**Sniffer de rede para interceptação de DHCP**

**Bruno Carvalho e Matheus Santos**

Redes de Computadores II – Pontifícia Universidade Católica do Rio Grande do Sul

* **INTRODUÇÃO**

Em suma, este projeto visa a implementação de um sniffer de rede, de forma que seja possível interceptar pacotes DHCP Discover enviados por máquinas que desejam receber IPs, e então gerar IPs para as mesmas. Para tal, o sniffer deve estar rodando em uma máquina conectada à rede da qual a máquina a ser atacada também esteja conectada. Para executar a simulação, é possível utilizar o comando Linux “dhclient -v” na máquina a ser atacada. Este comando envia um pacote DHCP Discovery para a rede, com o intuito de receber um IP válido para utilizar.

* **COMO FUNCIONA O DHCP**

O DHCP é um protocolo que realiza a alocação de dinâmica/automática dos IPs da rede, visando organização e segurança, pois realizar a configuração de IPs manualmente é custosa e cheio de riscos. O host que deseja conectar-se à rede e, portanto, receber um IP, realiza uma requisição DHCP Discovery para a rede. Esta requisição deve ser capturada pela server responsável por gerar os IPs e então devidamente processada. O server utiliza as informações necessárias recebidas pelo DHCP Discovery e, a partir de alguma política, gerar um endereço IP válido. Este IP é adicionado aos campos do DHCP Offer, do qual é enviado de volta para o host. O host, portanto, solicita um DHCP Request para confirmar a alteração realizada, do qual é recebido pelo server e, ao final, envia um DHCP Ack para finalizar a comunicação entre o host e server. Neste momento, o host possui um IP válido atribuído para si.

* **IMPLEMENTAÇÃO DO SNIFFER**

Para implementá-lo, utilizamos structs já disponíveis nas bibliotecas do Linux, exceto pela de DHCP, da qual tivemos de buscar na Internet. Instanciamos uma variável para cada struct, de forma que seja fácil o manuseio das mesmas ao longo do código.

Ao iniciar o programa, fazemos uma leitura da rede e interfaces da máquina que está rodando o sniffer, descobrindo qual o IP da interface conectada à rede e qual o IP da rede, para serem utilizadas mais tarde nos pacotes IP e DHCP. Então, num loop, o programa recebe pacotes da rede, inserindo os dados recebidos num buffer. A partir daí os passos praticamente são os mesmos: preencher as structs de cada pacote em ordem hierárquica com os valores do buffer. O preenchimento nada mais é do que um cast de tipo em posições definidas do buffer para a struct. Para não realizar operações desnecessárias, as structs são preenchidas uma a uma, e logo após seu preenchimento, são feitas as validações referentes ao próximo protocolo esperado.

Quando se preenche a struct Ethernet, por exemplo, é validado o campo Ethernet type, que deve ser igual ao valor de IPv4 (4). Caso seja verdade, avança-se para o preenchimento da struct IP é validação da mesma. Caso o campo *protocolo* de IP tenha o valor 17 (UDP), preenche-se a struct UDP e a mesma é validada pelo campo de *source address*. Se o campo possuir o valor 67, significa que o próximo protocolo é o DHCP, e, portanto, podemos avançar com as validações. A struct DHCP é preenchida. É importante notar que não consideramos o checksum nem no recebimento nem no envio de UDP.

No DHCP, é necessário verificar o campo *option*, e descobrir que tipo de mensagem é: *Discovery* ou *Request*. Caso seja *Discovery*, monta-se um pacote de DHCP Offer com os dados necessários, estes sendo: a inversão dos campos source e destiny do Ethernet; o preenchimento do campo IP com os dados da máquina sendo atacada, checksum correto e informações sobre o IP da máquina que roda o sniffer; informações DHCP com o IP gerado para a máquina requisitante. Após enviar o pacote Offer, volta-se a aguardar novos pacotes. Neste momento, habilita-se uma flag de “esperando Request”, da qual é utilizada na próxima verificação de pacote recebido. Espera-se que seja recebido o pacote DHCP Request da máquina que enviou o DHCP Discovery anteriormente, mas como apenas voltamos ao loop inicial após o envio do Offer, é possível que seja recebida uma mensagem DHCP Discovery de outra máquina neste meio tempo, portanto, a flag “esperando Request” é responsável por não autorizar o processamento de um novo Discovery.

Ao receber um DHCP Request, é montada a estrutura de resposta novamente da mesma forma que no DHCP Offer. Entretanto, a opção do tipo de mensagem DHCP é alterada para ACK, para que a comunicação entre a máquina atacada e a atacante seja finalizada.