TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 1. Introdução ao Hacking Ético

Módulo 2. Footprinting e Reconhecimento

Módulo 3. Scanning de Redes

Módulo 4. Enumeração

Módulo 5. Análise de Vulnerabilidade

Conceitos de enumeração:

Enumeração é definida como o processo de extração de nomes de usuário, nomes de máquinas, recursos de rede, compartilhamentos e serviços a partir de um sistema. Na fase de enumeração, o atacante cria conexões ativas com o sistema e executa consultas dirigidas para obter mais informações sobre o alvo. O atacante utiliza as informações coletadas para identificar as vulnerabilidades ou pontos fracos de segurança do sistema e, em seguida, tentar explorá-los.

CEHv12 (ANSI)

Conceitos de enumeração

Técnicas utilizadas

- Consultas de DNS
- Enumeração de rede
- Consultas de rede
- Identificação do Sistema Operacional
- Consultas organizacionais
- Ping sweepes
- Consultas de ponto de contato
- Varredura de portas
- Consultas do registrador (consultas WHOIS)
- consultas SNMP
- Spidering na World Wide Web

Kali/Ubuntu/Debian/Parrot Linux Install

```
git clone https://github.com/1N3/Sn1per
cd Sn1per
bash install.sh
```

Tipos de Footprinting

- **OPEN SOURCE OR PASSIVE INFORMATION GATHERING** – Coleta de informação passiva ou open source é a maneira mais fácil de coletar informações sobre a organização-alvo.
- **ACTIVE INFORMATION GATHERING** – Na coleta de informação ativa, o processo tomado pelo atacante incide essencialmente sobre os funcionários da organização-alvo.
- **ANONYMOUS FOOTPRINTING** – Refere-se ao processo de coleta de informações de fontes anônimas para que as atividades realizadas não possam ser rastreadas.
- **PSEUDONYMOUS FOOTPRINTING** – Pseudonymous footprinting refere-se ao processo de coleta de informações a partir das fontes que foram publicadas na Internet, mas não está diretamente ligada ao nome do autor.
- **ORGANIZATIONAL PRIVATE FOOTPRINTING** – Organizational Private Footprinting envolve a coleta de informações de serviços de calendário baseados na web e e-mail de uma organização.
- **INTERNET FOOTPRINTING** – Internet Footprinting refere-se ao processo de coleta de informações sobre a conexão de internet do alvo.

Informações sobre a rede

- Nome do domínio externo
- Nomes de domínio interno
- Blocos de rede
- Endereços IP dos sistemas alcançáveis
- Sites privados
- Serviços TCP e UDP em execução
- Mecanismos de controle de acesso e ACL’s
- Protocolos de rede
- Pontos VPN
- IDS/IPS em execução
- Números de telefone analógicos/digitais
- Mecanismos de autenticação
- Informações sobre o sistema

Informações sobre o sistema

- Nomes de usuários e grupos
- Nome do sistema
- Tipo de sistema
- Banners do sistema
- Tabelas de roteamento
- Informações SNMP
- Arquitetura do sistema
- senhas

Informações da organização

- Detalhes dos funcionários
- Sites da organização
- Diretório da empresa
- Detalhes do local
- Endereço e telefones
- Comentários no código-fonte HTML
- Políticas de segurança implementadas
- Links de servidores da Web relevantes para a empresa
- Antecedentes da organização
- Novos artigos
- artigos de imprensa

Metodologia de Footprinting:

O programa CEH (ANSI) exige que o candidato tenha dois anos de experiência profissional no domínio da Segurança da Informação e deve ser capaz de fornecer uma prova do mesmo conforme validado através do processo de candidatura, a menos que o candidato frequente um treinamento oficial.

https://cert.eccouncil.org/application-process-eligibility.html

Exame com treinamento oficial:

Se um candidato concluiu um treinamento oficial da EC-Council em um Centro de Treinamento Credenciado, por meio da plataforma iClass ou em uma instituição acadêmica aprovada, o candidato é elegível para tentar o exame EC-Council.

CEHv12 (ANSI)

Exame com treinamento oficial

Metodologia de Footprinting

- O objetivo do reconhecimento e/ou Footprinting é determinar o tamanho e o escopo do seu teste. Footprinting é apenas ter uma idéia da “pegada” da organização, ou seja, tamanho e aparência. Isso significa tentar identificar blocos de rede, hosts, locais e pessoas. As informações coletadas aqui serão utilizadas posteriormente à medida que você avança em estágios adicionais.

