



Assignment 1: Traffic Analysis

Segurança de Sistemas de Informação

João Figueiredo 1230194
João Tiago Araújo 1200584
Diogo Magalhães 1201100

Outubro 2023

Contents

1	Introdução	3
2	Objetivos	3
3	Análises das Capturas	3
3.1	Captura 1: Análise LDAP e Comunicações Adicionais	3
3.2	Captura 2: Recuperação de Email POP3	5
3.3	Captura 3: Transferência de Ficheiros FTP	7
3.4	Captura 4: Microsoft Telnet Service	10
3.5	Captura 5: Autenticação RADIUS	12
3.6	Captura 6: SQL Slammer	14
4	Conclusões	15
5	Referências	16

1 Introdução

A análise de tráfego é uma ferramenta fundamental para várias tarefas de gestão de rede e tem diversas aplicações relacionadas com a segurança informática, como a identificação de protocolos inseguros, recolha de informações de diversos tipos ou realização de reconhecimento de rede.

2 Objetivos

Os objetivos específicos deste trabalho são:

- **Identificação de Vulnerabilidades:** Ao observar os padrões e conteúdos dos pacotes, procuraremos por sinais de vulnerabilidades conhecidas ou de configurações inseguras que possam ser exploradas por atacantes.
- **Deteção de Anomalias e Potenciais Ameaças:** Além de vulnerabilidades, focaremos na identificação de comportamentos suspeitos que possam indicar tentativas de intrusão, falhas no sistema ou mau uso da rede.
- **Recomendações de Melhoria:** Com base nas descobertas, forneceremos recomendações para melhorar a postura de segurança da rede, seja através de configurações mais seguras, implementação de protocolos adicionais de segurança ou outras estratégias pertinentes.

Por fim, é importante dar ênfase que, enquanto o objetivo principal é identificar ataques ou vulnerabilidades, este trabalho também atribuirá a importância da prevenção. Afinal, em muitos casos, pode não haver um ataque em andamento, mas os problemas de segurança identificados podem representar portos abertos para futuras ameaças. Assim, ao destacar estas questões e propor soluções, este trabalho busca não apenas responder a incidentes, mas principalmente evitá-los.

3 Análises das Capturas

3.1 Captura 1: Análise LDAP e Comunicações Adicionais

- **Intervenientes:**
 - IP de Origem: 192.168.170.132 (MAC Address: 00:0c:29:15:14:76)
 - IP de Destino: 192.168.170.130 (e outros como 192.168.170.2, 239.255.255.250)
- **Protocolo Principal:** LDAP[6] e NBNS[12].
- **Operações Realizadas:**

- A máquina 192.168.170.132 fez consultas LDAP ao 192.168.170.130, abrangendo grupos como "RAS and IAS Servers", "Read-only Domain Controllers", e "Schema Admins".
- Observadas comunicações NBNS, com destaque para o nome "DESKTOP-IB1IL54".
- Comunicações SSDP[4] dirigidas a 239.255.255.250.

235	4.187528	192.168.170.130	192.168.170.132	LDAP	170	searchRequest(8) "CN=Aggregate,CN=Schema,CN=Configuration,DC=segsi_domain,DC=local" baseObject
236	4.188062	192.168.170.132	192.168.170.130	LDAP	204	searchResEntry(8) "CN=Aggregate,CN=Schema,CN=Configuration,DC=segsi_domain,DC=local" searchResDone(8) success [53 results]
237	4.188432	192.168.170.130	192.168.170.132	LDAP	147	searchRequest(9) "CN=Configuration,DC=segsi_domain,DC=local" baseObject
238	4.188923	192.168.170.132	192.168.170.130	LDAP	185	searchResEntry(9) "CN=Configuration,DC=segsi_domain,DC=local" searchResDone(9) success [53 results]
239	4.191584	192.168.170.130	192.168.170.132	LDAP	130	searchRequest(10) "DC=segsi_domain,DC=local" baseObject
240	4.191966	192.168.170.132	192.168.170.130	LDAP	172	searchResEntry(10) "DC=segsi_domain,DC=local" searchResDone(10) success [53 results]
241	4.195372	192.168.170.130	192.168.170.132	LDAP	148	searchRequest(11) "DC=domainDnsZones,DC=segsi_domain,DC=local" baseObject
242	4.195885	192.168.170.132	192.168.170.130	LDAP	190	searchResEntry(11) "DC=domainDnsZones,DC=segsi_domain,DC=local" searchResDone(11) success [53 results]
243	4.196721	192.168.170.130	192.168.170.132	LDAP	215	searchRequest(12) "CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local."
244	4.199181	192.168.170.132	192.168.170.130	LDAP	244	searchResEntry(12) "CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local."
245	4.200444	192.168.170.130	192.168.170.132	LDAP	232	searchRequest(13) "CN=NTDS Settings,CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local"
246	4.205452	192.168.170.132	192.168.170.130	LDAP	283	searchResEntry(13) "CN=NTDS Settings,CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local" searchResDone(13) success [53 results]
267	61.761590	192.168.170.130	192.168.170.132	LDAP	120	searchRequest(14) "DC=segsi_domain,DC=local" baseObject
269	61.791387	192.168.170.130	192.168.170.132	LDAP	131	searchRequest(15) "DC=segsi_domain,DC=local" singlelevel
271	61.791958	192.168.170.132	192.168.170.130	LDAP	945	searchResEntry(14) "DC=segsi_domain,DC=local" searchResDone(14) success [53 results]
273	61.792615	192.168.170.132	192.168.170.130	LDAP	1514	searchResEntry(15) "CN=Builtin,DC=segsi_domain,DC=local" searchResEntry(15) "CN=Computers,DC=segsi_domain,DC=local" searchResDone(15) success [53 results]
274	61.792655	192.168.170.132	192.168.170.130	LDAP	176	searchRequest(16) "CN=Users,DC=segsi_domain,DC=local" baseObject
278	80.243780	192.168.170.130	192.168.170.132	LDAP	129	searchRequest(16) "CN=Users,DC=segsi_domain,DC=local" baseObject
279	80.246624	192.168.170.132	192.168.170.130	LDAP	867	searchResEntry(16) "CN=Users,DC=segsi_domain,DC=local" searchResDone(16) success [53 results]
282	80.340321	192.168.170.130	192.168.170.132	LDAP	140	searchRequest(17) "CN=Users,DC=segsi_domain,DC=local" singlelevel
283	80.341805	192.168.170.132	192.168.170.130	LDAP	1514	searchResEntry(17) "CN=Administrator,CN=Users,DC=segsi_domain,DC=local" searchResEntry(17) "CN=Alice Wonderland,CN=Users,DC=segsi_domain,DC=local" searchResDone(17) success [53 results]
285	80.390919	192.168.170.132	192.168.170.130	LDAP	1514	searchResEntry(17) "CN=Domain Controllers,CN=Users,DC=segsi_domain,DC=local" searchResEntry(17) "CN=Domain Guests,CN=Users,DC=segsi_domain,DC=local" searchResDone(17) success [53 results]
286	80.390919	192.168.170.132	192.168.170.130	LDAP	321	searchResEntry(17) "CN=RAS and IAS Servers,CN=Users,DC=segsi_domain,DC=local" searchResEntry(17) "CN=Read-only Domain Controllers,CN=Users,DC=segsi_domain,DC=local" searchResDone(17) success [53 results]

