sempre tem criminosos ou hackers em busca de qualquer vulnerabilidade a ser explorada.

ADVANCED EXPLOIT

Backdooring PE exploit Windows

BACKDOOR PE

- Um **code cave** é uma série de bytes nulos na memória de um processo. O **code cave** dentro da memória de um processo geralmente é uma referência a uma seção das funções de script do código que tem capacidade para a injeção de instruções personalizadas. Por exemplo, se a memória de um script permitir 5 bytes e apenas 3 bytes forem usados, os 2 bytes restantes poderão ser usados para adicionar algum código externo ao script.

- Mais informações: https://www.codeproject.com/Articles/20240/The-Beginners-Guide-to-Codecaves

BACKDOOR PE: PRÁTICA e EXPLORAÇÃO DO WINDOWS

- https://captmeelo.com/exploitdev/osceprep/2018/07/16/backdoor101-part1.html
- **Backdoor Windows:** https://resources.infosecinstitute.com/back-dooring-pe-files-windows/#gref
- http://sector876.blogspot.com/2013/03/backdooring-pe-files-part-1.html
- https://www.cybrary.it/0p3n/windows-hacking-1-inject-backdoor-pe-file/
- https://haiderm.com/fully-undetectable-backdooring-pe-file/
- https://hansesecure.de/2018/06/backdooring-pe-file-with-aslr/
- https://www.youtube.com/watch?v=UdvoSBPjUgY
- https://gist.github.com/mgeeky/2193d0416e3c4ce49996ee6616e0bf0b

ADVANCED EXPLOIT

TÉCNICAS AVANÇADAS EM WINDOWS

MS07-017 – Dealing with Vista

- Vulnerabilidades no GDI que pode permitir a execução remota de código
- https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2007/ms07-017
- Detalhes da falha: https://support.microsoft.com/en-us/help/925902/ms07-017-vulnerability-in-gdi-could-allow-remote-code-execution

MS07-017 – Dealing with Vista: GDI

- **GDI**, ou **Graphics Device Interface**, é um dos três subsistemas principais do Microsoft Windows. É um padrão desse sistema operacional para representar objectos gráficos e transmiti-los para dispositivos de saída, como monitores e impressoras.

MS07-017 – Dealing with Vista: PRÁTICA

- https://medium.com/@notsoshant/windows-exploitation-aslr-bypass-ms07-017-8760378e3e84
- https://www.exploit-db.com/exploits/3688
- https://www.exploit-db.com/exploits/3804
- https://www.exploit-db.com/exploits/3755
- https://www.rapid7.com/db/vulnerabilities/WINDOWS-HOTFIX-MS07-017
- https://securiteam.com/windowsntfocus/5NP041FL5K/

CRACKING THE EGGHUNTER

- **O Egg Hunter** é uma técnica usada durante odesenvolvimento de **explorações** que pode pesquisar todo o intervalo de memória para um shellcode e redirecionar o fluxo para ele.

CRACKING THE EGGHUNTER: PRÁTICA

- https://www.nipunjaswal.com/2018/01/art-of-shellcoding-cracking-eggs-with-egghunters.html
- https://www.exploit-db.com/exploits/46018
- https://www.offensive-security.com/metasploit-unleashed/egghunter-mixin/
- https://medium.com/@rafaveira3/exploit-development-kolibri-v2-0-http-server-egg-hunter-example-1-5e435aa84879
- https://medium.com/egghunter/lampi%C3%A3o-1-vulnhub-walkthrough-c334aaa68cb9
- https://medium.com/@notsoshant/windows-exploitation-egg-hunting-117828020595
- https://subscription.packtpub.com/book/networking_and_servers/9781787121829/9/ch09lvl1sec94/exploiting-egg-hunters
- https://snowscan.io/egghunter/

ADVANCED EXPLOIT

0DAY de diferentes angulos

0DAY

- Uma nova vulnerabilidade que ainda não conta com *patch* ou revisões e pode ser empregada para realizar um ataque. O nome *0-day* (dia zero) faz referência a inexistência de revisões para minimizar o aproveitamento da vulnerabilidade.

0DAY Angle: Prática

- **Exploit Adobe 0day:** https://www.fireeye.com/blog/threat-research/2015/01/a_different_exploit.html
- **Exploit TFTP:** https://www.exploit-db.com/exploits/5314
- https://www.offensive-security.com/metasploit-unleashed/simple-tftp-fuzzer/
- https://github.com/nullsecuritynet/tools/tree/master/fuzzer/tftp-fuzz
- https://packetstormsecurity.com/files/111182/TFTP-Fuzzer-Script.html
- **Exploit HP OpenView NNM:** https://www.youtube.com/watch?v=2o3t16ED8g0
- https://www.youtube.com/watch?v=5CEAJTANsZk
- https://www.youtube.com/watch?v=CB625M1lWoo
- https://www.offensive-security.com/0day/hp-nnm-ov.py.txt
- https://greyshell.github.io/blog/2016/11/07/hpnmm-exploit/
- https://stateofsecurity.com/hp-openview-nnm-0day-lightthpd-dos/

ADVANCED EXPLOIT

NETWORK ATTACK ANGLE

NETWORK ATTACK ANGLE

- Alguns ângulos de ataques em infraestrutura
- Explorando falhas em serviços, equipamentos ou alguma configuração de um sistema

NETWORK ATTACK ANGLE: PRÁTICA

- **Bypassing Cisco Access Lists using Spoofed SNMP Requests:** https://securiteam.com/securitynews/5cp062agkc/
- https://www.reddit.com/r/networking/comments/6khyw2/bypassing_snmp_acls_on_a_cisco_router/
- https://github.com/nccgroup/Cisco-SNMP-Slap
- https://www.symantec.com/connect/articles/cisco-snmp-configuration-attack-gre-tunnel
- http://securiteam.net/securitynews/5CP062AGKC.html
- https://9emin1.github.io/progress/work/2019/02/11/osce-thoughts-and-opinions.html

NETWORK ATTACK ANGLE: PRÁTICA

- **Sniffing Remote Traffic via GRE tunnel:**
- https://worldhack3r.wordpress.com/2013/05/16/sniffing-remote-router-traffic-via-gre-tunnels/
- https://www.youtube.com/watch?v=ekz8LgTsD2o
- https://www.youtube.com/watch?v=XtnLiWjXRWg
- https://www.youtube.com/watch?v=wRIJe_depSI
- https://www.dailymotion.com/video/x3nkfac

CTP/OSCP/OSCE

https://www.securitysift.com/offsec-ctp-osce/
http://theevilbit.blogspot.com/2014/11/my-ctp-osce-story.html

REFERÊNCIAS

- https://pt.wikipedia.org/wiki/Software_como_servi%C3%A7o
- https://pt.wikipedia.org/wiki/Aplica%C3%A7%C3%A3o_web
- https://pt.wikipedia.org/wiki/Cliente-servidor
- https://www.owasp.org/index.php/DOM_Based_XSS
- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.welivesecurity.com/br/2018/12/27/cross-site-scripting-xss-entenda-o-que-e-e-saiba-como-estar-protegido/
- http://www.andradesoto.com.br/2017/02/28/a-vulnerabilidade-path-traversal/
- https://www.owasp.org/index.php/Path_Traversal

FIM

Parceiros:

https://www.facebook.com/cybersecup
https://www.facebook.com/Expersec/
https://www.facebook.com/exchangesec/
https://www.facebook.com/como.hackear.curso/
https://www.facebook.com/deepcript/