

CompTIA Security+ Exam SY0-701

Lesson 13



Analyze Indicators of Malicious Activity

Objectives

- Analyze indicators of malicious activity in malware, physical, network, and application attacks

Lesson 13

Topic 13A

Malware Attack Indicators

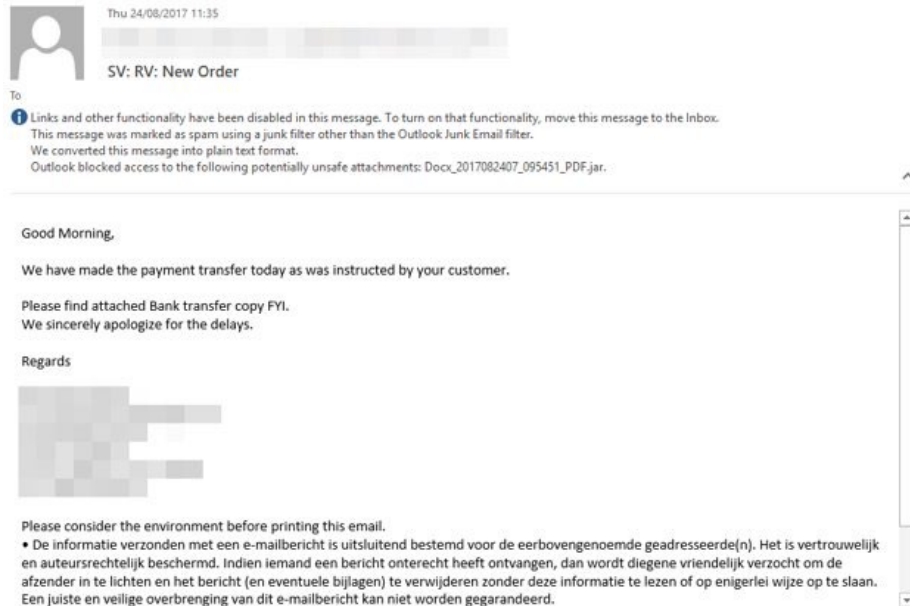
Malware Classification

- Classification by vector or infection method
- Viruses and worms
 - Spread within code without authorization
- Trojans
 - A malicious program concealed within a benign one
- Potentially unwanted programs/applications (PUPs/PUAs)
 - Pre-installed “bloatware” or installed alongside another app
 - Not completely concealed, but installation may be covert
 - Also called grayware
- Classification by payload



Computer Viruses

- Rely on some sort of host file or media delivery vector
 - Non-resident/file infector
 - Memory resident
 - Boot
 - Script/macro



Screenshot used with permission from Microsoft.

Computer Worms and Fileless Malware

- Early computer worms
 - Propagate in memory/over network links
 - Consume bandwidth and crash process
- Fileless malware
 - Exploiting remote execution and memory residence to deliver payloads
 - May run from an initial script or Trojan
 - Persistence via the registry
 - Use of shellcode to create backdoors and download additional tools
 - “Living off the land” exploitation of built-in scripting tools
- Advanced persistent threat (APT)/advanced volatile threat (AVT)/low observable characteristics (LOC)