Figure 1: *Captura1(1/2)*

235	4.187528	192.168.170.130	192.168.170.132	LDAP	170	searchRequest(8) "CN=Aggregate,CN=Schema,CN=Configuration,DC=segsi_domain,DC=local" baseObject
236	4.188062	192.168.170.132	192.168.170.130	LDAP	204	searchResEntry(8) "CN=Aggregate,CN=Schema,CN=Configuration,DC=segsi_domain,DC=local" searchResDone(8) success [53 results]
237	4.188432	192.168.170.130	192.168.170.132	LDAP	147	searchRequest(9) "CN=Configuration,DC=segsi_domain,DC=local" baseObject
238	4.188923	192.168.170.132	192.168.170.130	LDAP	185	searchResEntry(9) "CN=Configuration,DC=segsi_domain,DC=local" searchResDone(9) success [53 results]
239	4.191584	192.168.170.130	192.168.170.132	LDAP	130	searchRequest(10) "DC=segsi_domain,DC=local" baseObject
240	4.191966	192.168.170.132	192.168.170.130	LDAP	172	searchResEntry(10) "DC=segsi_domain,DC=local" searchResDone(10) success [53 results]
241	4.195372	192.168.170.130	192.168.170.132	LDAP	148	searchRequest(11) "DC=domainDnsZones,DC=segsi_domain,DC=local" baseObject
242	4.195885	192.168.170.132	192.168.170.130	LDAP	190	searchResEntry(11) "DC=domainDnsZones,DC=segsi_domain,DC=local" searchResDone(11) success [53 results]
243	4.196721	192.168.170.130	192.168.170.132	LDAP	215	searchRequest(12) "CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local."
244	4.199181	192.168.170.132	192.168.170.130	LDAP	244	searchResEntry(12) "CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local."
245	4.200444	192.168.170.130	192.168.170.132	LDAP	232	searchRequest(13) "CN=NTDS Settings,CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local"
246	4.205452	192.168.170.132	192.168.170.130	LDAP	283	searchResEntry(13) "CN=NTDS Settings,CN=WIN-6LNRHRRBQND,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=segsi_domain,DC=local" searchResDone(13) success [53 results]
267	61.761590	192.168.170.130	192.168.170.132	LDAP	120	searchRequest(14) "DC=segsi_domain,DC=local" baseObject
269	61.791387	192.168.170.130	192.168.170.132	LDAP	131	searchRequest(15) "DC=segsi_domain,DC=local" singlelevel
271	61.791958	192.168.170.132	192.168.170.130	LDAP	945	searchResEntry(14) "DC=segsi_domain,DC=local" searchResDone(14) success [53 results]
273	61.792615	192.168.170.132	192.168.170.130	LDAP	1514	searchResEntry(15) "CN=Builtin,DC=segsi_domain,DC=local" searchResEntry(15) "CN=Computers,DC=segsi_domain,DC=local" searchResDone(15) success [53 results]
274	61.792655	192.168.170.132	192.168.170.130	LDAP	176	searchRequest(16) "CN=Users,DC=segsi_domain,DC=local" baseObject
278	80.243780	192.168.170.130	192.168.170.132	LDAP	129	searchRequest(16) "CN=Users,DC=segsi_domain,DC=local" baseObject
279	80.246624	192.168.170.132	192.168.170.130	LDAP	867	searchResEntry(16) "CN=Users,DC=segsi_domain,DC=local" searchResDone(16) success [53 results]
282	80.340321	192.168.170.130	192.168.170.132	LDAP	140	searchRequest(17) "CN=Users,DC=segsi_domain,DC=local" singlelevel
283	80.341805	192.168.170.132	192.168.170.130	LDAP	1514	searchResEntry(17) "CN=Administrator,CN=Users,DC=segsi_domain,DC=local" searchResEntry(17) "CN=Alice Wonderland,CN=Users,DC=segsi_domain,DC=local" searchResDone(17) success [53 results]
285	80.390919	192.168.170.132	192.168.170.130	LDAP	1514	searchResEntry(17) "CN=Domain Controllers,CN=Users,DC=segsi_domain,DC=local" searchResEntry(17) "CN=Domain Guests,CN=Users,DC=segsi_domain,DC=local" searchResDone(17) success [53 results]
286	80.390919	192.168.170.132	192.168.170.130	LDAP	321	searchResEntry(17) "CN=RAS and IAS Servers,CN=Users,DC=segsi_domain,DC=local" searchResEntry(17) "CN=Read-only Domain Controllers,CN=Users,DC=segsi_domain,DC=local" searchResDone(17) success [53 results]

