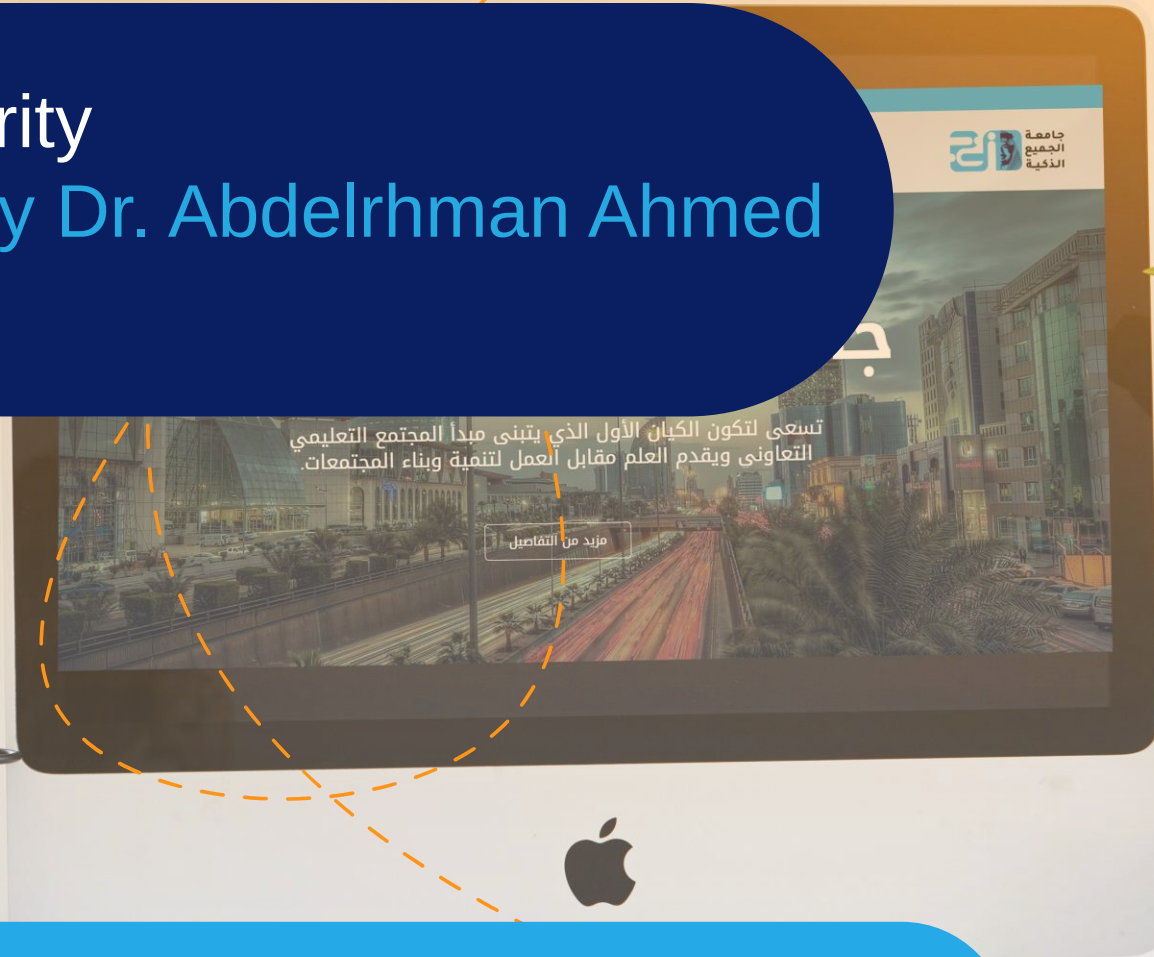


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 9



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Data monitoring and Analysis

Forward

- The document describes how to obtain valid information by technical means and analyze the information to locate security risks and threats.
- Data can be collected from network devices or from terminal systems that provide services. Data monitoring and analysis can reveal network security risks and strengthen the network. If a security event occurs, data monitoring and analysis help rapidly locate the threat, and provide support for defense and event investigation.

Objectives

- **Upon completion of this course, you will be able to:**
 - ☐ **Describe the technical means of data monitoring and analysis.**
 - ☐ **Describe the data collection process.**
 - ☐ **Use techniques to locate threats.**

- Evaluate network security before attacks occur, rectify the identified issues and strengthen the network.
- The following figure shows the security assessment method.



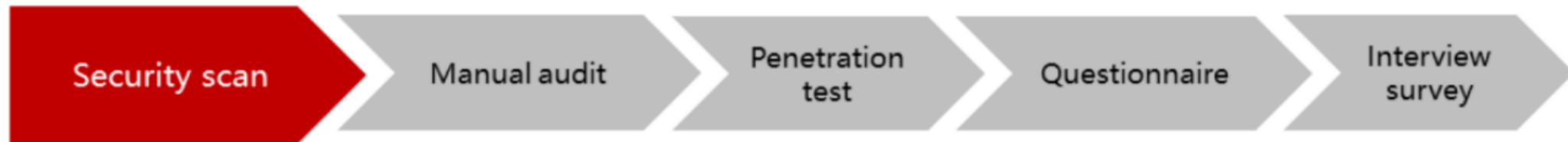
- **Objectives:** Use the scanning analysis and assessment tool to determine network security vulnerabilities of target systems.

- **Contents:**

- ☐ Enabled ports
- ☐ Weak passwords
- ☐ SQL injection vulnerability
- ☐ Cross-site scripting (XSS) vulnerability

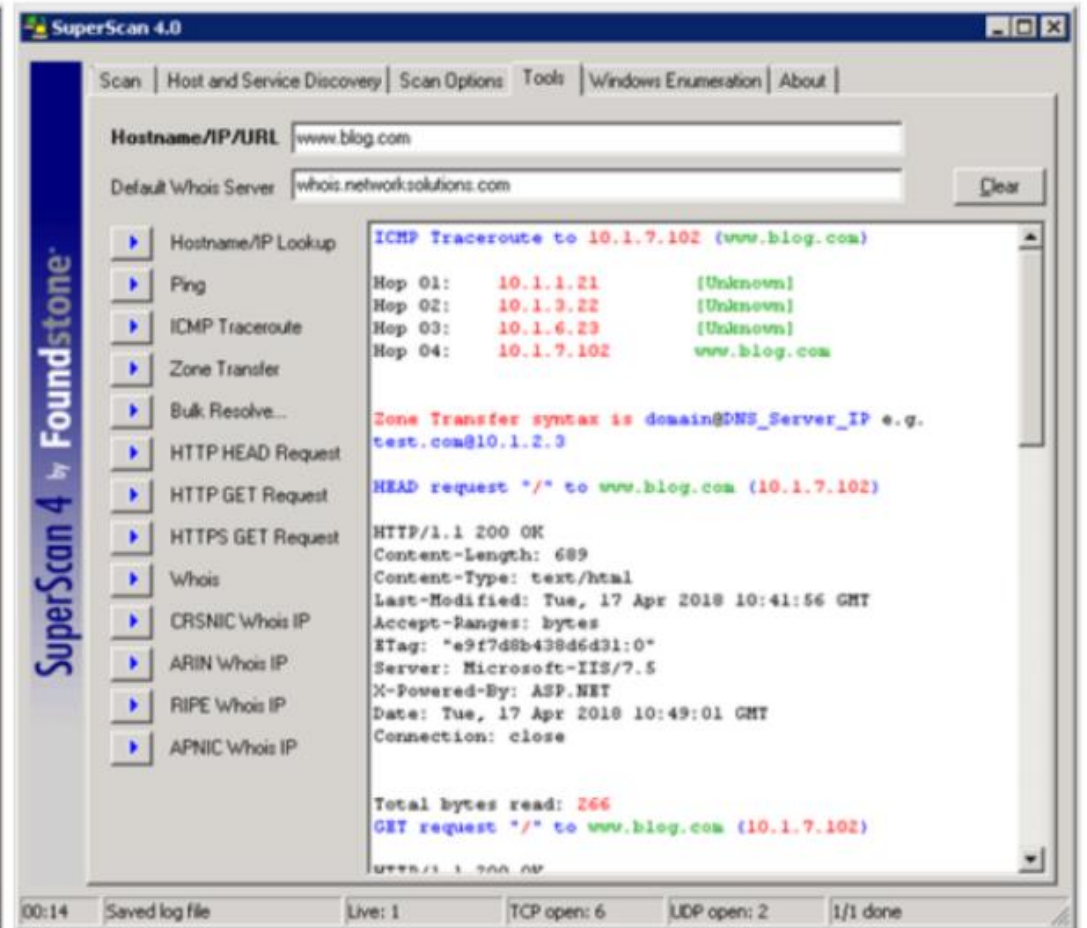
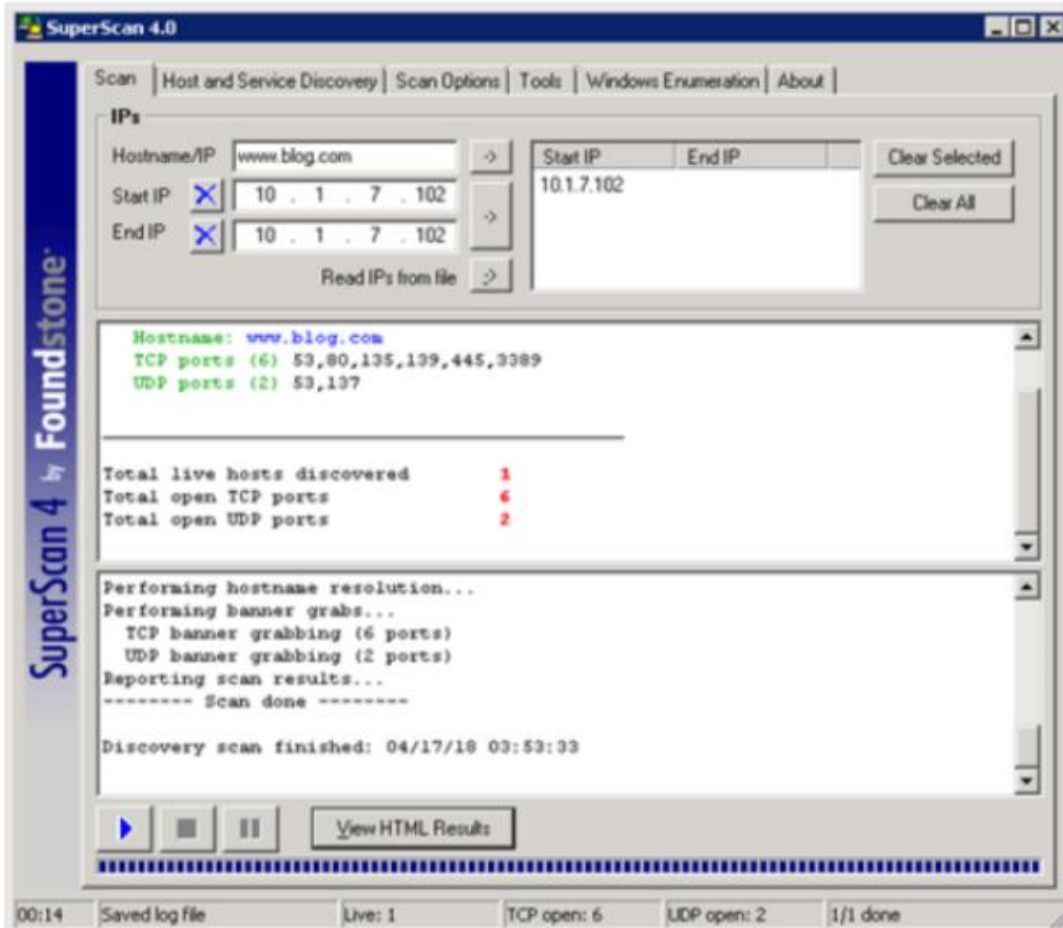
- **Output**