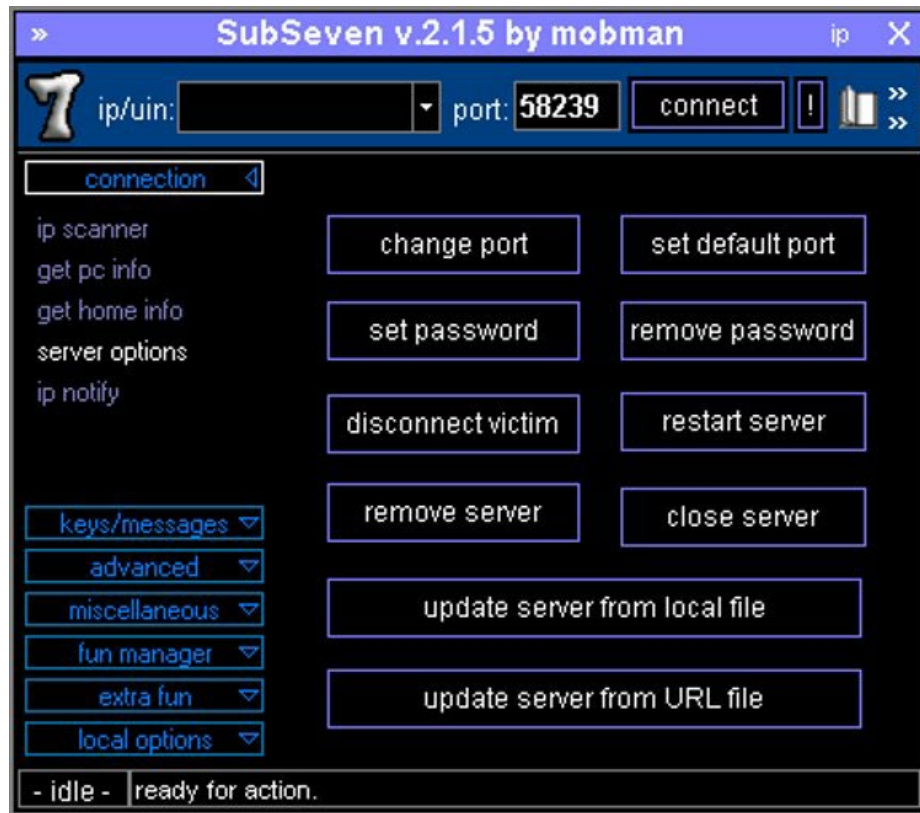
Spyware, Adware, and Keyloggers

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
https<Right Shift>://tickets.structureality.com/scp<CR>
jaime<Tab><Right Shift>Pa<Right Shift>$$w0rd
meterpreter > 
```

- Tracking cookies, supercookies, and beacons
- Adware (PUP/bloatware)
 - Changes to browser settings
- Spyware (malware)
 - Log all local activity
 - Use of recording devices and screenshots
 - Redirection
- Keylogger
 - Software and hardware

Backdoors and Remote Access Trojans

- Backdoor malware
- Remote access trojan (RAT)
- Bots and botnets
- Command & control (C2 or C&C)
- Backdoors from misconfiguration and unauthorized software



Screenshot used with permission from
Wikimedia Commons by CCAS4.0
International.

Rootkits

- Local administrator versus SYSTEM/root privileges
- Replace key system files and utilities
- Purge log files
- Firmware rootkits

Ransomware, Crypto-Malware, and Logic Bombs

- Ransomware
 - Nuisance (lock out user by replacing shell)
- Crypto-malware
 - High impact ransomware (encrypt data files or drives)
- Cryptomining/crypojacking
 - Hijack resources to mine cryptocurrency
- Logic bombs

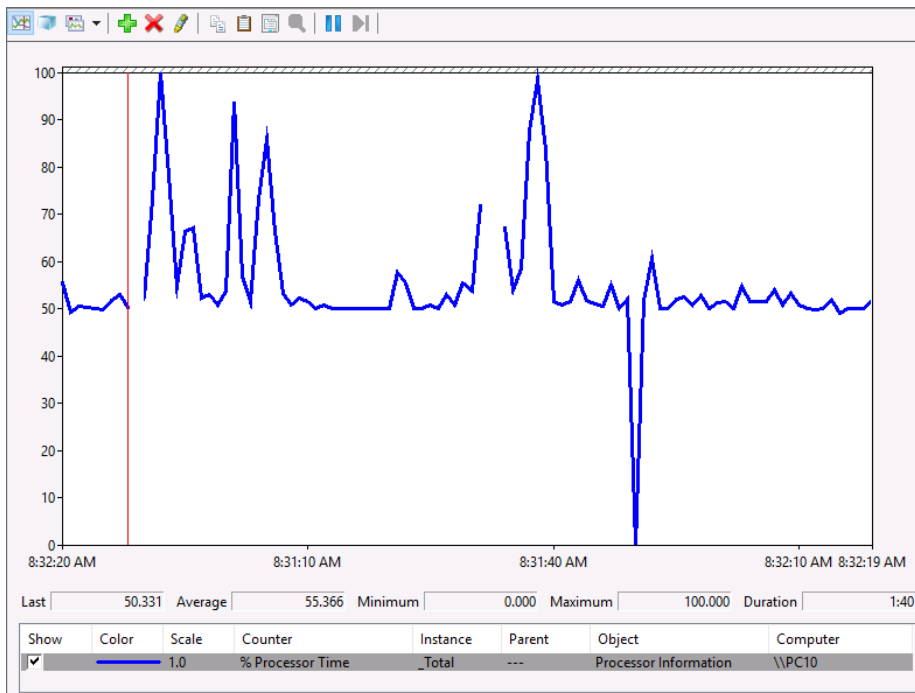


Image by Wikimedia Commons.

TTPs and IoCs

- Signature detection by anti-virus often ineffective
- Tactics, Techniques, and Procedures (TTPs)
- Indicators of Compromise (IoCs)
- Documented and published TTPs and IoCs
 - MITRE ATT&CK
 - Pattern-matching via artificial intelligence (AI) systems

Malicious Activity Indicators



Windows Performance Monitor recording CPU utilization on a client PC. Anomalous activity is difficult to diagnose, but this graph shows load rarely dropping below 50%. Continual load is not typical of a client system, and could be an indicator of cryptojacking malware. (Screenshot used with permission from Microsoft.)

- Browser changes or overt ransomware notification
- Sandbox execution
- Resource consumption
- File system
 - Blocked content
- Resource inaccessibility
- Account compromise
- Logging