Figure 2: *Captura1(2/2)*

• Problemas de Segurança:

- *Exposição de Informações:* O cliente LDAP autentica-se e realiza várias pesquisas (com filtros diferentes). O servidor responde e fornece a informação respetiva a essa pesquisa. Isto por si não apresenta um ataque direto. Mas o facto, de o canal não ser encriptado ou a própria informação, significa que qualquer atacante que intercete e "apanhe" estes pacotes terá acesso a todos os dados partilhados.
- *Uso de Protocolos Vulneráveis:* Utilizar LDAPS em vez de LDAP. Assim as comunicações são feitas no mesmo protocolo, mas com mecanismos de encriptação implementados.
- *Broadcasts NBNS:* Estes podem expor nomes de máquinas e outros detalhes.
- *Comunicações SSDP:* Indica busca por dispositivos/serviços na rede, podendo ser mal-intencionadas.

- **Recomendações:**
 - Investigar o propósito das frequentes consultas LDAP pelo IP 192.168.170.132.
 - Migrar para LDAPS, garantindo a encriptação do tráfego.
 - Estabelecer controlos mais rigorosos para tráfego NBNS e SSDP, utilizando ferramentas de deteção e prevenção.
- **Detalhes Adicionais:**
 - **Timestamp:**
 - * **Descrição:** Indica o início e o fim do período de captura dos pacotes.
 - * **Utilidade:** O timestamp ajuda a:
 - Correlacionar a atividade de rede com outros eventos no sistema ou na infraestrutura.
 - Identificar padrões temporais, como atividades suspeitas ocorrendo fora do horário de trabalho.
 - Comparar capturas de pacotes em diferentes períodos para analisar tendências ou mudanças no tráfego.
 - **Quantidade:**
 - * **Descrição:** Número total de pacotes capturados durante o período especificado.
 - * **Utilidade:** Saber a quantidade de pacotes ajuda a:
 - Estimar a carga de tráfego durante o período de captura.
 - Comparar com outros períodos para identificar aumentos ou diminuições inesperadas no tráfego.
 - Avaliar a necessidade de recursos de análise ou hardware mais robusto para lidar com grandes volumes de tráfego.
 - **Anomalias:**
 - * **Descrição:** Refere-se a padrões inesperados, picos de tráfego, ou pacotes mal-formados que possam ser identificados.
 - * **Utilidade:** A identificação de anomalias é crucial para:
 - Detetar potenciais ameaças ou atividades mal-intencionadas.
 - Identificar configurações incorretas ou falhas de equipamento.
 - Monitorizar a saúde e o desempenho da rede, sinalizando quando algo não está a trabalhar como esperado.
 - Facilitar investigações de incidentes de segurança, fornecendo pistas sobre a natureza e origem de um ataque.

3.2 Captura 2: Recuperação de Email POP3

- **Intervenientes:** Os principais intervenientes são o cliente com o endereço IP 192.168.2.100 e MAC Address 00:e0:4c:16:c8:94 e o servidor com o endereço IP 64.246.26.20 e MAC Address 00:e0:4e:10:f9:4c.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.100	64.246.26.20	TCP	60	1140 → 1140 [SYN] Seq=0 Min=5535 Len=0 MSS=1460 SACK_PERM
2	0.464000	64.246.26.20	192.168.2.100	TCP	62	1140 → 1140 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1452 SACK_PERM
3	0.464000	192.168.2.100	64.246.26.20	TCP	60	1140 → 1140 [ACK] Seq=1 Ack=1 Win=5535 Len=0
4	0.934000	64.246.26.20	192.168.2.100	POP	180	5: +OK POP3 mail.colasoft.com v2001.70rh server ready
5	0.937000	192.168.2.100	64.246.26.20	POP	79	C: USER test2@colasoft.com
6	1.395000	64.246.26.20	192.168.2.100	TCP	60	1140 → 1140 [ACK] Seq=53 Ack=26 Win=5840 Len=0
7	1.397000	64.246.26.20	192.168.2.100	POP	95	5: +OK User name accepted, password please
8	1.401000	192.168.2.100	64.246.26.20	POP	69	C: PASS test2123
9	1.920000	64.246.26.20	192.168.2.100	TCP	60	1140 → 1140 [ACK] Seq=94 Ack=41 Win=5840 Len=0
10	1.961000	64.246.26.20	192.168.2.100	POP	84	5: +OK Mailbox open, 1 messages
11	1.961000	192.168.2.100	64.246.26.20	POP	60	C: STAT
12	2.465000	64.246.26.20	192.168.2.100	TCP	60	1140 → 1140 [ACK] Seq=124 Ack=47 Win=5840 Len=0
13	2.465000	64.246.26.20	192.168.2.100	POP	65	5: +OK 1 904
14	2.466000	192.168.2.100	64.246.26.20	POP	60	C: UIDL
15	2.920000	64.246.26.20	192.168.2.100	POP	180	5: +OK Unique-ID listing follows
16	2.920000	192.168.2.100	64.246.26.20	POP	60	C: LIST
17	3.497000	64.246.26.20	192.168.2.100	POP	98	5: +OK Mailbox scan listing follows
18	3.499000	192.168.2.100	64.246.26.20	POP	62	C: RETR 1
19	3.959000	64.246.26.20	192.168.2.100	POP	1007	5: +OK 904 octets
20	3.967000	192.168.2.100	64.246.26.20	POP	62	C: DELE 1
21	4.422000	64.246.26.20	192.168.2.100	POP	75	5: +OK Message deleted
22	4.424000	192.168.2.100	64.246.26.20	POP	60	C: QUIT
23	4.889000	64.246.26.20	192.168.2.100	POP	68	5: +OK Sayonara
24	4.889000	192.168.2.100	64.246.26.20	TCP	60	1140 → 1140 [FIN, ACK] Seq=81 Ack=1271 Win=64205 Len=0
25	4.889000	64.246.26.20	192.168.2.100	TCP	60	1140 → 1140 [FIN, ACK] Seq=1271 Ack=81 Win=5840 Len=0
26	4.889000	192.168.2.100	64.246.26.20	TCP	60	1140 → 1140 [ACK] Seq=82 Ack=1272 Win=64205 Len=0
27	5.347000	64.246.26.20	192.168.2.100	TCP	60	1140 → 1140 [ACK] Seq=1272 Ack=82 Win=5840 Len=0