- ☐ Result generated by the scanner



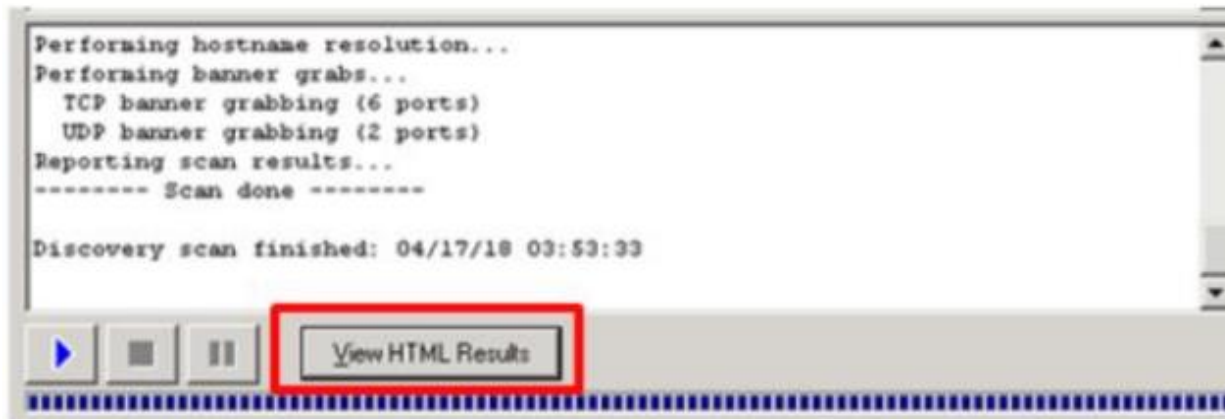
Type		Name	Function
Types	Port scanning software	SuperScan	Provides the following functions: • Uses PING to check whether IP addresses are reachable. • Checks service types provided by target computers. • Checks whether target computers in a certain scope are online and checks the ports of the target computers.
		Nmap	A network scanning and sniffing toolkit in Linux. Basic functions include: checking hosts are online, scanning host ports, sniffing the network services provided, and verifying the operating system used by the host.
	Vulnerability scanner	Sparta	Integrated in Kali Linux to detect the enabled services and ports, and crack user names and passwords of applications using a dictionary attack.
	App scanner	Burp Suite	An integrated platform to penetrate web applications. It includes a wide range of tools and relevant interfaces to speed up the attacks on applications.

- SuperScan is used to scan the web server in a lab environment.



Viewing the SuperScan Result

- ❖ On the Scan tab, click View HTML Result. The SuperScan report is displayed



SuperScan Report - 04/17/18 03:53:19

IP	10.1.7.102
Hostname	www.blog.com
Netbios Name	1
Workgroup/Domain	WORKGROUP

TCP Ports (6)	
53	Domain Name Server
80	World Wide Web HTTP
135	DCE endpoint resolution
139	NETBIOS Session Service
445	Microsoft DS
3389	MS Terminal Server

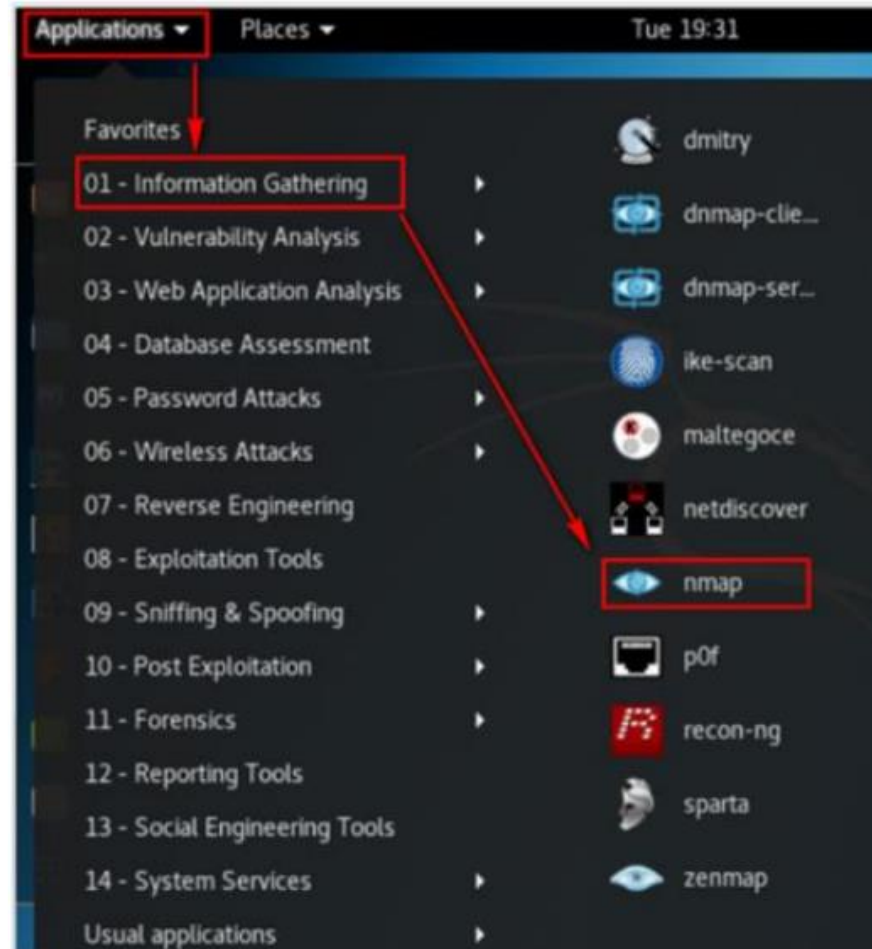
UDP Ports (2)	
53	Domain Name Server
137	NETBIOS Name Service

TCP Port	Banner
80 World Wide Web HTTP	HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Tue, 17 Apr 2018 10:41:58 GMT Accept-Ranges: bytes ETag: "e-1000000000" Server: Microsoft-IIS/7.5 X-Powered-By: ASP.NET Date: Tue, 17 Apr 2018 10:53:25 GMT Connection: close Content-Length: 589

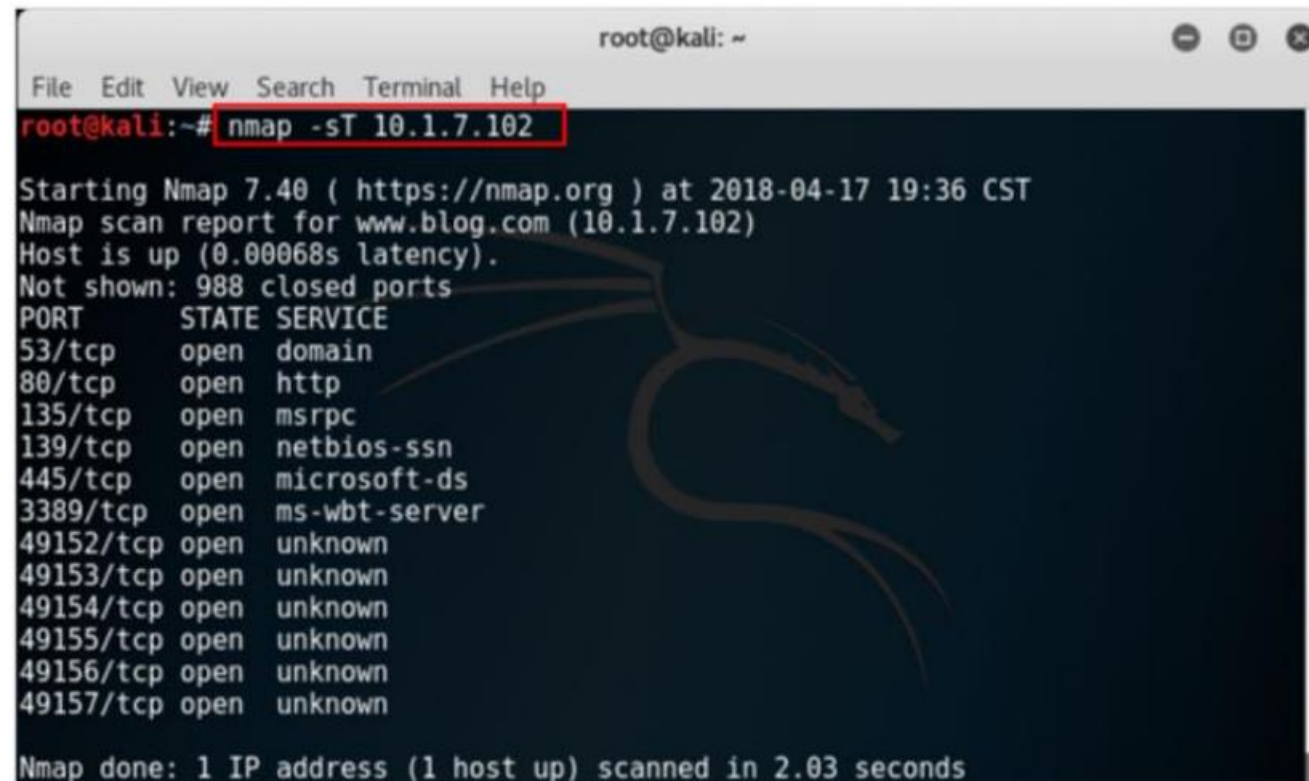
UDP Port	Banner
137 NETBIOS Name Service	MAC Address: 0-10-0-0-0-0 NIC Vendor : Unknown Netbios Name Table (0 names) 1-00-UNIQUE Workstation service name WORKGROUP-00-GROUP Workstation service name 1-20-UNIQUE Server services name

Total hosts discovered	1
Total open TCP ports	6
Total open UDP ports	2

- Click Applications > Information Gathering > nmap.