 - Missing and out-of-cycle logging

Review Activity: Malware Attack Indicators

- Malware classification
 - Vector versus payload
- Computer viruses
- Computer worms and fileless malware
- Spyware, adware, and keyloggers
- Backdoors and remote access trojans
- Rootkits
- Ransomware, crypto-malware, and logic bombs
- TTPs and IOCs
- Malicious activity indicators
 - Resource consumption, file system, resource inaccessibility, account compromise, logging

Lesson 13

Topic 13B

Physical and Network Attack Indicators

Physical Attacks

- Brute force
 - Physical denial of service
 - Breaking into premises/cabinets
- Environmental
- RFID cloning and skimming
 - Radio Frequency Identification (RFID) and Nearfield Communications (NFC)
 - Contactless cards, badges, and fobs
 - Static tokens versus cryptoprocessors

Network Attacks

- Reconnaissance and credential harvesting
- Denial of service
- Weaponization/delivery/breach
- Command and control (C2 or C&C), beaconing, and persistence
- Lateral movement, pivoting, and privilege escalation
- Data exfiltration

Distributed Denial of Service Attacks (1)

- Leverage bandwidth from compromised hosts/networks
 - Handlers form a command and control (C&C) network
 - Compromised hosts installed with bots that can run automated scripts
 - Co-ordinated by the C&C network as a botnet
- Overwhelm with superior bandwidth (number of bots)
- Consume resources with spoof session requests (SYN flood)

Distributed Denial of Service Attacks (2)

- Reflected attacks
 - Spoof victim's IP address and attempt to open connections with multiple servers
 - Those servers direct their SYN/ACK responses to the victim
- Amplified attacks
 - Bogus DNS/NTP queries
 - Direct responses at victim
 - Queries can be constructed to generate large response packets
- DDoS indicators