- Existem algumas maneiras de conduzir o reconhecimento ou Footprinting.
- Há dois tipos de Footprinting: ativo e passivo

1. Passivo envolve a coleta de informações sobre o alvo sem qualquer interação direta com os sistemas de destino ou rede.
2. Ativo requer algum nível de interação com o sistema alvo.

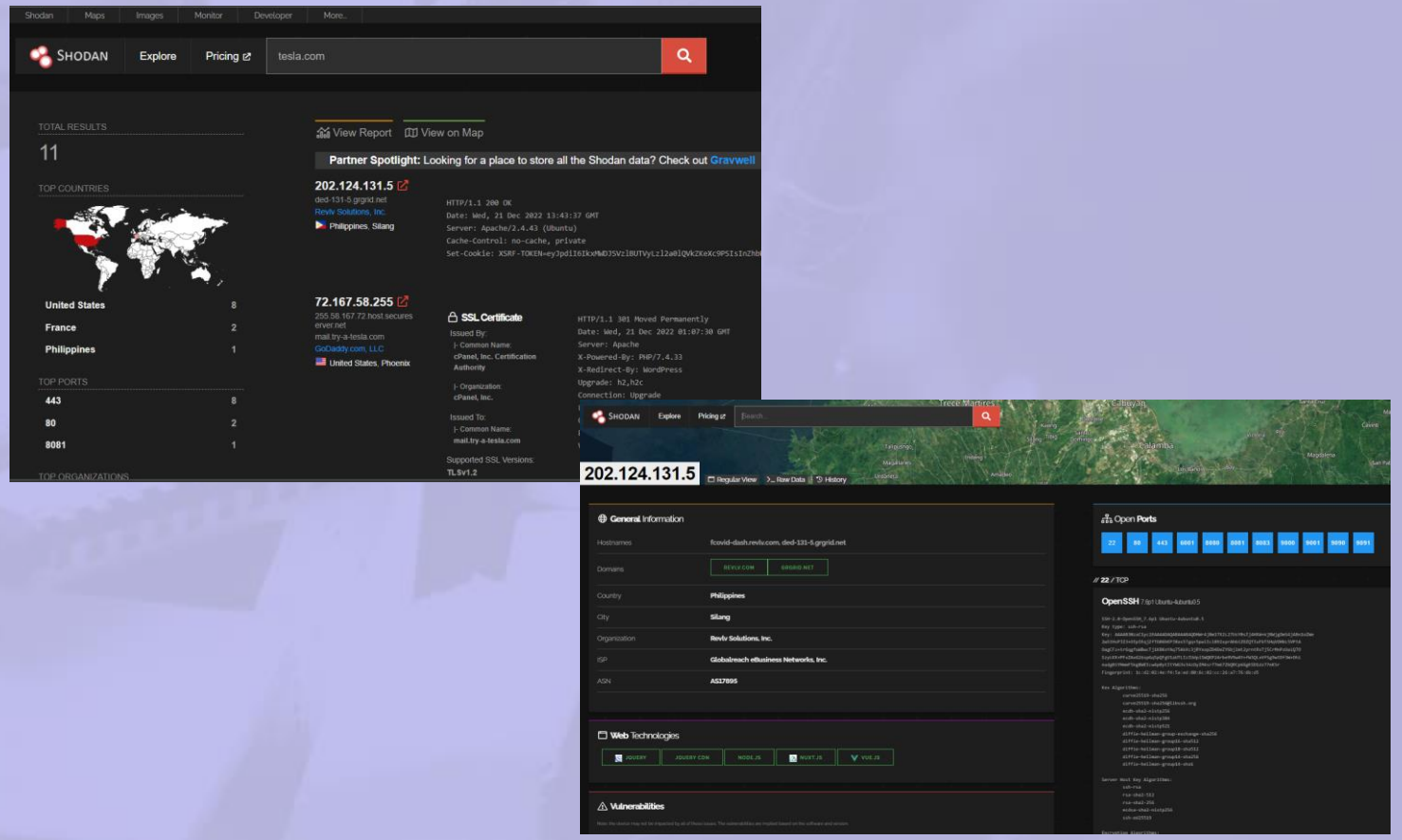
1. **Footprinting Através de motores de busca**
2. **Footprinting Utilizando Google Hacking Avançado**
3. **Footprinting Através de Redes Sociais**
4. **Footprinting em Websites**
5. **Footprinting em E-mail**
6. **Footprinting Competitive Intelligence**
7. **Footprinting de Whois**
8. **Footprinting de DNS**
9. **Footprinting de Rede**
10. **Footprinting Através de Engenharia Social**

Footprinting Através de motores de busca

- Atacantes utilizam motores de busca para extrair informações sobre um alvo, tais como tecnologias de plataforma, detalhes de empregados, paginas de login, portais de intranet e etc, que ajudam na realização de engenharia social e outros tipos de ataques avançados. Os caches dos motores de busca e arquivos de internet podem também fornecer informações sensíveis que foram removidas da internet.