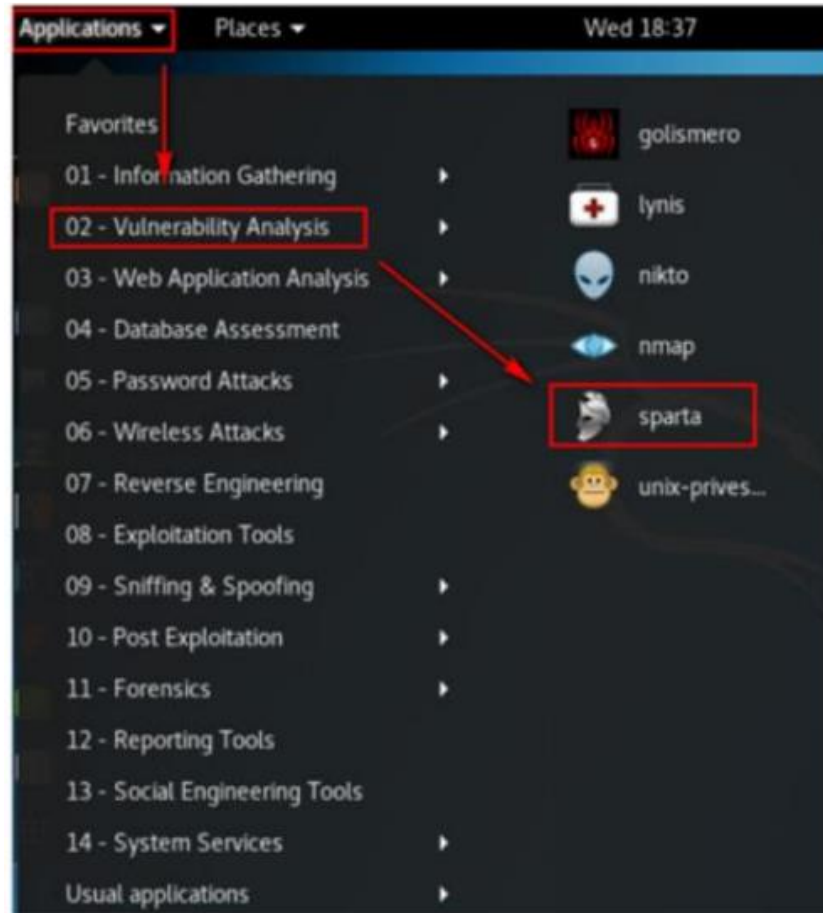
- Collect information about the target system based on the parameter rules of the Nmap tool.
- The following figure shows how to scan the TCP ports enabled on the host:



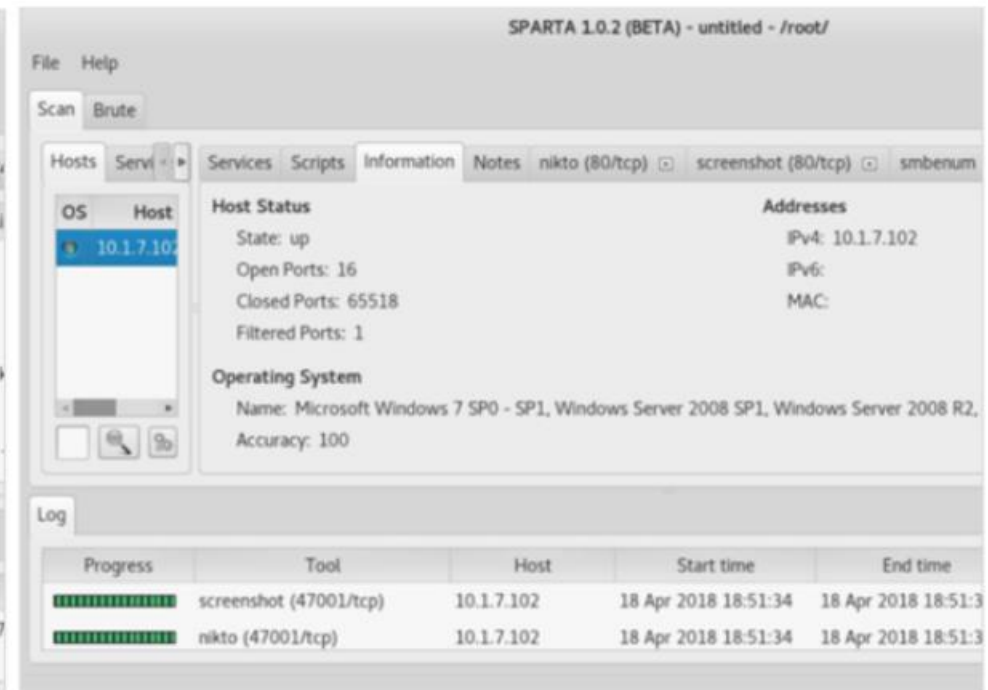
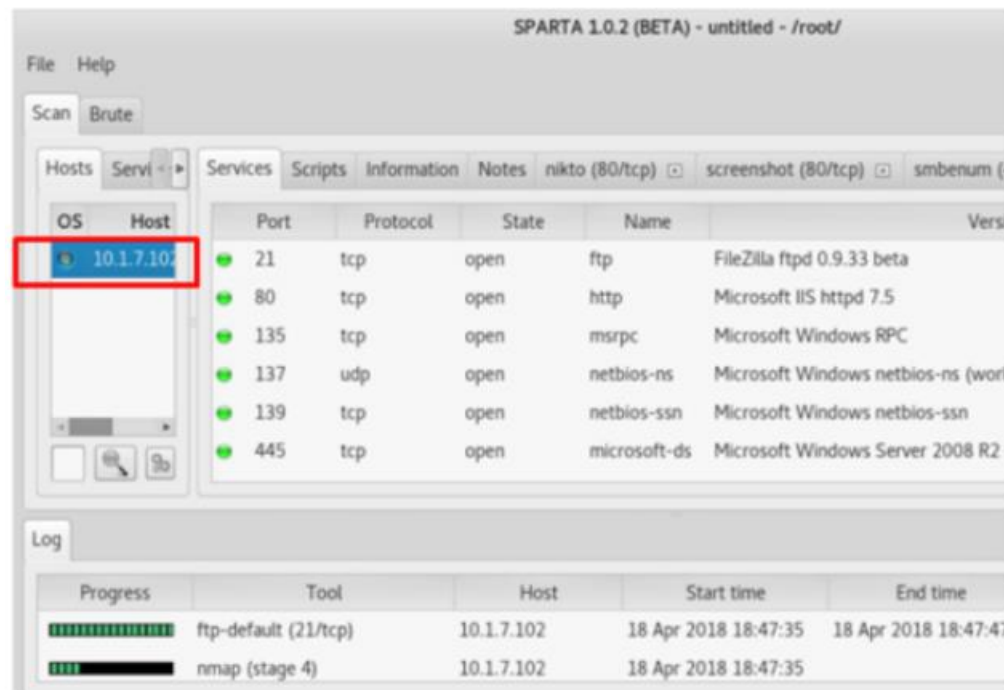
The screenshot shows a terminal window titled 'root@kali: ~'. The command 'nmap -sT 10.1.7.102' is entered and highlighted with a red box. The output of the command is as follows:

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-04-17 19:36 CST
Nmap scan report for www.blog.com (10.1.7.102)
Host is up (0.00068s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
```

- Click Applications > Vulnerability Analysis > sparta.

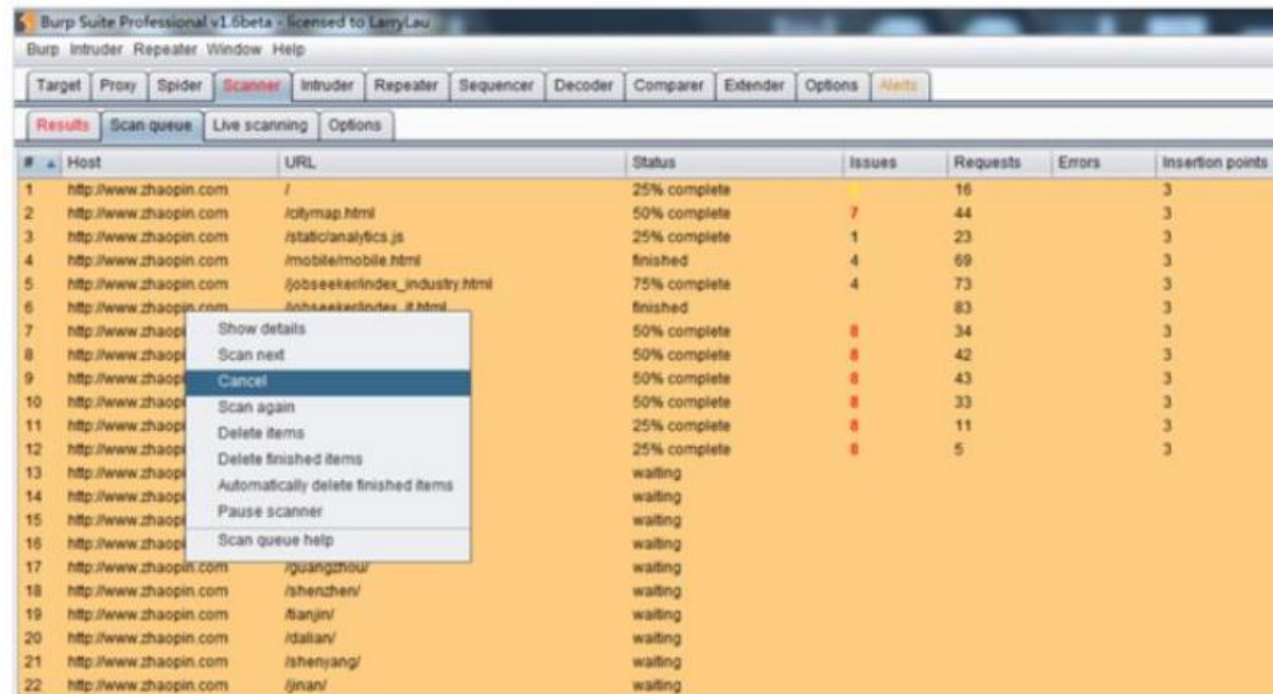


- On the Sparta page, add the address segment or host address to be scanned. The Sparta result shows the ports and apps enabled on the target host, as well as the operating system being used.

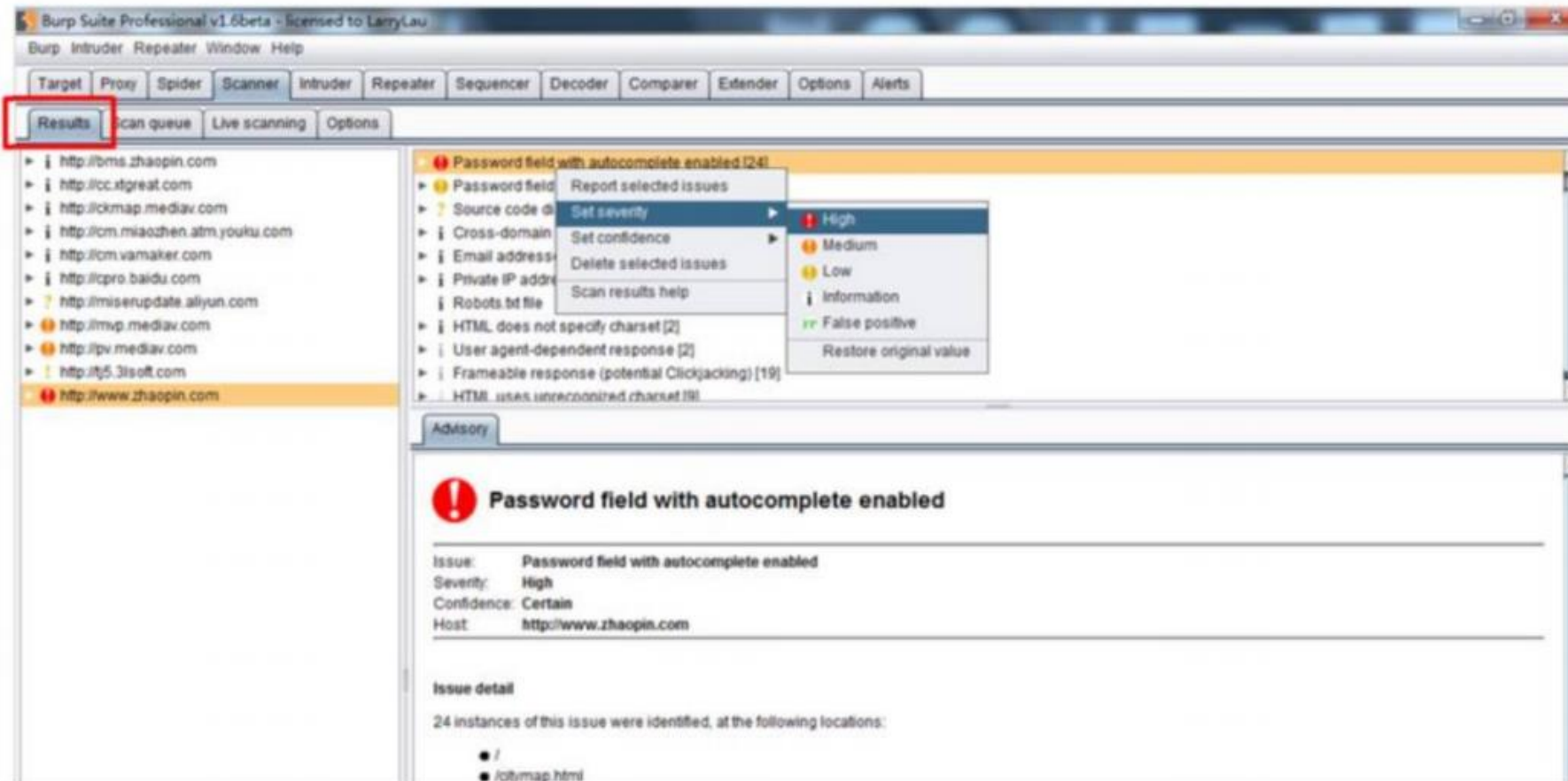


• Burp Suite sends requests to apps and uses payloads to verify vulnerabilities. Burp Suite can effectively scan the following vulnerabilities:

- ❑ Client vulnerabilities: XSS, HTTP header injection, and operation redirection
- ❑ Server vulnerabilities: SQL injection, command line injection, and file search



- The Results tab page displays the scanned vulnerability details.



- Objectives:

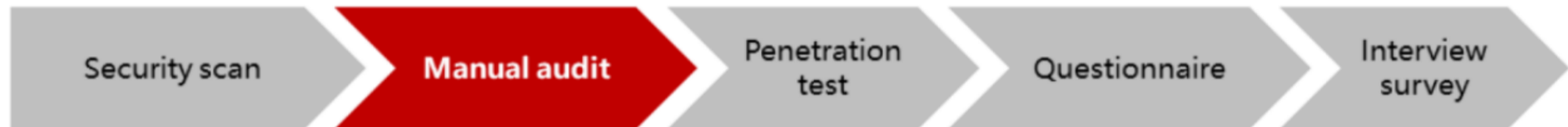
- ☐ Manual audit is a complement to security scan. It requires no software installation on the target system and does not affect the running status. It is useful for important hosts that do not allow software installation.

- Method:

- ☐ Security specialists manually inspect target systems, including the host system, service system, database, network device, and security device.

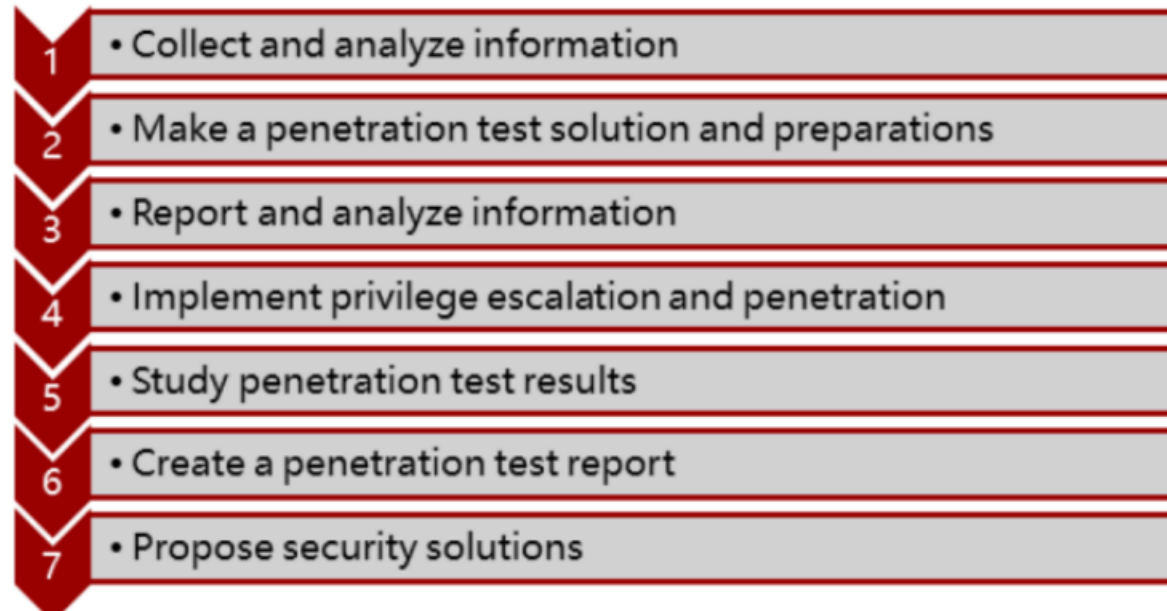
- ☐ The following check items may vary according to target systems:

- Latest patch installed or not
- Service minimization principle used or not, and unnecessary services and ports enabled or not
- Firewall configuration policy correct or not





- ❖ A penetration test is carried out as part of an external inspection. This test is an attempt to evaluate the security of operating systems and network services by safely exploiting vulnerabilities.
- ❖ The penetration test process is as follows:





- Survey audience
 - Network system administrator, security administrator, technical director, etc.
- Survey scope
 - Service, asset, threat, and vulnerability (from the perspective of management)
- Questionnaire style
 - Integrity, specificity, simplicity, and consistency

Operational operation

1. Does the network administrator recommend changes to the configuration of the network system?
A. Yes B. No C. Others_____
2. Are there regular audits and checks on important servers and routers running on the network?
A. Yes B. No C. Others_____
3. Are the backbone routers strictly using fixed terminals for configuration and management?
A. Yes B. No C. Others_____
4. Has the intrusion detection device running on the network system been selected to detect and control system intrusion events in a timely manner?
A. Yes B. No C. Others_____
5. Have you considered future resource and capacity requirements when designing a new application system?
A. Yes B. No C. Others_____
6. Are the administrators of important hosts monitoring the usage of major system resources, including processor, main memory, file storage, and communication system bandwidth?
A. Yes B. No C. Others_____



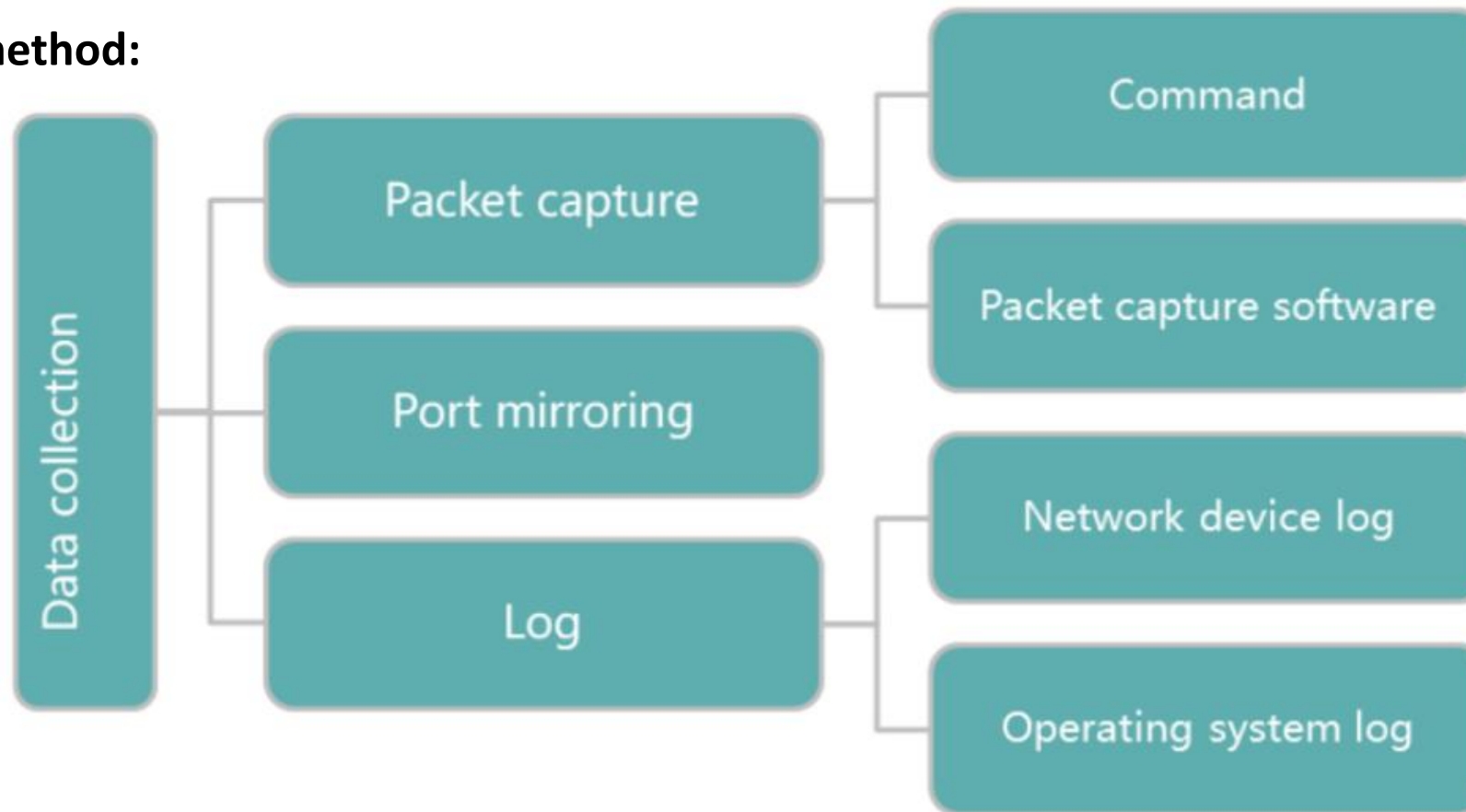
- Audience
 - Security administrator, technical director, network system administrator, etc.
- Interview topics
 - Questionnaire results
 - Obtaining management enforcement details
 - Users' opinions and comments

Security Management Interview Record

NO.	Category	Investigate Subject	Results
1	Security Strategy	Does the company have a systematic, unified security strategy?	
2	Security Strategy	Is the security policy detailed to the collective requirements of all aspects of information security?	
3	Security Strategy	Has the security policy been developed by a dedicated person for maintenance?	
4	Security Strategy	Are you reviewing your published security policy, checking and finding out where it is inappropriate or outdated?	
5	Security Organization	Has the company set up a dedicated information security department or working group responsible for security management?	
6	Security Organization	Does the company have relevant departments or leaders to coordinate the implementation of safety management in all departments?	
7	Security Organization	Does the company explicitly require individuals to be responsible for the safety of personally-managed assets? Is there a clear disciplinary rule for employees who violate security policies and security procedures?	

- When an attack occurs, users must collect data, analyze attack methods and vulnerabilities, and rectify the situation to minimize the impact.

- Data collection method:



- Command to check the OSPF neighbor states