Figure 3: *Captura2*

- **Protocolo Principal:** O protocolo em destaque é o Post Office Protocol version 3 (POP3) [7].
 - **Função Primária:** O POP3 é utilizado para descarregar mensagens de email de um servidor para um dispositivo local, seja este um computador, tablet ou smartphone. Ao contrário de outros protocolos, o POP3, por padrão, descarrega as mensagens e remove-as do servidor, ficando estas armazenadas no dispositivo do utilizador.
 - **Vantagens:** Ideal para utilizadores que desejam ler seus emails sem a necessidade de uma conexão constante com a internet, já que as mensagens são armazenadas localmente. Esta característica também oferece uma certa economia de espaço no servidor de email.
 - **Limitações:** Como o POP3 descarrega emails e remove-os do servidor (a menos que seja configurado de outra forma), pode ser desafiador gerir emails em vários dispositivos. Por exemplo, um email descarregado num computador pode não estar disponível num smartphone se ambos os dispositivos estiverem configurados para usar o POP3.
 - **Uso Atual:** Embora o POP3 ainda seja amplamente suportado e usado, muitos preferem protocolos mais modernos como o IMAP devido à sua flexibilidade e capacidade de sincronização entre dispositivos.
- **Operações Realizadas:**
 - O cliente inicia uma conexão com o servidor utilizando o standard TCP three-way handshake.
 - O servidor responde com uma saudação indicando a sua prontidão para iniciar uma sessão POP3.
 - O cliente envia o seu nome de utilizador ('test2@colasoft.com') ao servidor para autenticação.
 - O servidor reconhece o nome de utilizador e solicita a senha.

- O cliente envia a sua senha ('test2123') ao servidor.
- O cliente realiza várias operações POP3, como verificar correio, recuperar correio e eliminar correio.
- Finalmente, o cliente emite um comando QUIT para terminar a sessão.

- **Problemas de Segurança:**

- ***Credenciais em texto simples:*** O nome de utilizador e a senha são enviados em texto simples, o que os torna vulneráveis a escutas.
 - * Nome de Utilizador: test2@colasoft.com
 - * Password: test2123
- ***Falta de Encriptação:*** Toda a sessão não está encriptada, expondo todos os dados transmitidos à possível intercepção.
- ***Potencial para ataques de replay:*** A autenticação em texto claro pode ser repetida por atacantes para ganhar acesso não autorizado.
- ***Divulgação de informações do servidor:*** O servidor revela o seu tipo e versão, o que pode auxiliar os atacantes em ataques direcionados.

Recomendações para mitigação:

- Usar o POP encriptado (POP3S).
 - Implementar mecanismos de autenticação seguros que não exponham senhas em texto simples.
 - Minimizar a divulgação de informações do servidor. Assim, um atacante, não conhece detalhes do mesmo.
 - Monitorizar a rede, de forma regular, para detetar atividades suspeitas.
- **Observações Adicionais:** É essencial que qualquer organização ou indivíduo que use o POP3 esteja ciente das suas vulnerabilidades, especialmente quando não está encriptado. A transição para a recuperação de emails encriptados e mecanismos de autenticação seguros é altamente recomendada para manter a confidencialidade e integridade das comunicações.

3.3 Captura 3: Transferência de Ficheiros FTP

- **Intervenientes:** Os principais intervenientes são o cliente com o endereço IP 192.168.2.101 com o MAC Address 00:e0:4d:c0:01:8e e o servidor como endereço IP 192.186.2.100 e MAC Address 00:e0:4c:16:c8:94

- **Protocolo Principal:** O protocolo usado principalmente é o FTP(File Transfer Protocol), que é um protocolo de rede padrão usado para transferir ficheiros de um computador para outro através de uma rede baseada em TCP/IP. Também é utilizado o protocolo TCP(Transmission Control Protocol) que permite uma comunicação confiável e orientada para a conexão entre dois dispositivos numa rede. O TCP é responsável por dividir dados em pacotes, transmiti-los e montá-los novamente noutro lado de forma a garantir a entrega confiável e ordenada de dados.

- **Operações Realizadas:**

- *Quem inicia:* A origem 192.168.2.101 envia um 'Access-Request' de forma a autenticar o utilizador "administrador"
- *Quem responde:* O destino 192.168.2.100
- *Características da ligação:* O cliente (192.168.2.101) começa a por se conectar com o servidor(192.168.2.100) e de seguida realiza um pedido para iniciar a sessão como "administrador", é-lhe pedida a palavra-passe, onde é retribuída a Pass "123456" e fica logado com sucesso.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.101	192.168.2.100	TCP	62	2502 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
2	0.000000	192.168.2.100	192.168.2.101	TCP	62	21 → 2502 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM
3	0.000000	192.168.2.101	192.168.2.100	TCP	60	2502 → 21 [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.001000	192.168.2.100	192.168.2.101	FTP	112	Response: 220 colasoft_test_2 Microsoft FTP Service (Version 5.0).
5	0.150000	192.168.2.101	192.168.2.100	TCP	60	2502 → 21 [ACK] Seq=1 Ack=59 Win=17462 Len=0
6	3.956000	192.168.2.101	192.168.2.100	FTP	74	Request: USER administrator
7	3.997000	192.168.2.100	192.168.2.101	FTP	96	Response: 331 Password required for administrator.
8	4.163000	192.168.2.101	192.168.2.100	TCP	60	2502 → 21 [ACK] Seq=21 Ack=101 Win=17428 Len=0
9	6.100000	192.168.2.101	192.168.2.100	FTP	67	Request: PASS 123456
10	6.111000	192.168.2.100	192.168.2.101	FTP	97	Response: 230-Welcome to colasoft_test site,thanks!
11	6.266000	192.168.2.101	192.168.2.100	TCP	60	2502 → 21 [ACK] Seq=34 Ack=144 Win=17377 Len=0
12	6.266000	192.168.2.100	192.168.2.101	FTP	89	Response: 230 User administrator logged in.