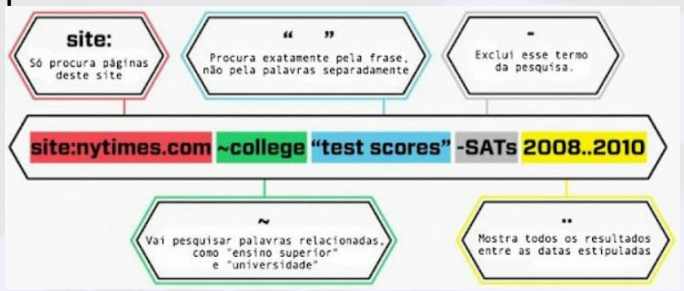
1 Footprinting Através de motores de busca

https://www.zoomeye.org/
https://search.censys.io/
https://www.shodan.io/



Footprinting Utilizando Google Hacking Avançado

- O Google possui diversos recursos que podem ser utilizados durante um teste de invasão e justamente por isso é considerada a melhor ferramenta para os atacantes, pois permite acesso a todo e qualquer tipo de informação que esteja desprotegida. Podemos usar como exemplo, o recurso de “cache” dos motores de busca, onde o mesmo armazena versões mais antigas de todos os sites que um dia já foram indexados por seus robôs.



2 Footprinting Utilizando Google Hacking Avançado

Operador	Exemplo	Propósito	Pode ser combinado com outros operadores
site	site:wikipedia.org	Busca um site específico	sim
related	related:wikipedia.org	Busca sites relacionados	sim
cache	cache:wikipedia.org	Busca com os sites salvos no cache do Google	sim
intitle	intitle:wikipedia	Busca um título de uma página	sim
inurl	inurl:wikipedia	Search URL	sim
filetype:env	filetype:pdf	Busca arquivos específicos	sim
intext	intext:wiki	Busca apenas no texto da página	sim
“”	“Wikipedia”	Busca por uma padrão exato	sim
+	jaguar + car	Busca por mais de uma palavra	sim
–	jaguar speed -car	Exclui palavras da busca	sim
OR	jaguar OR car	Combina duas palavras na busca	sim
*	how to * Wikipedia	Operador coringa, pode ser tudo ou nada na expressão	sim
imagesize	imagesize:320×320	Busca o tamanho da imagem	não
@	@wikipedia	Busca em redes sociais	sim
#	#wiki	Busca para hashtags	sim
$	camera $400	Busca preços	sim
..	camera $50..$100	Busca dentro de um leque de preços	sim

Footprinting Através de Redes Sociais

- Os atacantes criam perfis falsos em sites de redes sociais e depois utilizam a identidade falsa para manipular os funcionários e fazer com que eles passem as informações desejadas.
- Funcionários podem postar informações pessoais, tais como data de aniversário, nível de graduação, experiência profissional e informações sobre a organização tais como clientes em potenciais, parceiros de negócios, negócios secretos da organização, sites, notícias não divulgadas, aquisições e etc.

3 Footprinting Através de Redes Sociais

- **Facebook** a maior rede social do planeta possui uma base de usuários extremamente grande com um grande número de grupos para compartilhar interesses. Facebook também é usado para compartilhar comentários em uma infinidade de sites, tornando seu alcance ainda mais longe.
- **Twitter** tem milhões de usuários, muitos dos quais publicam atualizações várias vezes ao dia.
- **Google+** Esta é a resposta do Google ao popular Facebook. Embora o serviço ainda não tem a popularidade generalizada do Facebook, há uma boa dose de informações presentes no site que você pode pesquisar e usar.
- **LinkedIn** Um site muito bom para a coleta de informações pessoais. O site é uma plataforma de rede social para candidatos a emprego e, como tal, tem histórico de emprego, informações de contato, habilidades e nomes das pessoas com quem trabalha ou trabalhou.
- **Instagram** Este serviço de mídia social permite o compartilhamento de fotos on-line. O serviço é extremamente popular e é utilizado por um grande número de pessoas em todo o mundo.