The screenshot displays the Security Onion IDS interface. At the top, there are tabs for 'EVENTS', 'SUMMARY', and 'VIEWS'. Below these, a search bar and filters are visible. The main content area shows a table of 'TOP SIGNATURES' with 401 events. The table has columns for COUNT, %TOTAL, #SRC, #DST, SIGNATURE, and ID. The first row shows 82 events, 20.45% total, 82 sources, and 1 destination, with the signature 'ET DROP Spamhaus DROP Listed Traffic Inbound group 6'. Below this, there are sections for 'TOP SOURCE IPS' (viewing 10 of 314 results) and 'TOP DESTINATION IPS' (viewing 2 of 2 results). The 'TOP SOURCE IPS' table shows the top source IP is 192.168.2.192 from RFC1918. The 'TOP DESTINATION IPS' table shows the top destination IP is 10.1.0.10 from RFC1918.

COUNT	%TOTAL	#SRC	#DST	SIGNATURE	ID
82	20.45%	82	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 6	2400005
58	14.46%	1	1	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	2009358
35	8.73%	35	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 5	2400004
32	7.98%	32	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 7	2400006
31	7.73%	31	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 10	2400009
30	7.48%	30	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 9	2400008
21	5.24%	21	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 8	2400007
19	4.74%	19	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 26	2400025
18	4.49%	18	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 11	2400010
12	2.99%	12	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 12	2400011

COUNT	%TOTAL	#SIG	#DST	IP	COUNTRY
84	20.95%	16	1	192.168.2.192	RFC1918 (ko)
5	1.25%	3	1	10.1.0.10	RFC1918 (ko)
1	0.25%	1	1	114.8.151.185	- (-)
1	0.25%	1	1	139.47.144.204	- (-)
1	0.25%	1	1	114.8.55.8	- (-)
1	0.25%	1	1	143.135.246.239	- (-)
1	0.25%	1	1	116.129.134.220	- (-)

COUNT	%TOTAL	#SIG	#SRC	IP	COUNTRY
396	98.75%	39	313	10.1.0.10	RFC1918 (ko)
5	1.25%	3	1	192.168.2.192	RFC1918 (ko)

Dropping traffic from blocklisted IP ranges using Security Onion IDS. (Screenshot used with permission from Security Onion.)

On-path Attacks

- Threat actor positioned between two hosts
 - “Man-in-the-middle”
 - Can target forwarding/protocols at different network layers
- Address Resolution Protocol (ARP) poisoning