Figure 4: Captura3 Login

De seguida é efetuado um pedido "Request: PORT 192,168,2,101,9,200", este é usado para informar o servidor FTP sobre a conexão de dados que o cliente deseja estabelecer, é necessário especificar o endereço IP e o número da porta, sendo estes o IP "192.168.2.101," e o número da porta é calculado como "9 * 256 + 200," que resulta na porta 2504. Depois, é pedido um "Request: NLST" que é um comando para solicitar uma lista de ficheiros no diretório atual no servidor FTP. É-lhe retribuído os ficheiros e procede à transferência, o servidor confirma que a transferência do ficheiro foi concluída com sucesso. É solicitado uma listagem dos ficheiros e diretórios no diretório atual no

16	7.784000	192.168.2.101	192.168.2.100	FTP	60	Request: NLST
17	7.784000	192.168.2.100	192.168.2.101	FTP	109	Response: 150 Opening ASCII mode data connection for file list.
18	7.784000	192.168.2.100	192.168.2.101	TCP	62	20 → 2504 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
19	7.784000	192.168.2.101	192.168.2.100	TCP	62	2504 → 20 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PERM
20	7.784000	192.168.2.100	192.168.2.101	TCP	54	20 → 2504 [ACK] Seq=1 Ack=1 Win=65535 Len=0
21	7.786000	192.168.2.100	192.168.2.101	FTP-DATA	132	FTP data: 78 bytes (PORT) (NLST)
22	7.792000	192.168.2.100	192.168.2.101	TCP	54	20 → 2504 [FIN, ACK] Seq=79 Ack=1 Win=65535 Len=0
23	7.799000	192.168.2.101	192.168.2.100	TCP	60	2504 → 20 [ACK] Seq=1 Ack=80 Win=17442 Len=0
24	7.803000	192.168.2.101	192.168.2.100	TCP	60	2504 → 20 [FIN, ACK] Seq=1 Ack=80 Win=17442 Len=0
25	7.803000	192.168.2.100	192.168.2.101	TCP	54	20 → 2504 [ACK] Seq=80 Ack=2 Win=65535 Len=0
26	7.969000	192.168.2.101	192.168.2.100	TCP	60	2502 → 21 [ACK] Seq=66 Ack=264 Win=17257 Len=0
27	7.969000	192.168.2.100	192.168.2.101	FTP	78	Response: 226 Transfer complete.

Figure 5: Captura3 NLST

itada uma listagem dos ficheiros e diretórios no diretório atual no

servidor FTP e depois é solicitada a recuperação ou download de um ficheiro do servidor, neste caso o "logagent.exe". Após isso, realiza-se o download até que a janela TCP para a comunicação esteja completa. Quando fica completa, a transmissão dos dados é interrompida até que os reconhecimentos sejam recebidos. Isto pode sugerir um problema de congestionamento ou de rede onde não é possível receber mais dados até que a janela seja libertada. Assim que é libertada, a transferência é concluída. E inicia-se a transferência de mais ficheiros, como o "mplayr2.exe".

31	9.451000	192.168.2.101	192.168.2.100	FTP	68	Request: LIST
32	9.451000	192.168.2.100	192.168.2.101	FTP	107	Response: 150 Opening ASCII mode data connection for /bin/ls.
33	9.451000	192.168.2.100	192.168.2.101	TCP	62	20 → 2585 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
34	9.452000	192.168.2.101	192.168.2.100	TCP	62	2585 → 20 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PERM
35	9.452000	192.168.2.100	192.168.2.101	TCP	54	20 → 2585 [ACK] Seq=1 Ack=1 Win=65535 Len=0
36	9.452000	192.168.2.100	192.168.2.101	FTP-DATA	366	FTP Data: 312 bytes (PORT) (LIST)
37	9.452000	192.168.2.100	192.168.2.101	TCP	54	20 → 2585 [FIN, ACK] Seq=313 Ack=1 Win=65535 Len=0
38	9.453000	192.168.2.101	192.168.2.100	TCP	68	2585 → 20 [ACK] Seq=1 Ack=314 Win=17280 Len=0
39	9.470000	192.168.2.101	192.168.2.100	TCP	68	2585 → 20 [FIN, ACK] Seq=1 Ack=314 Win=17280 Len=0
40	9.470000	192.168.2.100	192.168.2.101	TCP	54	20 → 2585 [ACK] Seq=314 Ack=2 Win=65535 Len=0
41	9.571000	192.168.2.101	192.168.2.100	TCP	68	2582 → 21 [ACK] Seq=98 Ack=371 Win=17150 Len=0
42	9.571000	192.168.2.100	192.168.2.101	FTP	78	Response: 226 Transfer complete.
43	9.771000	192.168.2.101	192.168.2.100	TCP	68	2582 → 21 [ACK] Seq=98 Ack=395 Win=17126 Len=0
44	17.120000	192.168.2.101	192.168.2.100	FTP	88	Request: PORT 192,168,2,101,9,282
45	17.120000	192.168.2.100	192.168.2.101	FTP	84	Response: 200 PORT command successful.
46	17.124000	192.168.2.101	192.168.2.100	FTP	73	Request: RETR logagent.exe