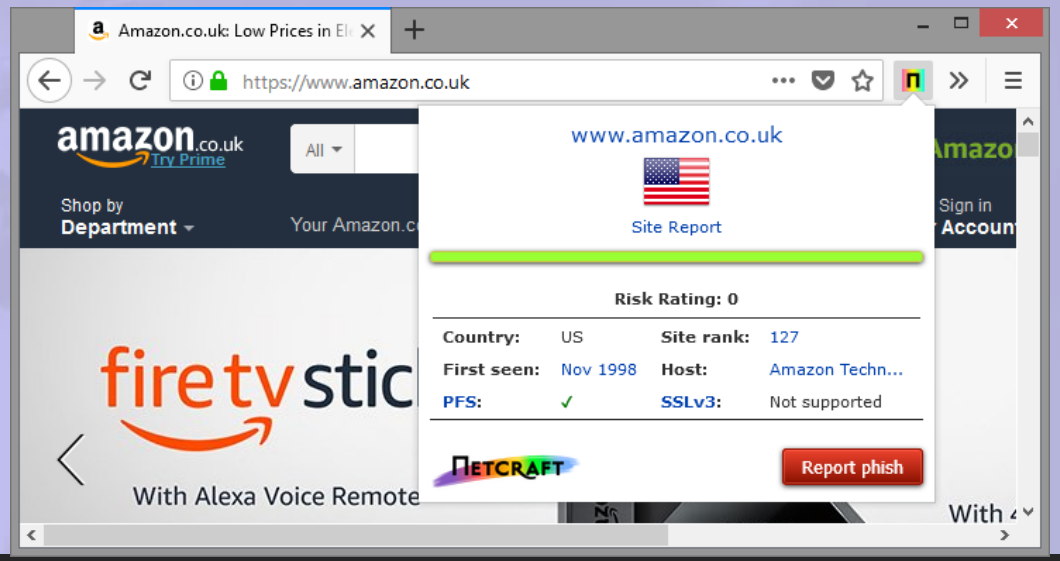
Footprinting em Websites

- É possível um atacante construir um mapa detalhado da estrutura de um website sem gerar alertas pelo IDS (Sistema de detecção de intrusão) ou despertar alguma suspeita no administrador do sistema. Utilizando a ferramenta Netcraft podemos reunir informações do site, como endereço IP, nome registado e endereço do proprietário do domínio, nome de domínio, host e etc. Mas esta ferramenta pode não dar todos estes detalhes para cada site. Nesses casos, você deve procurar o site de destino.

4 Footprinting em Websites

Navegando o site de destino irá fornecer-lhe as seguintes informações:

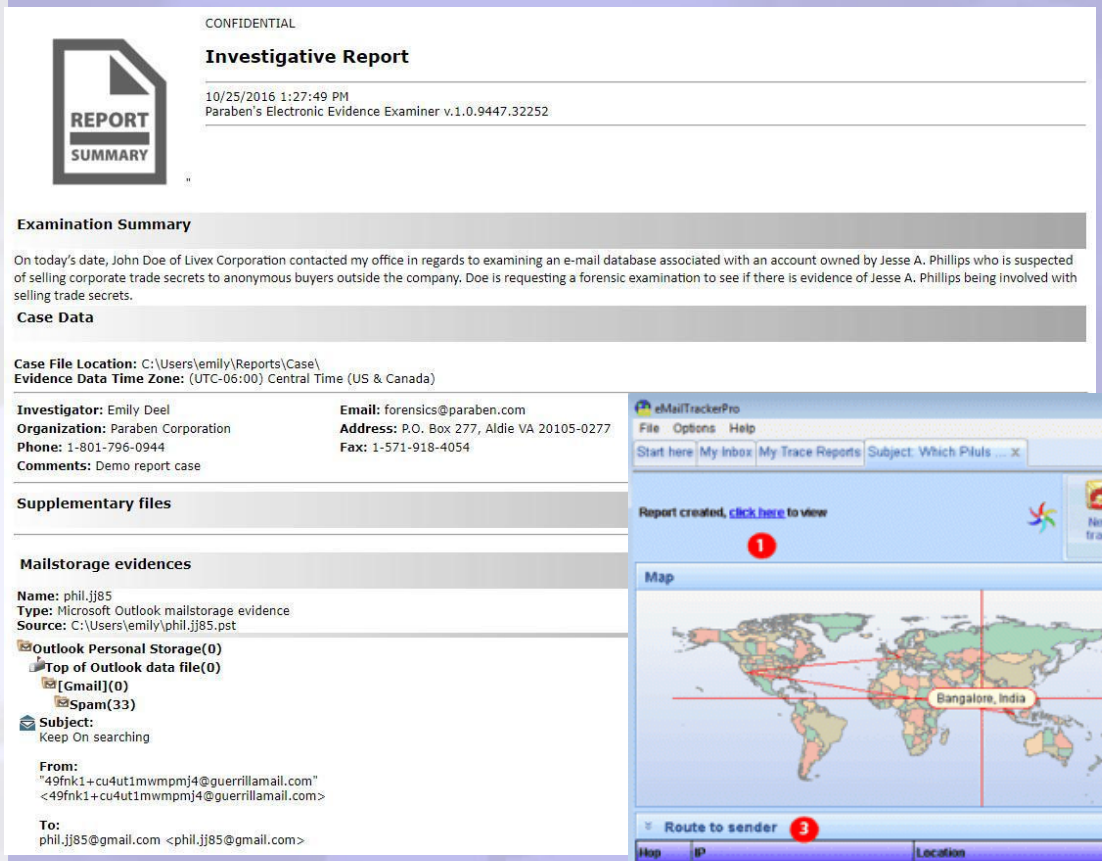
- Software utilizado e sua versão
- Sistema operacional utilizado
- Subdiretórios e parâmetros
- Nome do arquivo, caminho, nome de campo de banco de dados ou consulta
- Plataforma de script
- Detalhes de contato e detalhes do CMS



Footprinting em E-mail

5 **Footprinting em E-mail**

- O rastreamento de e-mail é um método que ajuda a monitorar, bem como acompanhar os e-mails de um usuário específico. Este tipo de acompanhamento é possível através dos registros de time stamp que revelam a hora e data em um e-mail, no qual foi recebido ou aberto pelo destino.
- Várias ferramentas de rastreamento de email estão disponíveis no mercado, com o qual você pode coletar informações como endereços IP, servidores de correio e prestador de serviços a partir do qual o e-mail foi enviado. Exemplos de ferramentas de rastreamento de e-mail incluem: eMailTrackerPro e Paraben E-mail Examiner.



Footprinting Competitive Intelligence

- Inteligência competitiva é um processo que reúne, analisa e distribui informações sobre produtos, clientes, concorrentes e tecnologias utilizando a Internet. A informação que é obtida pode ajudar os gestores e executivos de uma empresa tomar decisões estratégicas.
- Aquisição de informações sobre os produtos, concorrentes e tecnologias de uma empresa utilizando a Internet é definido como inteligência competitiva. Inteligência competitiva não é apenas sobre análise de concorrentes, mas também analisando os seus produtos, clientes, fornecedores, etc., que afetam a organização.

6 Footprinting Competitive Intelligence

Locais para obter informações competitivas:

- O **EDGAR** (o Sistema Eletrônico de Coleta, Análise e Recuperação de Dados) contém relatórios que as empresas negociadas publicamente fazem para a Securities and Exchange Commission (SEC). Saiba mais em www.sec.gov/edgar.shtml.
- **LexisNexis** mantém um banco de dados de informações de registro público sobre empresas que inclui detalhes como notícias legais e comunicados de imprensa. Saiba mais em www.lexisnexis.com/en-us/home.page
- **BusinessWire** (www.businesswire.com/portal/site/home/) é outro grande recurso que fornece informações sobre o status de uma empresa, bem como dados financeiros e outros.
- **CNBC** (www.cnbc.com) oferece uma riqueza de detalhes da empresa, bem como planos futuros e análise aprofundada.

Ao analisar esses recursos, procure por informações específicas que possam trazer ideias, como as seguintes:

- Quando a empresa começou?
- Como evoluiu?
- Essas informações dão uma visão de sua estratégia de negócios e filosofia, bem como cultura corporativa.
- Quem são os líderes da empresa?
- Análise de fundo adicional desses indivíduos pode ser possível.
- Onde estão a sede e os escritórios localizados?