 - Broadcasting unsolicited ARP replies to poison the cache of local hosts with spoofed MAC address
 - Attacker usually tries to masquerade as default gateway

No.	Time	Source	Destination	Protocol	Length	Info
6	10.022521400	Microsof_01:ca:4a	Microsof_01:ca:76	ARP	42	10.1.0.102 is at 00:15:5d:01:ca:76
7	10.032593900	Microsof_01:ca:4a	Microsof_01:ca:76	ARP	42	10.1.0.2 is at 00:15:5d:01:ca:76
8	10.032605300	Microsof_01:ca:4a	Microsof_01:ca:76	ARP	42	10.1.0.101 is at 00:15:5d:01:ca:76
9	18.219200600	10.1.0.101	10.1.0.2	TCP	66	1702 → 80 [SYN] Seq=0 win=65535
10	18.220473400	10.1.0.101	10.1.0.2	TCP	66	[TCP Out-Of-Order] 1702 → 80
11	18.223616200	10.1.0.2	10.1.0.101	TCP	66	80 → 1702 [SYN, ACK] Seq=0 Ack=1702
12	18.228456800	10.1.0.2	10.1.0.101	TCP	66	[TCP Retransmission] 80 → 1702
13	18.228797700	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=1 Ack=1702
14	18.229264100	10.1.0.101	10.1.0.2	HTTP	433	GET / HTTP/1.1
15	18.238162600	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=1 Ack=1702
16	18.238250400	10.1.0.101	10.1.0.2	TCP	433	[TCP Retransmission] 1702 → 80
17	18.239342200	10.1.0.2	10.1.0.101	HTTP	412	HTTP/1.1 302 Redirect (text/css)
18	18.244530700	10.1.0.2	10.1.0.101	TCP	412	[TCP Retransmission] 80 → 1702
19	18.245021200	10.1.0.101	10.1.0.2	TCP	54	1702 → 80 [ACK] Seq=380 Ack=1702
20	18.252481800	10.1.0.101	10.1.0.2	TCP	54	[TCP Dup ACK 19#1] 1702 → 80
21	18.255190400	10.1.0.101	10.1.0.2	TCP	66	1703 → 443 [SYN] Seq=0 win=65535
22	18.260503200	10.1.0.101	10.1.0.2	TCP	66	[TCP Retransmission] 1703 → 443
23	18.261065300	10.1.0.2	10.1.0.101	TCP	66	443 → 1703 [SYN, ACK] Seq=0 Ack=1703
24	18.268454300	10.1.0.2	10.1.0.101	TCP	66	[TCP Retransmission] 443 → 1703

Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Microsof_01:ca:4a:77 (00:15:5d:01:ca:77), Dst: Microsof_01:ca:4a (00:15:5d:01:ca:4a)
Destination: Microsof_01:ca:4a (00:15:5d:01:ca:4a)
Source: Microsof_01:ca:77 (00:15:5d:01:ca:77)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.1.0.101, Dst: 10.1.0.2
Transmission Control Protocol, Src Port: 1702, Dst Port: 80, Seq: 0, Len: 0