Figure 6: Captura3 LIST

91	17.150000	192.168.2.100	192.168.2.101	FTP-DATA	1514	[TCP Window Full] FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
92	17.150000	192.168.2.101	192.168.2.100	TCP	68	2586 → 20 [ACK] Seq=1 Ack=38661 Win=17520 Len=0
93	17.150000	192.168.2.100	192.168.2.101	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
94	17.150000	192.168.2.100	192.168.2.101	FTP-DATA	1514	[TCP Window Full] FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
95	17.150000	192.168.2.101	192.168.2.100	TCP	68	2586 → 20 [ACK] Seq=1 Ack=33581 Win=17520 Len=0
96	17.151000	192.168.2.100	192.168.2.101	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
97	17.151000	192.168.2.100	192.168.2.101	FTP-DATA	1514	[TCP Window Full] FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
98	17.151000	192.168.2.101	192.168.2.100	TCP	68	2586 → 20 [ACK] Seq=1 Ack=36581 Win=17520 Len=0
99	17.151000	192.168.2.100	192.168.2.101	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
100	17.151000	192.168.2.101	192.168.2.100	FTP-DATA	1514	[TCP Window Full] FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
101	17.151000	192.168.2.101	192.168.2.100	TCP	68	2586 → 20 [ACK] Seq=1 Ack=39421 Win=17520 Len=0
102	17.151000	192.168.2.100	192.168.2.101	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
103	17.151000	192.168.2.100	192.168.2.101	FTP-DATA	1514	[TCP Window Full] FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
104	17.151000	192.168.2.101	192.168.2.100	TCP	68	2586 → 20 [ACK] Seq=1 Ack=42341 Win=17520 Len=0
105	17.151000	192.168.2.100	192.168.2.101	FTP-DATA	1514	FTP Data: 1460 bytes (PORT) (RETR logagent.exe)
106	17.151000	192.168.2.100	192.168.2.101	FTP-DATA	1514	[TCP Window Full] FTP Data: 1460 bytes (PORT) (RETR logagent.exe)

Figure 7: Captura3 WindowFull

Após isso, o cliente envia um pedido FTP ao endereço IP de destino com o comando "XPWD" para questionar qual é o diretório de trabalho actual. Recebe como resposta "/", o que significa que o diretório em questão é o diretório raiz ("/"), indicando uma mudança de diretório realizada com sucesso.

142	42.219000	192.168.2.101	192.168.2.100	TCP	68	2582 → 21 [ACK] Seq=188 Ack=644 Win=16877 Len=0
143	48.684000	192.168.2.101	192.168.2.100	FTP	68	Request: XPWD
144	48.685000	192.168.2.100	192.168.2.101	FTP	85	Response: 257 "/" is current directory.
145	48.828000	192.168.2.101	192.168.2.100	TCP	68	2582 → 21 [ACK] Seq=194 Ack=675 Win=16846 Len=0

Figure 8: Captura3 XPWD

Ao longo da captura o FTP comunica através de duas conexões TCP. A porta 21 é para o controlo de tráfego e a porta 20 é para a transmissão de dados.[1]

- **Dados:** É possível obter o tamanho e nome dos ficheiros listados/descarregados. É possível saber os dados de login do cliente.

- **Problemas de Segurança e como mitigar:**

- *FTP em texto simples*: Em vez de ser usado FTP, poderia ser utilizada uma alternativa mais segura, como FTPS(FTP Secure) ou o SFTP (SSH File Transfer Protocol) que fornece criptografia e autenticação para proteger os dados durante a transmissão, que é o caso do nome do utilizador e palavra passe.
- *Comando PORT*: Com a utilização do comando "PORT" pode ser exposto o endereço IP interno do cliente ao servidor. Esta informação poderá ser utilizada para atingir a rede interna do cliente.
- *Número do PORT*: O número é incrementado 1 a 1, o atacante ao saber um número do PORT, conseguirá aceder às restantes PORT's mais facilmente.
- *Listagem dos diretórios*: A utilização dos comandos "LIST" e "NLST" podem revelar o diretório atual e informações de ficheiros para utilizadores não autorizados no servidor. É necessário configurar corretamente os servidores FTP de forma a restringir a listagem de diretórios apenas para utilizadores autorizados.
- *FTP em modo ativo*: pode introduzir várias preocupações de segurança, porque requer que o cliente abra um PORT para se conectar ao servidor. Como o servidor sempre que inicia a conexão de dados a partir de sua porta 20 em modo ativo, é mais previsível para configurações de firewall, para isso, os administradores devem definir regras de firewall que permitem o tráfego apenas da porta 20.
- **Observações Adicionais:**
 - *Segurança de senha*: A captura mostra a senha "123456" que foi utilizada para autenticação do cliente, esta é uma senha fraca deve-se impor políticas de senha fortes para melhorar a segurança, como por exemplo usar senhas fortes e únicas.
 - *Integridade de dados*: A captura não indica informações sobre verificações de integridade de dados, por isso deve-se garantir a integridade dos dados durante a transferência, é crucial detetar modificações não permitidas ou corrupção de dados durante a comunicação.
 - *Deteção de intrusão*: Pode ser necessário implementar sistemas de deteção de intrusão para gerir atividade de rede incomum ou potencialmente maliciosa.

3.4 Captura 4: Microsoft Telnet Service

- **Intervenientes**: Os principais intervenientes são o utilizador com o IP 192.268.251.1 e MAC Address 00:0c:29:2c:d8:db e o servidor o IP 192.268.251.11 e MAC Address 00:0c:29:da:82:be, ambos estão a comunicar através de uma Virtual Machine(VM).
- **Protocolo Principal**: Os protocolos mais utilizados são o Teletype Network(TELNET)[11] e o TCP.