```
<Switch> debugging ospf event
Apr 12 2018 12:03:16.370.1-05:00 SW3 RM/6/RMDEBUG:
FileID: 0x7017802d Line: 1136 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv HelloReceived State Down -> Init.
Apr 12 2018 12:03:16.380.1-05:00 SW3 RM/6/RMDEBUG:
FileID: 0x7017802d Line: 1732 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv 2WayReceived State Init -> 2Way.
Apr 12 2018 12:03:16.390.1-05:00 SW3 RM/6/RMDEBUG:
FileID: 0x7017802d Line: 1732 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv AdjOk? State 2Way -> ExStart.
Apr 12 2018 12:03:16.400.1-05:00 SW3 RM/6/RMDEBUG:
FileID: 0x7017802d Line: 1845 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv NegotiationDone State ExStart -> Exchange.
Apr 12 2018 12:03:16.410.1-05:00 SW3 RM/6/RMDEBUG:
FileID: 0x7017802d Line: 1957 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv ExchangeDone State Exchange -> Loading.
Apr 12 2018 12:03:16.430.1-05:00 SW3 RM/6/RMDEBUG:
FileID: 0x7017802d Line: 2359 Level: 0x20
  OSPF 1: Nbr 10.1.10.34 Rcv LoadingDone State Loading -> Full.
```

- Command to view OSPF packet information

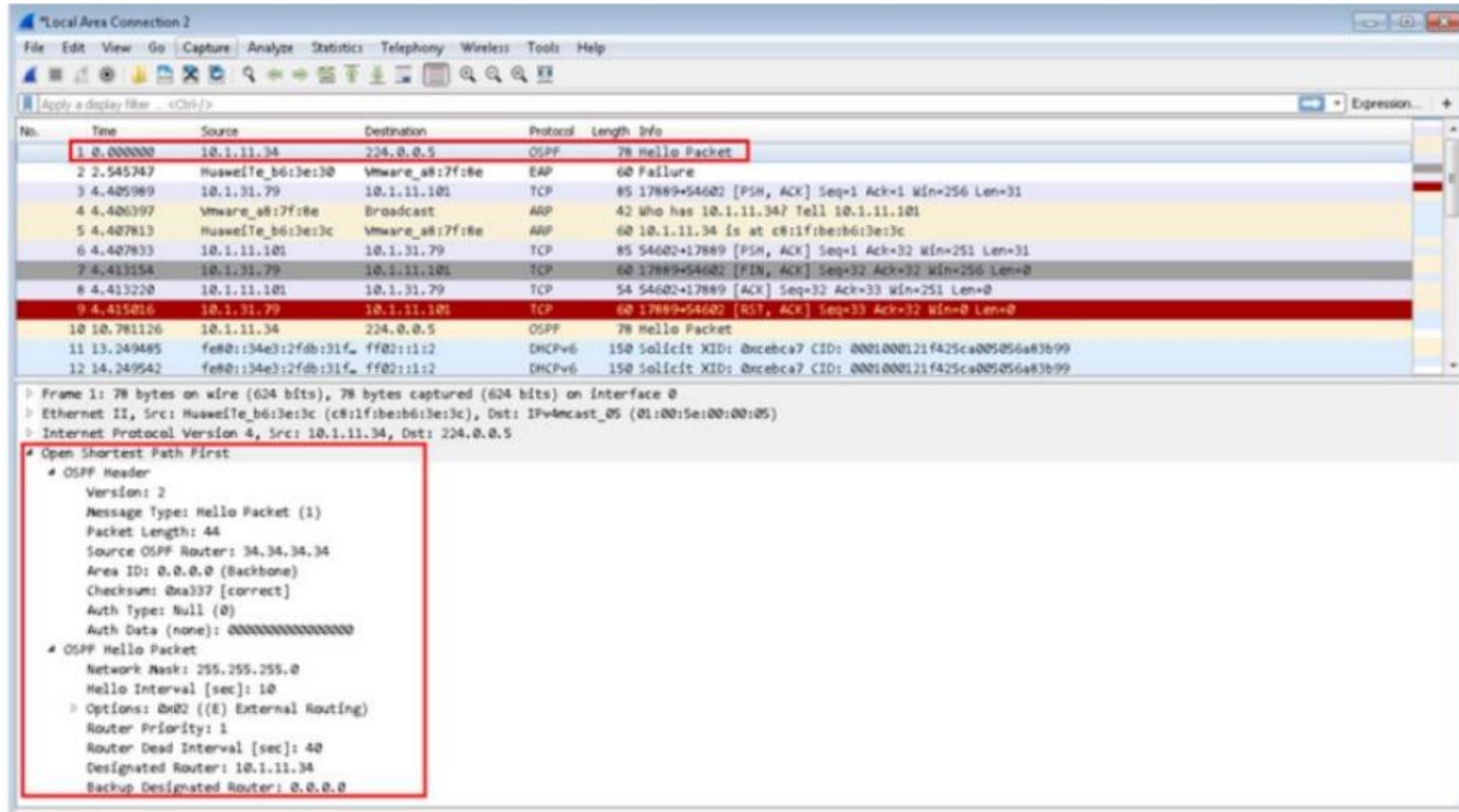
```
<Switch> debugging ospf packet
```