0000 00 15 5d 01 ca 4a 00 15 5d 01 ca 77 08 00 45 00 ...w..E.
0010 00 34 1c ca 40 00 80 06 c9 91 0a 01 00 65 0a 01 .4...@.....e..
0020 00 02 06 a6 00 50 dc 52 ee 41 00 00 00 00 80 02P.R.A.....
0030 ff ff 89 1d 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02 ..

Destination Hardware Address (eth.dst), 6 bytes Packets: 286 · Displayed: 286 (100.0%) Profile: Default

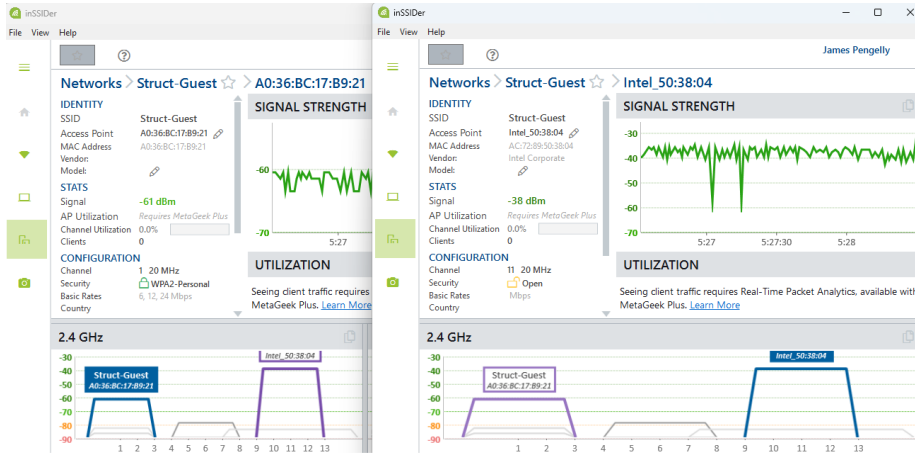
Screenshot used with permission from wireshark.org.

Domain Name System Attacks

- Attacks on public DNS services
 - Typosquatting, DRDoS, and hijacking
- DNS poisoning
- DNS-based on-path attacks
 - Get client to use malicious resolver
- DNS client cache poisoning
 - HOSTS file
- DNS server cache poisoning
- DNS attack indicators

Wireless Attacks

- Rogue access points
 - Non-malicious backdoors
 - Evil twins masquerade as legitimate AP
 - Launch on-path attacks
 - Indicators and detection
- Wireless denial of service
 - Jamming and disassociation
- Wireless replay and key recovery



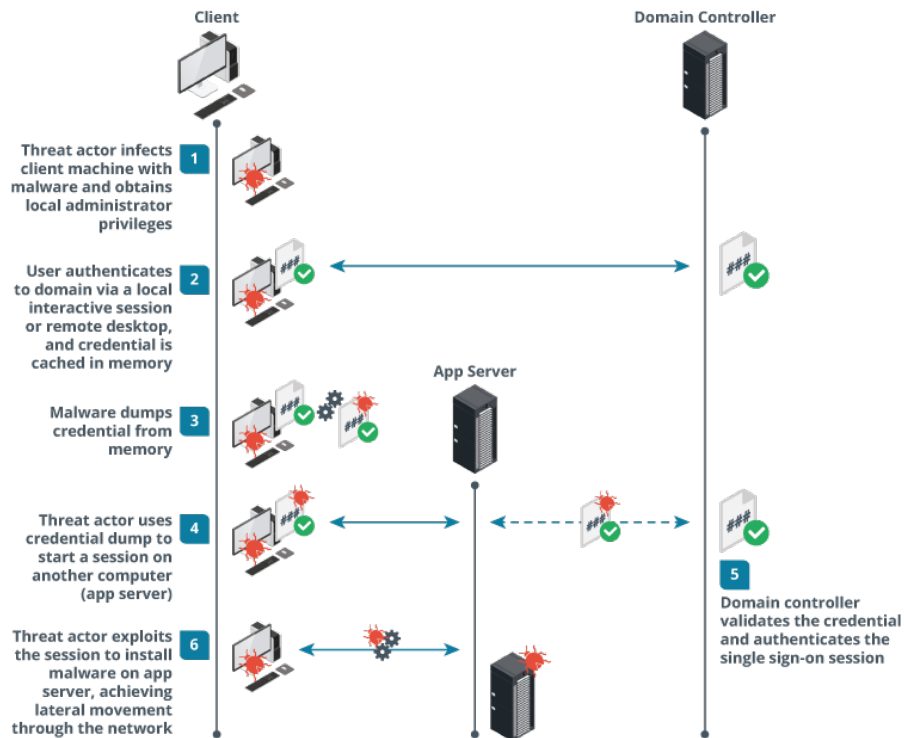
Screenshot used with permission from MetaGeek.

Password Attacks

- Online password attack
 - Adversary interacts with authentication service
- Offline attacks
 - Password database
 - Hash transmitted directly
 - Hash used as key to sign an HMAC
- Brute force attack
- Dictionary and hybrid attacks
- Password spraying

Credential Replay Attacks

- Credential dumping against Windows cached credentials
 - Kerberos tickets
 - NTLM hashes
 - Reversible encryption passwords
- Credential replay against hosts and applications
 - Pass the hash (PtH) against NTLM
 - Pass the ticket (PtT) against Kerberos



Cryptographic Attacks

- Downgrade attacks
 - Reduce transport encryption version/force use of weak cipher suites
 - Use weak cipher suites in Kerberos
- Collision attacks
 - Forge digital signatures
- Birthday attacks
 - Design more efficient collision attacks

Malicious Code Indicators

- Shellcode
- Credential dumping
- Lateral movement
 - Psexec
 - PowerShell code
- Persistence
 - Registry keys
 - Scheduled tasks