- *Quem inicia*: O utilizador com o IP 192.168.251.1 e endereço MAC VMware2c : d8 : dbtentaestabelecerumaconexãootravezdeumTCPthree-wayhandshake.*Quem responde* : OservidorcomoIP192.168.251.11eendereçoMACVMware4a : 82 : bedáacknowledgeeestabelececonexãocomoutilizador.

- * O protocolo TCP tem como origem o porto 36099 e destino o porto 23.
- * É realizada uma tentativa de comunicação com o porto 137 utilizando o protocolo NetBIOS Name Service(NBNS)[12], mas este encontra-se inacessível.

Figure 9: *Captura4NBNS*

- * O utilizador tenta fazer login no Microsoft Telnet Service, resultando num erro de login com username ou password incorretas(linhas 19-69).
- * O utilizador realiza outro login, mas desta vez é sucedido(linhas 70-124).
- * O utilizador navega até a pasta "secrets" e dá type ao ficheiro "pin.txt"(linhas 125-225).
- * O utilizador termina a navegação(linhas 226-242).

- * É possível retirar os dados de login no Microsoft Telnet Server
username: esegi-boss e password:segred0.
- * É possível retirar do ficheiro "pin.txt" o código 89384.

- *Texto Simples*: Os dados inseridos encontram-se no formato texto simples por causa do protocolo Telnet, desta forma este dados podem ser facilmente intercetados e lidos por qualquer pessoa com acesso à rede.

- *Servidor DHCP*
 - * *DHCP Flood*: O atacante envia vários pedidos para o servidor, limitando assim o número de IPs disponíveis.
 - * *DHCP Spoofing*: O atacante consegue ver e responder aos pedidos dos utilizadores do servidor DHCP.
- *Mitigação*:
 - * *Secure Shell(SSH)* para encriptar os dados transmitidos e ter mecanismos de autenticação para proteger os dados.
 - * *Limitação de Rate* para limitar um número de pedidos dentro de um intervalo de tempo, assim vai prevenir o tráfego excessivo de sobrecarregar o servidor DHCP.
 - * *Autenticação do servidor DHCP* para identificar que os servidores que estão a ser utilizados são legítimos.
- **Observações Adicionais**: Os utilizadores do Telnet devem ter em consideração que este protocolo contem vários riscos de segurança, pois os dados que são transmitidos encontram-se em texto simples e não estão encriptados. Ou seja, qualquer pessoa que tenha acesso á rede que está a ser utilizada poderá ler esses dados facilmente.

3.5 Captura 5: Autenticação RADIUS

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.170.135	192.168.170.131	RADIUS	200	Access-Request 16-240
2	0.000064	192.168.170.131	192.168.170.135	RADIUS	126	Access-Accept 16-240

Figure 11: *Captura5*

- **Intervenientes**:
 - *Origem*: 192.168.170.135 (Identificado como ‘pfSense.home.arpa’ com o MAC ‘00:0c:29:ae:77:ff’ pela VMware)
 - *Destino*: 192.168.170.131 com MAC 00:0c:29:d5:9f:77
- **Protocolo Principal**: RADIUS[8] (Remote Authentication Dial-In User Service)
- **Operações Realizadas**:
 - *Quem Inicia*: A origem 192.168.170.135 envia um ‘Access-Request’ para tentar autenticar o utilizador ”bob”.
 - *Quem Responde*: O destino 192.168.170.131 responde com um ‘Access-Accept’, indicando que a autenticação foi bem-sucedida.
 - *Características da Comunicação*: A comunicação ocorre sobre o protocolo UDP, especificamente nas portas 58157 (origem) e 1812 (destino).

- *Dados*: Os dados mais relevantes incluem o nome de utilizador ("bob") e vários pares de atributos de valor (AVP) que detalham o tipo de serviço, o identificador NAS, entre outros.

- **Problemas de Segurança:**

- *Intercepção*:: Como o RADIUS só encripta o atributo "User-Password" (que nem está presente nas pacotes da captura), toda a outra informação estará exposta. Assim, se um atacante interceptar este pacote, terá acesso a todos os dados usados pelo cliente na autenticação.
- *Ataque de Replay*: Um atacante que capture o 'Access-Request' pode tentar reenviá-lo para ganhar acesso.
- *Lack of Integrity Check*: Sem uma verificação de integridade adequada, os pacotes podem ser alterados durante o trânsito.
- *Mitigação*: Eis algumas formas de torná-mos este processo mais seguro, assim, protegendo-nos de possíveis ataques.
 - * Utilizar o RADIUS sobre TLS (RadSec[9]) para garantir a encriptação.
 - * Implementar uma autenticação baseada em desafio-resposta. O primeiro pacote menciona "MS-CHAP", mas a captura não possui nenhum pacote de "Access-Challenge". portanto, podemos deduzir algumas possibilidades:
 - O cliente está a autenticar-se outra vez, daí o servidor não enviar o pacote respetivo ao desafio.
 - A captura foi alterada e o(s) pacote(s) foram removidos.
 - * Manter os sistemas atualizados.
 - * Monitorizar o tráfego de rede para detetar atividades suspeitas.

- **Observações Adicionais:** A autenticação RADIUS é amplamente utilizada em infraestruturas empresariais e, portanto, assegurar a sua comunicação é de extrema importância. A capacidade de um atacante interceptar ou mesmo alterar pacotes pode ter implicações significativas para a segurança da rede.