```
Apr 12 2018 12:05:42.930.2-05:00 SW3 RM/6/RMDEBUG: Source Address: 10.1.10.34
Apr 12 2018 12:05:42.930.3-05:00 SW3 RM/6/RMDEBUG: Destination Address: 224.0.0.5
Apr 12 2018 12:05:42.940.1-05:00 SW3 RM/6/RMDEBUG: Ver# 2, Type: 1 (Hello)
Apr 12 2018 12:05:42.940.2-05:00 SW3 RM/6/RMDEBUG: Length: 48, Router: 34.34.34.34
Apr 12 2018 12:05:42.940.3-05:00 SW3 RM/6/RMDEBUG: Area: 0.0.0.0, Chksum: 4dcf
Apr 12 2018 12:05:42.940.4-05:00 SW3 RM/6/RMDEBUG: AuType: 00
Apr 12 2018 12:05:42.940.5-05:00 SW3 RM/6/RMDEBUG: Key(ascii): * * * * * * * d
Apr 12 2018 12:05:42.940.6-05:00 SW3 RM/6/RMDEBUG: Net Mask: 255.255.255.0e
Apr 12 2018 12:05:42.940.7-05:00 SW3 RM/6/RMDEBUG: Hello Int: 10, Option: _E_
Apr 12 2018 12:05:42.940.8-05:00 SW3 RM/6/RMDEBUG: Rtr Priority: 1, Dead Int: 40
Apr 12 2018 12:05:42.940.9-05:00 SW3 RM/6/RMDEBUG: DR: 10.1.10.34
Apr 12 2018 12:05:42.940.1-05:00 SW3 RM/6/RMDEBUG: BDR: 10.1.10.33
Apr 12 2018 12:05:42.940.2-05:00 SW3 RM/6/RMDEBUG: # Attached Neighbors: 1
Apr 12 2018 12:05:42.940.3-05:00 SW3 RM/6/RMDEBUG: Neighbor: 33.33.33.33
```

- Use the Wireshark to capture packets, and check how OSPF adjacency is formed.



- Use the Wireshark to capture packets, and check OSPF packet information.



The image shows a Wireshark packet capture window titled "Local Area Connection 2". The packet list on the left shows a table of captured packets. Packet 1 is highlighted in red and is an OSPF Hello Packet from 10.1.11.34 to 224.0.0.5. The packet details pane on the right shows the structure of this packet, with the OSPF Header and OSPF Hello Packet sections expanded and highlighted in red.

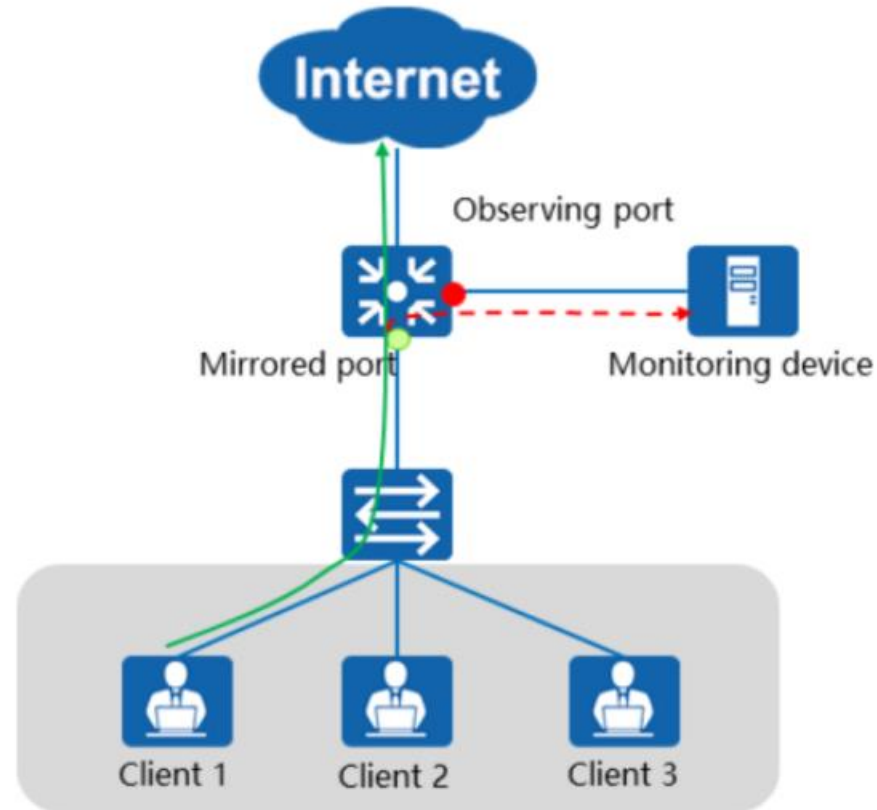
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.11.34	224.0.0.5	OSPF	78	Hello Packet
2	2.545747	HuaweiTe_b6:3e:3c	Vmware_s8:7f:8e	EAP	60	Failure
3	4.405989	10.1.31.79	10.1.11.101	TCP	85	17889→54602 [PSH, ACK] Seq=1 Ack=1 Win=256 Len=31
4	4.406397	Vmware_s8:7f:8e	Broadcast	ARP	42	Who has 10.1.11.34? Tell 10.1.11.101
5	4.407813	HuaweiTe_b6:3e:3c	Vmware_s8:7f:8e	ARP	60	10.1.11.34 is at c8:1f:8e:b6:3e:3c
6	4.407833	10.1.11.101	10.1.31.79	TCP	85	54602→17889 [PSH, ACK] Seq=1 Ack=32 Win=251 Len=31
7	4.413154	10.1.31.79	10.1.11.101	TCP	60	17889→54602 [FIN, ACK] Seq=32 Ack=32 Win=256 Len=0
8	4.413220	10.1.11.101	10.1.31.79	TCP	54	54602→17889 [ACK] Seq=32 Ack=33 Win=251 Len=0
9	4.415016	10.1.31.79	10.1.11.101	TCP	60	17889→54602 [RST, ACK] Seq=33 Ack=32 Win=0 Len=0
10	10.781126	10.1.11.34	224.0.0.5	OSPF	78	Hello Packet
11	13.249485	fe80::34e3:2fdb:31f_	ff02::1:2	DHCPv6	150	Solicit XID: 0xcebca7 CID: 0001000121f425ca005056a83b99
12	14.249542	fe80::34e3:2fdb:31f_	ff02::1:2	DHCPv6	150	Solicit XID: 0xcebca7 CID: 0001000121f425ca005056a83b99

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 Ethernet II, Src: HuaweiTe_b6:3e:3c (c8:1f:8e:b6:3e:3c), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
 Internet Protocol Version 4, Src: 10.1.11.34, Dst: 224.0.0.5

Open Shortest Path First

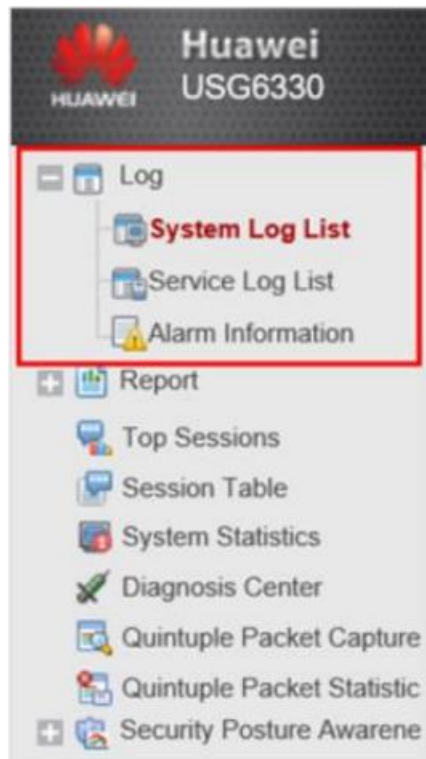
- OSPF Header
 - Version: 2
 - Message Type: Hello Packet (1)
 - Packet Length: 44
 - Source OSPF Router: 34.34.34.34
 - Area ID: 0.0.0.0 (Backbone)
 - Checksum: 0xa337 [correct]
 - Auth Type: Null (0)
 - Auth Data (none): 0000000000000000
- OSPF Hello Packet
 - Network Mask: 255.255.255.0
 - Hello Interval [sec]: 10
 - Options: 0x02 ((E) External Routing)
 - Router Priority: 1
 - Router Dead Interval [sec]: 40
 - Designated Router: 10.1.11.34
 - Backup Designated Router: 0.0.0.0

- Port mirroring enables a device to copy the packets passing through a mirrored port and send them to a specified observing port for analysis and monitoring.

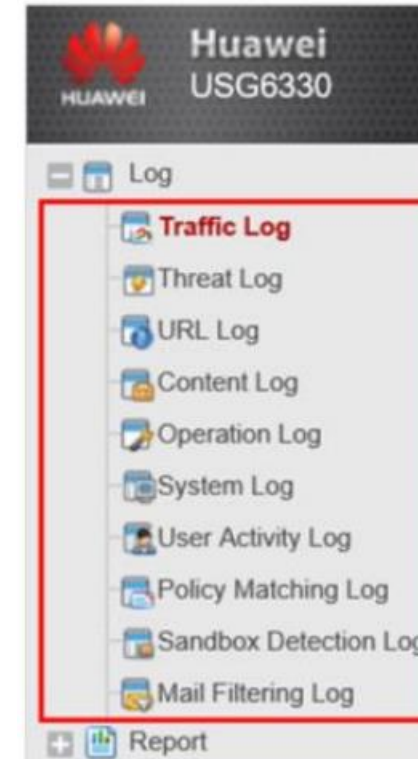


- The USG6330 firewall is used as an example. It supports logs and reports. When the hard disk is unavailable, you can only view and export system logs and service logs.

- **Hard disk unavailable:**



- **Hard disk available:**



- Log formats supported by the firewall:

Format	Scenario
Binary	Session logs are output in binary format and consume few network resources. Such logs, however, cannot be viewed on the firewall. You must export them to a log server.
Syslog	If the session logs, packet loss logs, and system logs are generated in Syslog format, the log information is displayed in text.
NetFlow	The firewall can also export session logs in NetFlow format to a log server for the administrator to analyze IP packet flows on the network.
Dataflow	Service logs are generated in Dataflow format so that they can be viewed on the log server.

- This example uses the USG6000 firewall to describe how to view system logs.

□ Choose Monitor > Log > System Log.

Export Refresh Please select a security level Search Clear Search Condition				
Security Level	Log Type	Time	Log Source	Description
Warning	CFGCHECK	Apr 13 2018 15:49:57	FW1 %N01HRP1/4/CFGCHECK(1)[0]:	HRP checks the local and the remote devices, and the result is Different Configuration.