Review Activity: Physical and Network Attack Indicators

- Physical attacks
 - Brute force, environmental, card cloning
- Network attacks
 - Reconnaissance, weaponization, C&C, data exfiltration
- Distributed denial of service attacks
- On-path, Domain Name System, and wireless attacks
- Password and credential replay attacks
- Cryptographic attacks
- Malicious code indicators
 - Shellcode, credential dumping, lateral movement/pivoting, persistence

Lesson 13

Topic 13C

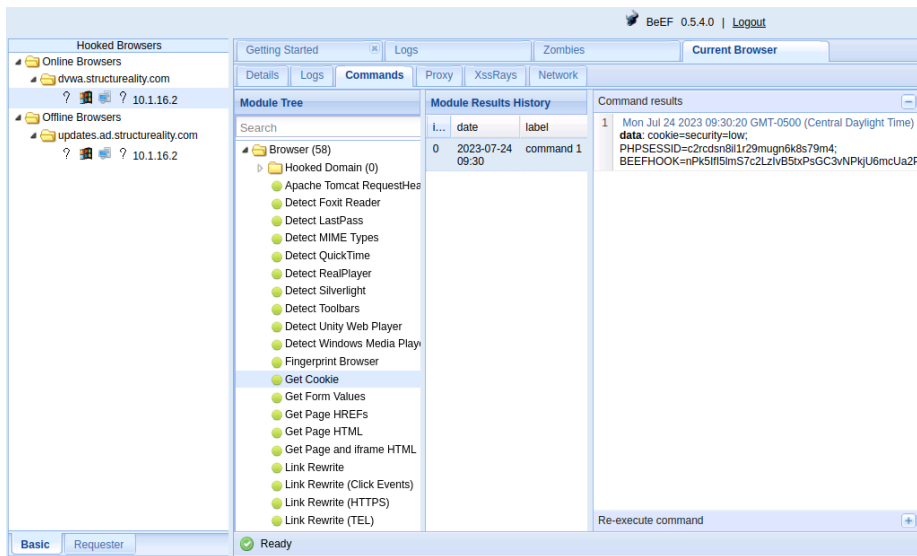
Application Attack Indicators

Application Attacks

- Attacks that target vulnerabilities in application code or architecture/design
- Privilege escalation
 - Get privileges from target vulnerable process to run arbitrary code
 - Remote execution when code is transferred from another machine
 - Vertical and horizontal privilege escalation
 - Detect by process logging and auditing plus automated detection scanning
- Buffer overflow

Replay Attacks

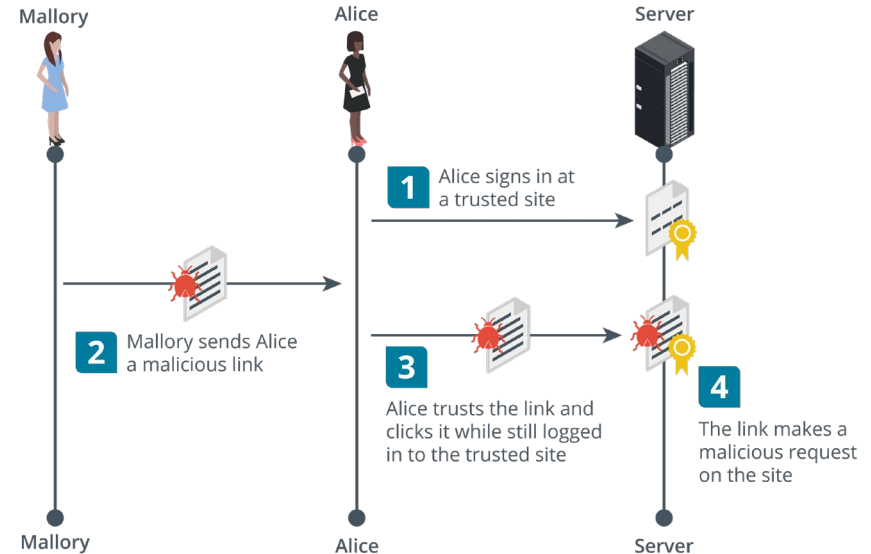
- Resubmitting or guessing authorization tokens
- Session management cookies
- Replay cookie to obtain authenticated session



Using The Browser Exploitation Framework (BeEF) to obtain the session cookie from a browser.

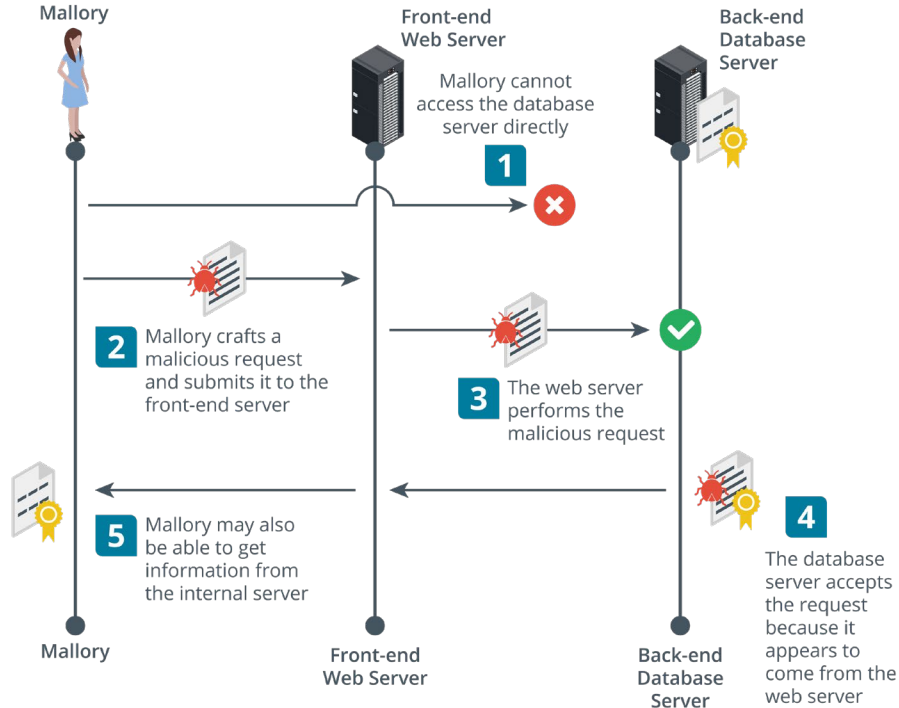
Forgery Attacks (1)

- Cookie hijacking and session prediction
- Client-side/cross-site (CSRF/XSRF) request forgery
 - Passes a URL to another site where the user has an authenticated session
 - Confused deputy



Images © 123rf.com.

Forgery Attacks (2)



- Server-side Request Forgery (SSRF)
- Cause a server to make API calls or HTTP requests with arbitrary parameters
 - Weak authentication/access control between internal services
 - Weak input validation and faults in request parsing

Injection Attacks

- Persistent XSS and SQL injection
- Extensible Markup Language (XML) injection
 - XML tagged documents
 - XML External Entity (XXE) to exfiltrate data and files
- Lightweight Directory Access Protocol (LDAP) injection
 - Query language to read and update network directories