Footprinting de Whois

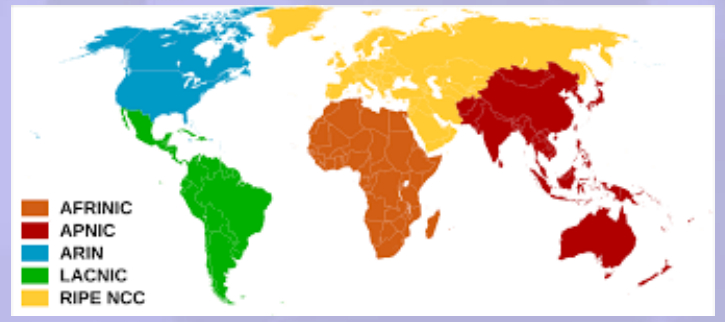
- WHOIS é um protocolo de consulta e de resposta utilizado para consultar bancos de dados que armazenam os registrados de usuários de um recurso na Internet, como um nome de domínio, um bloco de endereço IP ou um sistema autonomo. Bases de dados WHOIS são mantidas por Registros Regionais da Internet e contêm as informações pessoais dos proprietários de domínios.

7 **Footprinting de Whois**

Um Registro Regional da Internet (RIR) é uma organização que supervisiona a atribuição e registro dos recursos de números Internet dentro de uma determinada região do mundo. Os recursos incluem endereço IPs (tanto IPv4 como IPv6) e números de sistemas autônomos (para uso em roteamento BGP).

Atualmente, existem cinco RIRs em operação:

1. American Registry for Internet Numbers (ARIN):[1] América do Norte e partes do Caribe;
2. Réseaux IP Européens Network Coordination Centre (RIPE NCC):[2] Europa, Oriente Médio e Ásia Central;
3. Asia-Pacific Network Information Centre (APNIC):[3] Ásia e Pacífico;
4. Latin American and Caribbean Internet Addresses Registry (LACNIC):[4] América Latina e partes do Caribe;
5. African Network Information Centre (AfriNIC):[5] África.



Footprinting de DNS

- Footprinting de DNS permite obter informações sobre dados de zona DNS. Estes dados de zona de DNS inclui nomes de DNS de domínio, nomes de computadores, endereços IP, Mail Servers e muito mais sobre uma rede particular.
- O atacante executa o footprinting de DNS na rede de destino, a fim de obter informações sobre o DNS. Em seguida, ele utiliza estas informações de DNS do alvo para determinar hosts-chave na rede e, em seguida, executar ataques de engenharia social para reunir mais informações.

8

Footprinting de DNS

Registros de DNS fornecem informações importantes sobre a localização e tipo de servidores.