Warning	DOWNLOAD_FAIL	Apr 12 2018 22:40:50	FW1 %N01UPDATE/4/DOWNLOAD_FAIL(1)[1]:	Failed to download the new version. (SyslogId=140, User=SystemTimer, IP=**, Module=CNC, Status=au...
Warning	DOWNLOAD_FAIL	Apr 12 2018 22:40:43	FW1 %N01UPDATE/4/DOWNLOAD_FAIL(1)[2]:	Failed to download the new version. (SyslogId=139, User=SystemTimer, IP=**, Module=IP-REPUTATION, ...
Warning	DOWNLOAD_FAIL	Apr 12 2018 22:40:30	FW1 %N01UPDATE/4/DOWNLOAD_FAIL(1)[3]:	Failed to download the new version. (SyslogId=138, User=SystemTimer, IP=**, Module=SA-SDB, Status=...
Warning	DOWNLOAD_FAIL	Apr 12 2018 22:40:23	FW1 %N01UPDATE/4/DOWNLOAD_FAIL(1)[4]:	Failed to download the new version. (SyslogId=137, User=SystemTimer, IP=**, Module=AV-SDB, Status=...
Warning	DOWNLOAD_FAIL	Apr 12 2018 22:40:10	FW1 %N01UPDATE/4/DOWNLOAD_FAIL(1)[5]:	Failed to download the new version. (SyslogId=136, User=SystemTimer, IP=**, Module=IPS-SDB, Statu...
Warning	CFGCHECK	Apr 12 2018 15:49:57	FW1 %N01HRP1/4/CFGCHECK(1)[6]:	HRP checks the local and the remote devices, and the result is Different Configuration.
Warning	NBR_CHANGE_E	Apr 12 2018 11:20:01	FW1 %N01OSPF/4/NBR_CHANGE_E(1)[7]:	Neighbor changes event: neighbor status changed. (ProcessId=1, NeighborAddress=10.1.50.33, Neighb...
Warning	NBR_CHANGE_E	Apr 12 2018 11:20:01	FW1 %N01OSPF/4/NBR_CHANGE_E(1)[8]:	Neighbor changes event: neighbor status changed. (ProcessId=1, NeighborAddress=10.1.50.33, Neighb...
Warning	NBR_CHANGE_E	Apr 12 2018 11:20:01	FW1 %N01OSPF/4/NBR_CHANGE_E(1)[9]:	Neighbor changes event: neighbor status changed. (ProcessId=1, NeighborAddress=10.1.50.33, Neighb...
Warning	NBR_CHANGE_E	Apr 12 2018 11:20:01	FW1 %N01OSPF/4/NBR_CHANGE_E(1)[10]:	Neighbor changes event: neighbor status changed. (ProcessId=1, NeighborAddress=10.1.50.33, Neighb...
Warning	NBR_CHANGE_E	Apr 12 2018 11:19:54	FW1 %N01OSPF/4/NBR_CHANGE_E(1)[11]:	Neighbor changes event: neighbor status changed. (ProcessId=1, NeighborAddress=10.1.50.33, Neighb...
Error	NBR_DOWN_REASON	Apr 12 2018 11:19:54	FW1 %N01OSPF/3/NBR_DOWN_REASON(1)[12]:	Neighbor state leaves full or changed to Down. (ProcessId=1, NeighborRouterId=33.33.33.33, Neighb...

- This example uses the USG6000 to describe how to view service logs.

□ Choose Monitor > Log > Service Log

Service Log List

Export Refresh Please select a security level Search Clear Search Condition

Security Level	Log Type	Time	Log Source	Description
Warning	FIREWALLATCK	Mar 21 2018 18:04:44	FW1 %01ATK/4/FIREWALLATCK(1)[30]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 21 2018 17:57:44	FW1 %01ATK/4/FIREWALLATCK(1)[31]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 21 2018 17:52:44	FW1 %01ATK/4/FIREWALLATCK(1)[32]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 20 2018 20:20:44	FW1 %01ATK/4/FIREWALLATCK(1)[33]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 20 2018 20:19:44	FW1 %01ATK/4/FIREWALLATCK(1)[34]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 20 2018 20:19:14	FW1 %01ATK/4/FIREWALLATCK(1)[35]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 20 2018 20:15:44	FW1 %01ATK/4/FIREWALLATCK(1)[36]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 20 2018 20:10:14	FW1 %01ATK/4/FIREWALLATCK(1)[37]:	AttackType="Syn flood attack", slot=" ", cpu="0", receive interface=" ", proto="TCP", src="...
Warning	FIREWALLATCK	Mar 20 2018 20:09:44	FW1 %01ATK/4/FIREWALLATCK(1)[38]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 20 2018 20:08:44	FW1 %01ATK/4/FIREWALLATCK(1)[39]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/5 ", proto="TCP...
Warning	FIREWALLATCK	Mar 20 2018 20:08:14	FW1 %01ATK/4/FIREWALLATCK(1)[40]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/5 ", proto="TCP...
Warning	FIREWALLATCK	Mar 20 2018 20:08:14	FW1 %01ATK/4/FIREWALLATCK(1)[41]:	AttackType="Syn flood attack", slot=" ", cpu="0", receive interface=" ", proto="TCP", src="...
Warning	FIREWALLATCK	Mar 20 2018 20:07:44	FW1 %01ATK/4/FIREWALLATCK(1)[42]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/1 ", proto="UDP...
Warning	FIREWALLATCK	Mar 20 2018 20:05:44	FW1 %01ATK/4/FIREWALLATCK(1)[43]:	AttackType="IP spoof attack", slot=" ", cpu="0", receive interface="GE1/0/5 ", proto="ICM...

- This example uses the USG6000 to describe how to view alarms.

□ Choose Monitor > Log > Alarm Information.

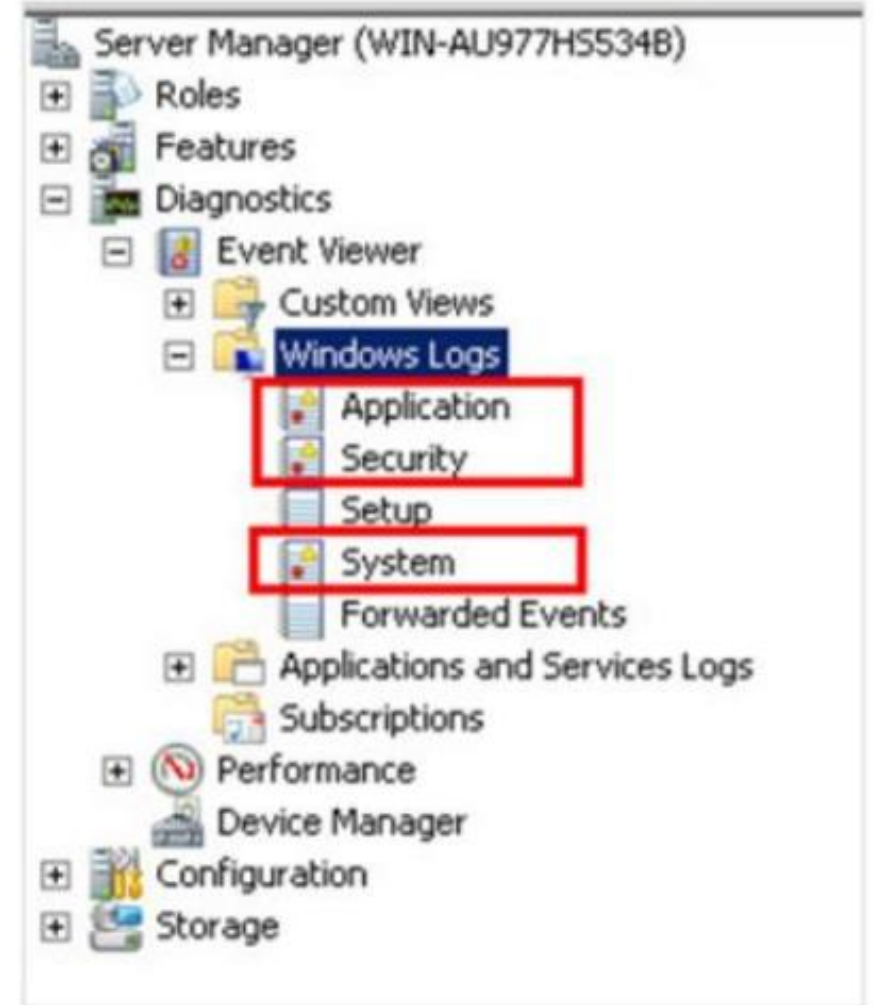
Security Level	Time	Alarm Source	Description
Warning	Aug 22 2018 11:30:42	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.100.251, Local inte...
Warning	Aug 22 2018 11:28:44	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=192.168.0.1, Local interfa...
Warning	Aug 22 2018 11:28:18	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.20.13, Local interf...
Warning	Aug 22 2018 11:20:37	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.100.251, Local inte...
Warning	Aug 22 2018 11:18:42	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=192.168.0.1, Local interfa...