```
SELECT * FROM tbl_user WHERE  
username = ' ' or 1=1--#
```

```
<?xml version="1.0" encoding="UTF-8"?>  
  
<!DOCTYPE foo [<!ELEMENT foo ANY  
><!ENTITY bar SYSTEM  
"file:///etc/config"> ]>  
  
<bar>&bar;</bar>
```

```
(&(username=Bob)(&))
```


Directory Traversal and Command Injection Attacks

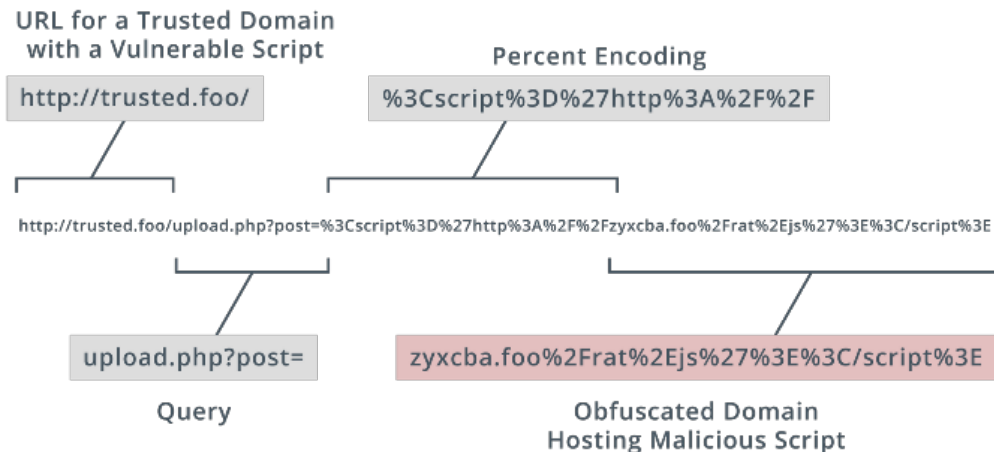
- Directory traversal
 - Obtain access to files outside web site root directory
 - Canonicalization attack and percent encoding
- Command injection
 - Cause server to run OS shell commands

http://victim.foo/?show=../../../../etc/config

http://victim.foo/?show=%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f
etc/config

URL Analysis

- Uniform Resource Locator (URL) format
- HTTP methods
 - TCP connections
 - GET, POST, PUT
 - URL (query parameters)
- Percent encoding



Web Server Logs

- Error log
- Traffic log
- Status codes
- HTTP headers

```
1 203.0.113.100 [10:52:38] "GET / HTTP/1.1" 200 1392 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
2 203.0.113.100 [10:52:38] "GET /images/icon-email.png HTTP/1.1" 200 747 "http://www.structureality.com/" "Mozilla/5.0..."
3 203.0.113.100 [10:52:38] "GET /images/icon-receiver.png HTTP/1.1" 200 1383 "http://www.structureality.com/" "Mozilla/5.0..."
4 203.0.113.100 [10:52:38] "GET /images/structureality-logo-banner.png HTTP/1.1" 200 151731 "http://www.structureality.com/" "Mozilla/5.0..."
5 203.0.113.100 [10:52:38] "GET /images/icon-post.png HTTP/1.1" 200 1021 "http://www.structureality.com/" "Mozilla/5.0..."
6 203.0.113.100 [10:52:38] "GET /favicon.ico HTTP/1.1" 200 1450 "http://www.structureality.com/" "Mozilla/5.0..."
7 203.0.113.66 [10:53:04] "GET / HTTP/1.1" 200 2965 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:Port Check)"
8 203.0.113.66 [10:53:05] "GET /cgi.cgi/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
9 203.0.113.66 [10:53:05] "GET /webcgi/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
10 203.0.113.66 [10:53:05] "GET /bin/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
11 203.0.113.66 [10:53:05] "GET /cgi/ HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi dir check)"
12 203.0.113.66 [10:53:05] "GET /robots.txt HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:robots)"
13 203.0.113.66 [10:53:05] "GET /crossdomain.xml HTTP/1.1" 404 494 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:crossdomain)"
14 203.0.113.66 [10:53:05] "GET / HTTP/1.1" 200 2964 "-" "Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:origin_reflection)"
```

Review Activity: Application Attack Indicators

- Application attacks
 - Arbitrary/remote code execution, privilege escalation, buffer overflow
- Replay attacks
- Forgery attacks
 - Cross-site and server-side forgery
- Injection attacks
 - SQL, XML, LDAP, directory traversal, command injection
- URL analysis
- Web server logs

CompTIA Security+ Exam SY0-701

Lesson 13



Summary