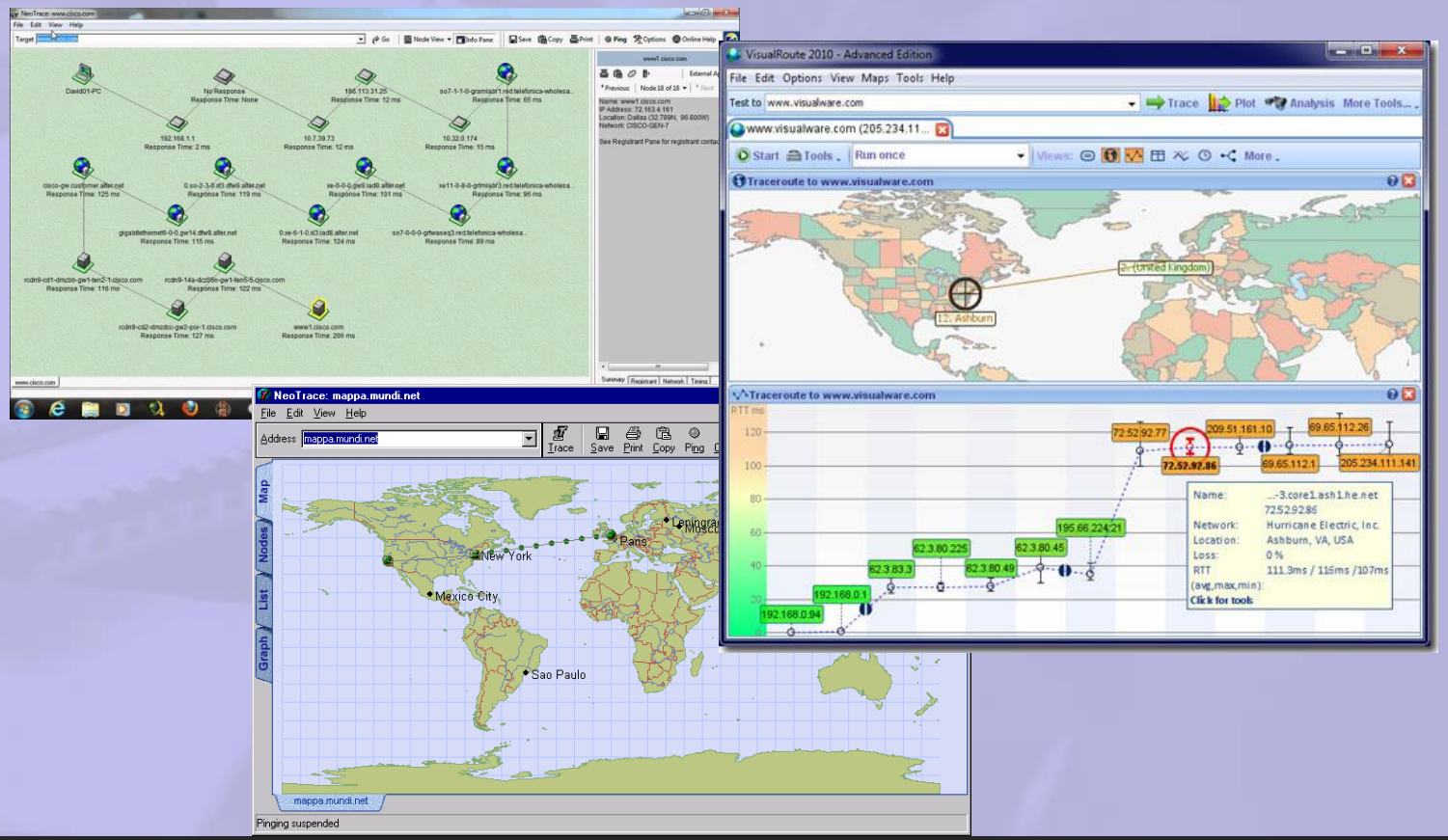
- **A** - Aponta para o endereço IP de um host
- **MX** - Aponta para o servidor de correio do domínio
- **NS** - Aponta para o servidor de nomes do host
- **CNAME** - Nomenclatura canônica permite aliases para um host
- **SOA** - Indica autoridade para domínio
- **SRV** - Registros de serviço
- **PTR** - Mapeia o endereço IP para um nome de host
- **RP** - Responsável
- **HINFO** - Registro de informações do host inclui tipo de CPU e sistema operacional

```
root@packt:~# fierce -dns iitk.ac.in
DNS Servers for iitk.ac.in:
        ns2.iitk.ac.in
        proxy.iitk.ac.in
        ns1.iitk.ac.in

Trying zone transfer first...
        Testing ns2.iitk.ac.in

Whoah, it worked - misconfigured DNS server found:
iitk.ac.in.     43200   IN      SOA     ns1.iitk.ac.in. root.ns1.iitk.ac.in. (
                                        201510271       ;serial
                                        10800           ;refresh
                                        3600            ;retry
                                        1209600         ;expire
                                        43200   )       ;minimum
iitk.ac.in.     43200   IN      MX      10 mail0.iitk.ac.in.
iitk.ac.in.     43200   IN      MX      10 mail1.iitk.ac.in.
iitk.ac.in.     43200   IN      A       202.3.77.184
iitk.ac.in.     43200   IN      NS      ns1.iitk.ac.in.
iitk.ac.in.     43200   IN      NS      ns2.iitk.ac.in.
iitk.ac.in.     43200   IN      NS      proxy.iitk.ac.in.
access.iitk.ac.in.      43200   IN      A       202.3.77.172
agropedia.iitk.ac.in.   43200   IN      A       202.3.77.67
agropedialabs.iitk.ac.in.       43200   IN      A       202.3.77.191
all-iits.iitk.ac.in.    43200   IN      A       202.3.77.160
alumni.iitk.ac.in.      43200   IN      A       202.3.77.176
antaragni.iitk.ac.in.   43200   IN      CNAME   students.iitk.ac.in.
appsgate.iitk.ac.in.    43200   IN      A       202.3.77.165
```

Footprinting de Rede

- Para realizar footprinting de rede, é preciso reunir informações básicas e importantes sobre a organização de destino, como o que a organização faz, para quem eles trabalham, e que tipo de trabalho que executam. As respostas a estas perguntas lhe dar uma ideia sobre a estrutura interna da rede de destino.
- Depois de reunir as informações acima referidas, um atacante pode proceder para encontrar o intervalo de rede de um sistema de destino. Um invasor também pode determinar a máscara de sub-rede do domínio. Ele pode rastrear a rota entre a origem e o destino. Duas ferramentas de traceroute populares são NeoTrace e Visual Route.

O range de rede dá uma ideia sobre a forma como a rede é, quais máquinas na rede estão ativas, e ajuda a identificar a topologia da rede, dispositivo de controle de acesso e sistema operacional utilizado na rede alvo.



Footprinting Através de Engenharia Social

- A engenharia social é um processo totalmente não técnico em que um atacante engana uma pessoa e obtém informações confidenciais sobre o alvo de tal forma que o alvo não tem conhecimento de que alguém está roubando sua informação confidencial.
- O atacante, na verdade, joga um jogo de astúcia com a meta de obter informações confidenciais.

10

Footprinting Através de Engenharia Social

Para realizar engenharia social, você primeiro precisa ganhar a confiança de um usuário autorizado e, em seguida enganá-lo para que revele informações confidenciais. O objetivo básico da engenharia social é a obtenção de informações confidenciais necessárias e, em seguida, usar essa informação no ataque, como obter acesso não autorizado ao sistema, o roubo de identidade, espionagem industrial, de intrusão de rede, cometer fraudes, etc.

A informação obtida por meio de engenharia social pode incluir detalhes de cartão de crédito, números de segurança social, nomes de usuário e senhas, outras informações pessoais, sistemas operacionais e versões de software, endereços IP, nomes de servidores, informações de layout de rede, e muito mais.

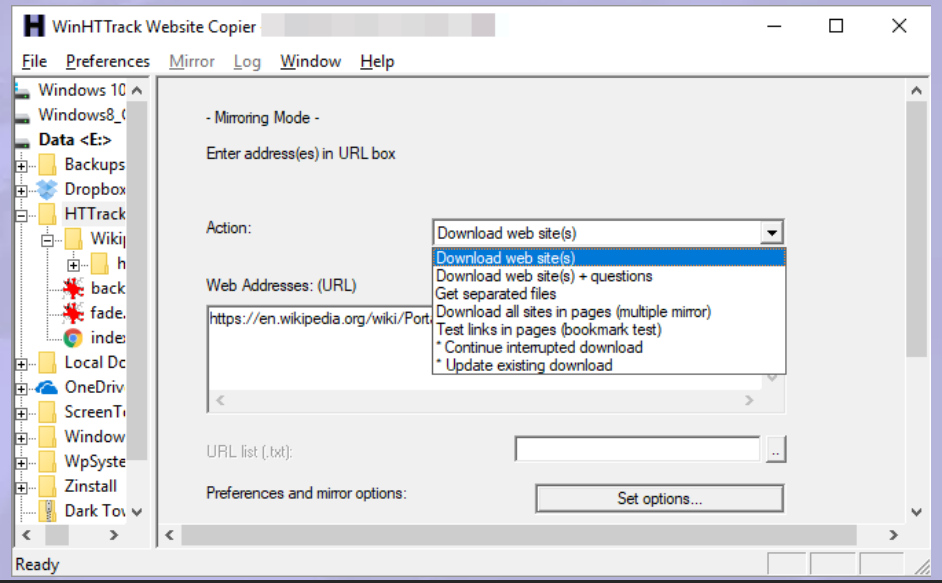
Footprinting Através de clonagem de sites

- Além de fazer toda essa análise online, nós temos a opção da análise offline, onde o atacante faz uma cópia do site alvo para analisá-lo em um segundo momento. Isso pode ser feito com a ajuda de ferramentas de clonagem de sites. Estas ferramentas permitem baixar o site alvo para seu diretório local.

11 **Footprinting Através de clonagem de sites**

Algumas ferramentas de clonagem de sites são:

- TTrack Web Site Copier – http://www.httrack.com
- SurfOffline – http://www.surfoffline.com
- BlackWidow – http://www.softbytelabs.com
- Webripper – http://www.calluna-software.com
- Site Ripper Copier – http://www.tensons.com
- Teleport Pro – http://www.tenmax.com
- PageNest – http://www.pagenest.com
- Backstreet Browser – http://www.spadixbd.com
- Offline Explorer Enterprise – http://www.metaproduts.com
- GNU Wget – http://www.gnu.org



Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.