Warning	Aug 22 2018 11:18:14	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.20.13, Local interf...
Warning	Aug 22 2018 11:10:32	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.100.251, Local inte...
Warning	Aug 22 2018 11:08:39	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=192.168.0.1, Local interfa...
Warning	Aug 22 2018 11:08:09	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.20.13, Local interf...
Warning	Aug 22 2018 11:00:27	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.100.251, Local inte...
Warning	Aug 22 2018 10:58:39	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=192.168.0.1, Local interfa...
Warning	Aug 22 2018 10:58:06	FW3 ARP/4/ARP_IPCONFLICT_TRAP:	OID 1.3.6.1.4.1.2011.5.25.123.2.6 ARP detects IP conflict. (IP address=172.21.20.13, Local interf...

- When using Windows:

1. Click Start.
2. Right-click Computer and choose Manage.
3. Select System Tools > Event Viewer > Windows Logs

Windows system logs are classified into:

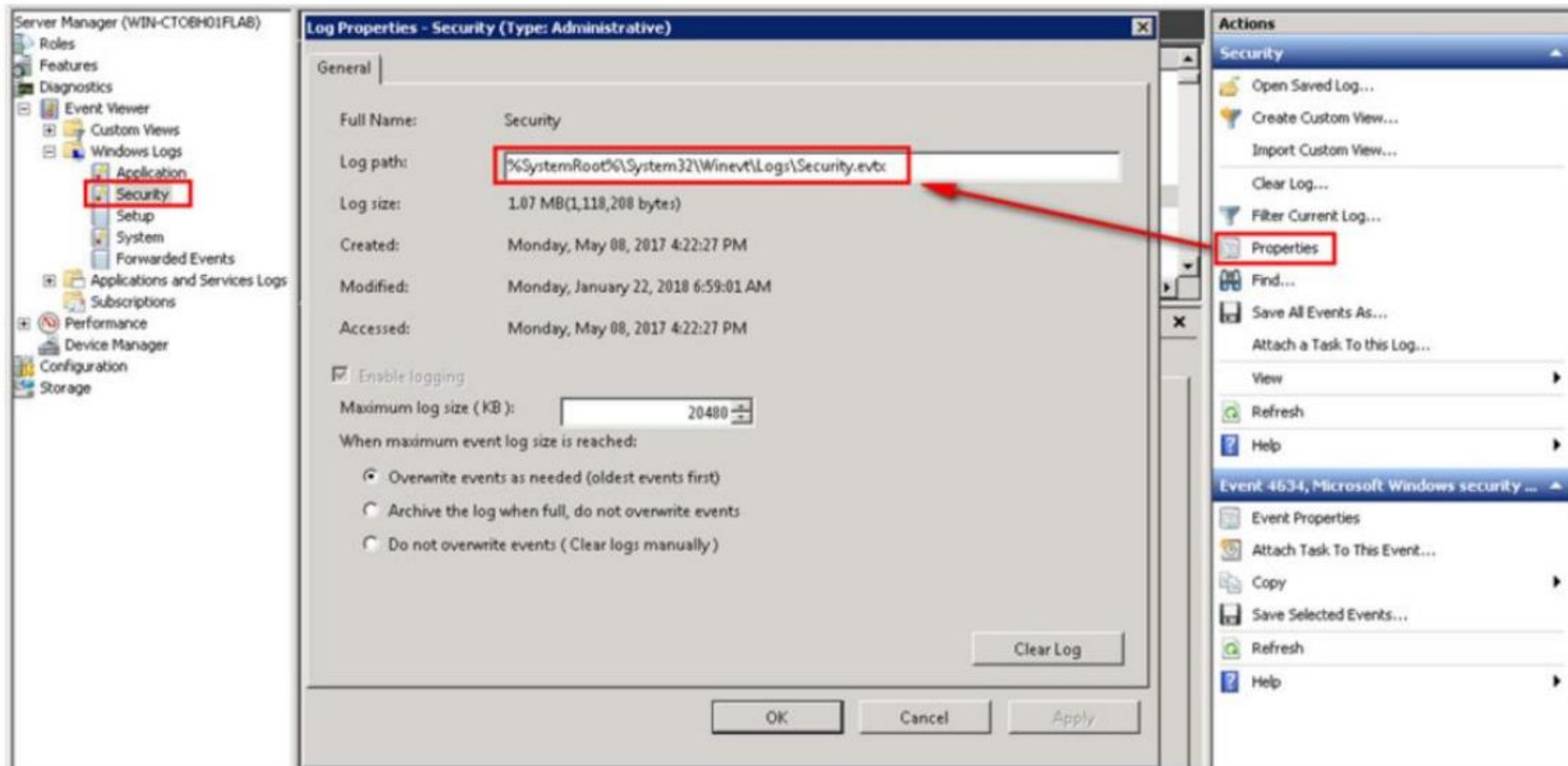
- ☐ System logs
- ☐ Application logs
- ☐ Security logs



- Windows log types:

Log Type	Function	Storage Location in Vista/Win7/Win8/Win10/ Server 2008/Server 2012
System log	Records events generated by operating system components, including the breakdown information and data of drivers, system components, and application software.	%SystemRoot%\System32\Winevt\Logs\System.evtx
Application log	Includes events (mainly about program running) recorded by application or system programs.	%SystemRoot%\System32\Winevt\Logs\Application.evtx
Security log	Records system security audit events, including login logs, object access logs, process tracing logs, privilege usage, account management, policy change, and system events.	%SystemRoot%\System32\Winevt\Logs\Security.evtx

- To check the location of security logs, choose Properties.



- Log and event types:

Type	Function
Information	An event of successful operation of an application, driver, or service
Warning	It is neither a direct nor major event, but will lead to potential issues. For example, if the disk space is insufficient or no printer is found, a "Warning" event is recorded.
Error	Error events refer to function unavailability and data loss. For example, if a service cannot be loaded as a system boot, an error event is generated.
Success audit	Successful security audit on access attempts. Success audit events mainly refer to security logs recording login/logout, object access, privilege use, account management, policy change, detailed tracking, directory service access, and other security events. For example, all successful system logins are recorded as success audit events.
Failure audit	Failed security audit on login attempts. For example, if a user attempts to access a network drive but fails, this attempt is recorded as a failure audit event.

- A Windows log consists of two parts: header field and description field.

The screenshot displays the Windows Event Viewer interface. The top pane shows a list of security events. The bottom pane provides a detailed view of Event 4634, which is a 'Logoff' event. The event is categorized as 'Special Logon' and 'Logoff'. The description field contains the text 'An account was logged off.' and details about the user 'Administrator'. The header field contains metadata such as 'Log Name: Security', 'Source: Microsoft Windows security', 'Event ID: 4634', 'Task Category: Logoff', 'Level: Information', 'Keywords: Audit Success', 'User: N/A', 'Computer: [redacted]', and 'OpCode: Info'. The event is dated 3/19/2018 10:00:37 AM.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	3/19/2018 10:16:00 AM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	3/19/2018 10:16:00 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	3/19/2018 1:16:37 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	3/19/2018 1:16:37 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	3/19/2018 10:07:08 AM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	3/19/2018 10:00:37 AM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	3/19/2018 9:58:51 AM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	3/19/2018 9:58:51 AM	Microsoft Windows security auditing.	4624	Logon
Audit Success	3/19/2018 9:58:51 AM	Microsoft Windows security auditing.	4648	Logon
Audit Success	3/19/2018 9:58:51 AM	Microsoft Windows security auditing.	4776	Credential Validation

Event 4634, Microsoft Windows security auditing.

General | Details

An account was logged off.

Subject:

Security ID: [redacted] Administrator

Account Name: Administrator

Account Domain: [redacted]

Logon ID: 8c2637d179

Logon Type: 18

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

Log Name: Security

Source: Microsoft Windows security

Event ID: 4634

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Task Category: Logoff

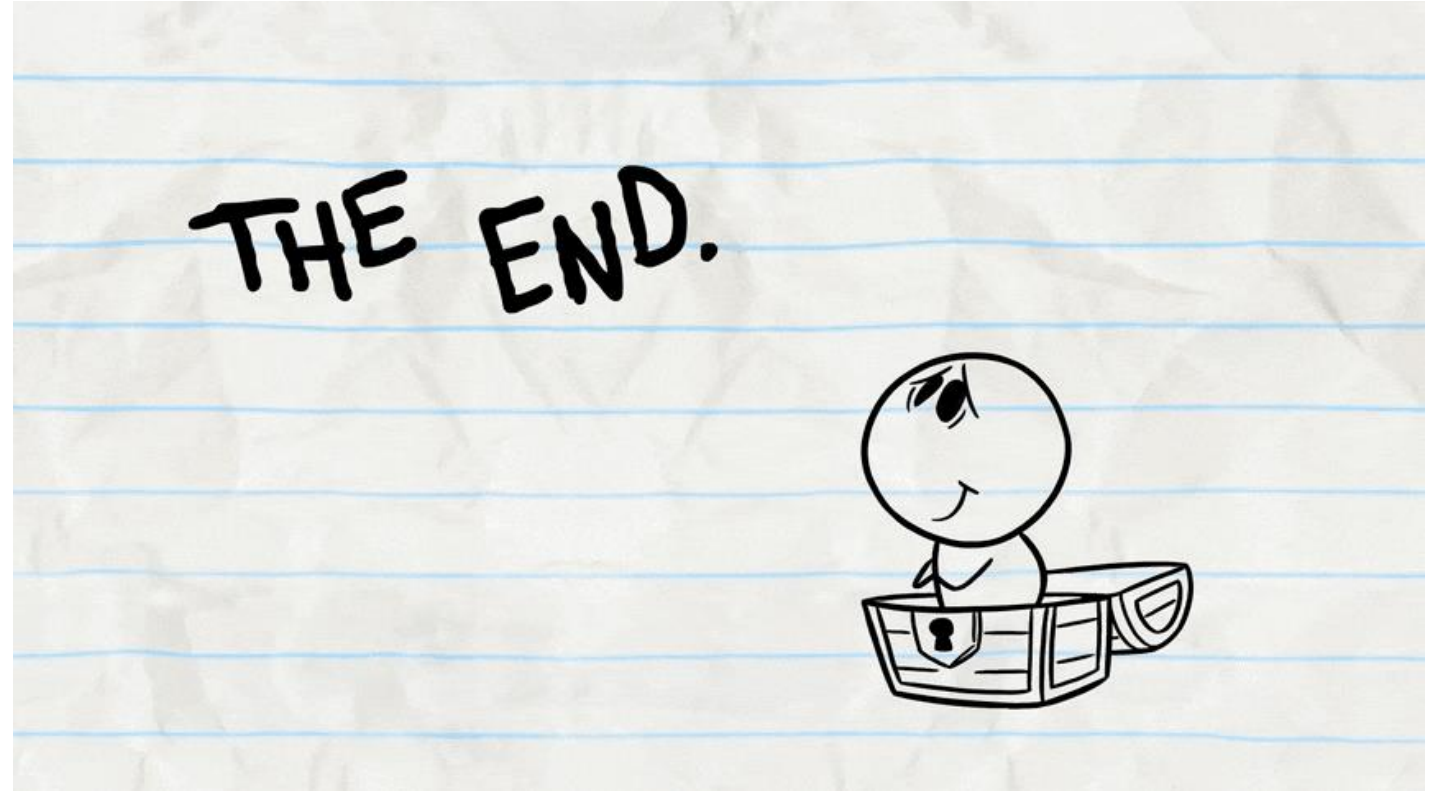
Keywords: Audit Success

Computer: [redacted]

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY