Red Team Operations
24 Maio 2024

Rooted Portugal

TRAINING DOSSIER

/RootedPT

Portugal

24 e 25 de Maio

Apresentações de oradores internacionais e profissionais técnicos

Fundação Oriente (Lisboa)

Apresentação

- Missão: queremos partilhar conhecimentos, atrair diferentes culturas, expor o talento local e fazer a diferença.
- Visão: ser responsável por fazer algo diferente, partilhando cultura e construindo uma rede de conhecimento. Ser um evento honesto, fiável e rentável e estabelecer alianças e colaborações com parceiros, clientes e concorrentes.
- A nossa cultura vencedora e os nossos valores fundamentais: colaboração, diversidade, talento em todo o lado, paixão, qualidade e atenção ao cliente (cada pessoa que participa nos nossos congressos).

Formador: Eduardo Arriols

- CEO e Diretor Ofensivo da SilentForce, uma start-up especializada em Simulação Adversária e desenvolvimento de produtos para a proteção e gestão da superfície de ataque na Internet.
- 13 anos de experiência em segurança ofensiva, e mais de 8 anos a desenvolver e coordenar exercícios de Red Team em grandes organizações nacionais e internacionais.
- Professor de graduação e pós-graduação em Cibersegurança em diversas universidades.
- Autor do livro "CISO: The Company's Red Team", da editora 0xWord.
- Orador em conferências nacionais e internacionais como Defcon, RootedCON, Navaja Negra, STIC Conference (CCN-Cert) e 8.8 Security Conference (Chile e Bolívia).
- Engenheiro informático pela UAM e mestre em Cibersegurança pela UOC.

Objetivos

O objetivo desta formação é dotar os participantes de capacidades para desenvolver exercícios de intrusão e simulações de ataques reais, compreendendo o processo, fases e ações, bem como as técnicas, ferramentas e orientações.

Durante a formação, os alunos irão trabalhar os principais aspectos para desenvolver uma intrusão, desde o reconhecimento de activos no perímetro e procura de vectores de acesso, até acções internas como movimento lateral entre sistemas, comprometimento da infraestrutura ou implantação de persistência, entre outros. Devido às limitações de tempo, será dada prioridade às técnicas e acções de intrusão na infraestrutura interna.

A formação têm o objetivo claro de mostrar de forma prática uma metodologia e técnicas úteis para o desenvolvimento de ataques direcionados, razão pela qual não se aprofundará em técnicas que vão para além disso. Os alunos terão acesso a um laboratório, tanto local como na nuvem, para simular todas as técnicas aprendidas.

A quem se dirige?

A formação não se destina a servir de introdução ao hacking ético, uma vez que o objetivo é aprofundar técnicas avançadas que permitam o desenvolvimento de intrusões reais. Por conseguinte, a formação está especialmente vocacionada para os profissionais do sector da cibersegurança e, em especial, para os profissionais ligados à auditoria de segurança e ao pentesting.

A formação está também aberta, em qualquer caso, a todos aqueles que já possuam conhecimentos de auditoria que serão apresentados posteriormente, tais como: estudantes, programadores, administradores de sistemas e/ou redes, Forças e Corpos de Segurança, bem como qualquer pessoa que esteja interessada em aprender e aprofundar o desenvolvimento de exercícios de Red Team.

Conhecimentos necessários

Conhecimentos básicos de:

- ✔ Administração e gestão de sistemas Windows ou Linux.
- ✔ Programação básica em linguagens como Bash scripting e Python.
- ✔ Funcionamento e operações de ambientes Microsoft com Active Directory.
- ✔ Utilização de ferramentas de hacking ético como Metasploit, Nmap, Sqlmap,...
- ✔ Processo de intrusão e exploração de vulnerabilidades em sistemas e redes.
- ✔ Exploração de vulnerabilidades web como SQL Injection, XSS, RCE ou File Upload.

Para o máximo aproveitamento da formação, será fornecido antes do início, material teórico sobre o desenvolvimento dos exercícios e aspectos básicos que o aluno deve ler.

Requisitos técnicos

Para que a formação funcione corretamente, será necessário que os alunos disponham de computadores com acesso de administrador para poder adicionar, apagar software ou alterar qualquer configuração do mesmo.

As máquinas devem ter as seguintes características mínimas:

- ✔ Acesso de administrador aos equipamentos pessoais que serão utilizados no laboratório.
- ✔ Capacidade de ligação com e sem fios.
- ✔ Capacidade para executar três máquinas virtuais em simultâneo utilizando VMware Workstation/Player ou VirtualBox (as máquinas serão fornecidas em .ova).
- ✔ 120 GB de espaço livre em disco.
- ✔ Pelo menos 12 GB de RAM.

Agenda

1. Introdução e conceitos básicos
2. Implementação da infra-estrutura
3. Reconhecimento da superfície de ataque
4. Vectores de acesso
5. Obtenção de credenciais e cracking de palavras-passe
6. Movimento lateral e técnicas de pivotagem
7. Técnicas de ataque ao domínio
8. Implantação de persistência

A formação centrar-se-á e aprofundará as técnicas que são novas ou que são atualmente muito utilizadas no desenvolvimento de cenários de intrusão. Os participantes terão acesso a ferramentas SilentForce privadas para automatizar acções durante o processo de intrusão.

Informação adicional (i)

1. Introdução e conceitos básicos: Todos os conhecimentos necessários sobre os detalhes da metodologia e fases do modelo de intrusão, Ameaça e Violação, potenciais vetores em função da organização, técnicas de medição e análise das capacidades de deteção e resposta da Blue Team, bem como aspectos a ter em conta em matéria de OPSEC nos exercícios de Red Team.

2. Implementação da infra-estruturas: Detalhes, orientações e metodologia para a construção de infra-estruturas de enumeração, intrusão, persistência e anonimato na Cloud. Será aprofundado o desenvolvimento de uma plataforma de anonimato para a ocultação de acções, a implantação de sistemas C&C para a receção de comunicações em túnel e a persistência, bem como técnicas como o Domain Fronting ou o IP Laundry.

Informação adicional (ii)

3. Reconhecimento da superfície de ataque: Conjunto de técnicas para mapear todos os activos sobre os quais serão efectuados testes de intrusão para obter um vetor de acesso, dando especial ênfase à detecção de activos não controlados (Shadow IT) e à hierarquização de activos.

4. Vectores de acesso: Principais vectores de acesso ao perímetro e tunelamento através de ferramentas como o reGeorg/NeoRegeorg, ataques de pulverização de palavras-passe, evasão de 2FA ou falsificação de serviços Internet.

5. Obtenção de credenciais e cracking de palavras-passe**:** Conjunto de técnicas para obter credenciais durante o processo de intrusão, como a obtenção de chaves através de ficheiros locais, DPAPI, chaves, hashes e bilhetes em memória ou falsificação de serviços, tanto localmente como na rede. Além disso, serão analisadas as diferentes técnicas (dicionários, utilização de regras, máscaras, combinações e ataques híbridos) para a recuperação de palavras-passe claras.

Informação adicional (iii)

6. Técnicas de movimentação lateral e de pivotagem: Conjunto de técnicas de acesso para se deslocar entre computadores, redes e domínios internos, acedendo a sistemas, com a utilização de protocolos permitidos como SSH, SMB, WMI, WinRM ou DCOM. As diferentes técnicas possíveis serão analisadas em função do nível de credenciais obtidas (pass-the-hash, overpass-the-hash, pass-the-ticket, ...). Para além disso, serão analisadas as técnicas de compromisso e de movimento lateral em MSSQL.

7. Técnicas de ataque ao domínio: Principais técnicas para obter controlo sobre a infraestrutura Microsoft através da utilização de ataques como Kerberoast, ASREPRoast, Unconstrained/Contraned Delegations, Alternate Service Name, Linux Cache Credentials, DACLs ou relações de confiança, entre outros.

8. Implantação de persistência: Técnicas para o desdobramento de persistência sobre a organização em todos os níveis (sistemas internos, Directorio Ativo, DMZ, Cloud e técnicas alternativas). Aprofundar-se-á tanto nas técnicas para manter a persistência, como nas vias de comunicação ou uso dessas persistências.

Preço da formação

- O Preço da formação RootedLAB é de €180

- Pode inscrever-se e efetuar o pagamento em: https://reg.rootedcon.com

IMPORTANTE:

É necessário um mínimo de DEZ (10) participantes para que o curso se realize.

FAQ

- Onde é que se realiza a formação?
  - A formação realiza-se na Fundação Oriente em Lisboa. Google Maps
- Duração da formação?
  - A formação terá uma duração prevista de 8 horas.
- Que horário têm a formación?
  - A formação começa às 9h, comparece um pouco antes para realizar o processo de acreditação e teres o portátil preparado :)
  - As formações normalmente acabam entre as 18h e 19h.
- Como posso inscrever-me?
  - Para se inscrever, vá diretamente para o RootedManager RootedManager: https://reg.rootedcon.com. Uma vez inscrito, poderá selecionar a formação e pagar diretamente. Uma vez confirmada a formação, pode solicitar a fatura seguindo os passos indicados.
- Posso pagar por transferência bancária?
  - Sim, a partir do RootedManager é possível gerir o pagamento por transferência bancária
- A formação inclui alimentação?
  - A formação não inclui alimentação. Mas existem várias opções na zona, e o professor dar-te-á mais informações.

/Rooted

Contacto:

info@rootedcon.com