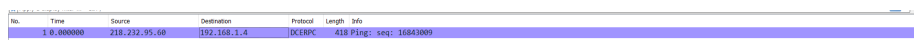
3.6 Captura 6: SQL Slammer

- **Intervenientes:**
 - *Origem:* 218.232.95.60 (MAC 11:22:33:44:55:66)
 - *Destino:* 192.168.1.4 (MAC de:ad:ca:fe:ba:be)
- **Protocolo Principal:** DCERPC[5] (Distributed Computing Environment / Remote Procedure Call)
- **Operações Realizadas:**
 - *Quem Inicia:* O endereço de origem 218.232.95.60.
 - *Quem Responde:* Não há resposta registada na captura.
 - *Características da Comunicação:* O pacote é enviado para a porta 1434, associada ao Microsoft SQL Server.
 - *Dados:* O pacote contém um comando de "ping" no protocolo DCERPC.

Esta captura em questão, possui apenas um pacote. Mas uma análise do mesmo, levanta várias suspeitas.

- **Análise Detalhada:**
 - *porto de Destino:* A porta 1434 é associada ao Microsoft SQL Server, um alvo conhecido do SQL Slammer[10].
 - *Tamanho do Pacote:* A pequena dimensão de 376 bytes (tamanho da payload) coincide com a conhecida assinatura do SQL Slammer.
 - *Dados Repetitivos:* Valores como '01010101-0101-0101-0101-010101010101' sugerem uma tentativa de *overflow* de buffer, ao invés de dados genuínos.
 - *Protocolo DCERPC:* A tentativa de "ping" não se alinha com o comportamento esperado do tráfego normal, indicando potencialmente atividade maliciosa.
- **Problemas de Segurança:**
 - *Ausência de resposta:* A falta de uma resposta na captura pode ser devido a dois motivos:
 - * A captura registou aquele pacote apenas, dificultando a interpretação do que poderá ter acontecido.
 - * A captura não possui um pacote de resposta, pois o servidor já se encontraria num estado, impossibilitado de responder. A vulnerabilidade já havia sido explorada.
 - *Natureza do Ataque:* Dadas as características acima, é provável que o pacote seja uma instância do worm SQL Slammer que tenta explorar vulnerabilidades do Microsoft SQL Server.

- *Impacto*: Interrupção dos serviços, consumo exagerado da largura de banda e recursos do sistema.
- *Mitigação*:
 - * Aplicar patches e atualizações de segurança ao Microsoft SQL Server.
 - * Bloquear o tráfego na porto 1434.
 - * Monitorizar constantemente o tráfego da rede.
- **Observações Adicionais**: O SQL Slammer teve um impacto significativo na internet em 2003, realçando a importância de manter os sistemas atualizados e de monitorizar o tráfego da rede.[2]



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.4	192.168.1.4	DC10PC	418	Port 1434

Figure 12: *Captura6*

4 Conclusões

Ao longo deste trabalho, conseguimos perceber a importância da análise de capturas de pacotes na identificação e prevenção de potenciais vulnerabilidades e ameaças à segurança informática. O tráfego de rede, muitas vezes, esconde padrões e atividades que, à primeira vista, podem parecer inocentes, mas, ao serem examinados mais profundamente, revelam tentativas de invasão, malware em comunicação com servidores de comando e controlo, ou até mesmo falhas na configuração de dispositivos que podem deixar a rede exposta.

Algumas das nossas principais descobertas incluem:

- A presença de tráfego não encriptado, mesmo em aplicações que transmitem dados sensíveis, sublinhando a necessidade de adoção generalizada de protocolos seguros, como HTTPS e TLS.
- Tentativas recorrentes de acesso a portos conhecidas por serem usadas por serviços vulneráveis, sugerindo tentativas de exploração por atores maliciosos.
- Padrões de tráfego que indicam a possibilidade de dispositivos comprometidos na rede, servindo de lembrete da importância de manter todos os dispositivos, não apenas servidores, atualizados e protegidos.

A capacidade de interpretar e analisar o tráfego de rede é uma habilidade inestimável para qualquer profissional de segurança informática. Como demonstrado, mesmo uma simples análise pode descobrir falhas graves que, se não forem tratadas, podem levar a violações de dados, downtime e perda de confiança por parte dos utilizadores e clientes.

Finalmente, este trabalho reforça a noção de que a segurança não é um estado, mas sim um processo contínuo. Com a evolução constante das ameaças e do cenário de segurança, é imperativo que as organizações não apenas implementem soluções de segurança robustas, mas também invistam em monitorização e análise proativas para se manterem um passo à frente dos atores maliciosos.

5 Referências

- [1] firewall. *FTP*. 2023. URL: <https://www.firewall.cx/networking/network-protocols/protocols-ftp.html>.
- [2] geeksforgeeks. *SQLSlammer2003*. 2023. URL: <https://www.geeksforgeeks.org/what-is-sql-slammer-virus/>.
- [3] microsoftlearn. *DHCP*. 2023. URL: <https://learn.microsoft.com/pt-br/windows-server/networking/technologies/dhcp/dhcp-top>.
- [4] wiki. *SSDP*. 2023. URL: https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol.
- [5] Wikipedia. *DCE/RPC*. 2023. URL: <https://en.wikipedia.org/wiki/DCE/RPC>.
- [6] Wikipedia. *LDAP*. 2023. URL: https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol.
- [7] Wikipedia. *POP*. 2023. URL: https://en.wikipedia.org/wiki/Post_Office_Protocol.
- [8] Wikipedia. *RADIUS*. 2023. URL: <https://en.wikipedia.org/wiki/RADIUS>.
- [9] Wikipedia. *RadSec*. 2023. URL: <https://en.wikipedia.org/wiki/RadSec>.
- [10] Wikipedia. *SQL Slammer*. 2003. URL: https://en.wikipedia.org/wiki/SQL_Slammer.
- [11] Wikipedia. *TelNet*. 2023. URL: <https://en.wikipedia.org/wiki/Telnet>.
- [12] wikiwireshark. *NBNS*. 2023. URL: <https://wiki.wireshark.org/NetBIOS/NBNS>.