SEC+
Lesson 13:
Analyze Indicators of Malicious Activity

Objectives

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

Lesson 13

Topic 13A

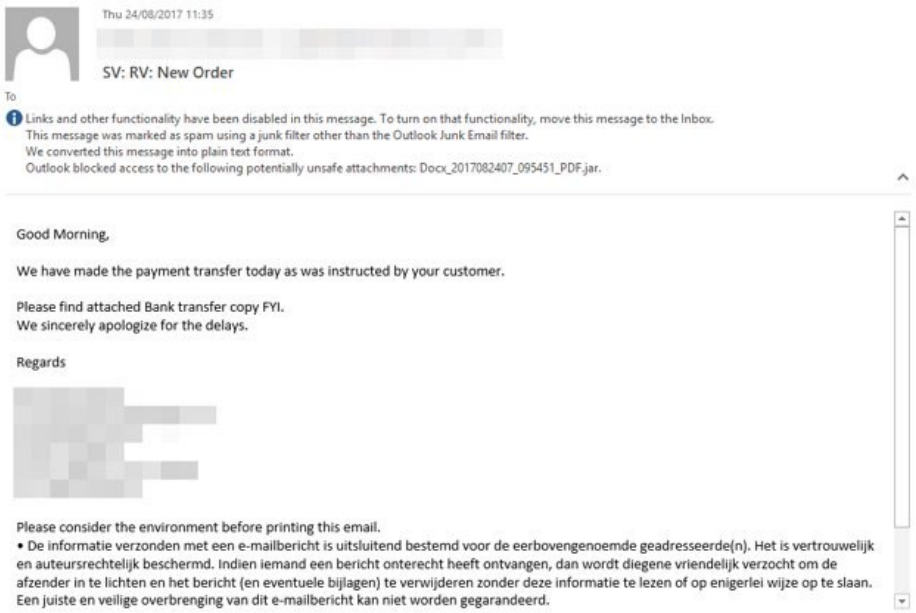
Malware Attack Indicators

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

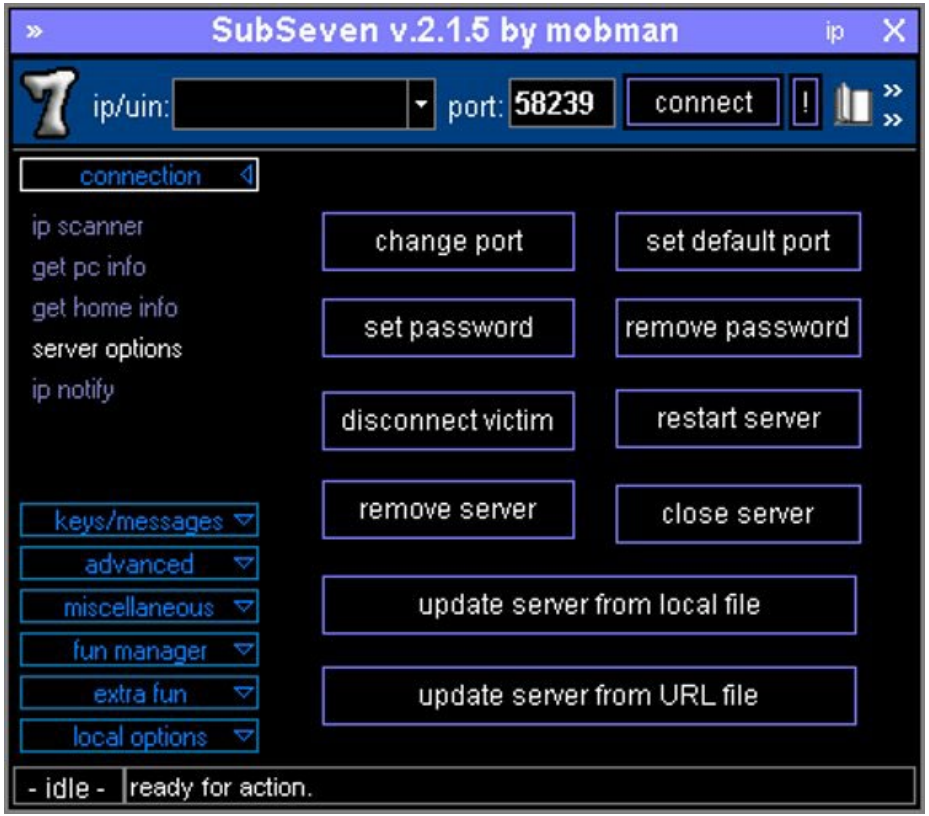
```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
https<Right Shift>://tickets.structureality.com/scp<CR>
jaime<Tab><Right Shift>Pa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



Rootkits

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

Ransomware, Crypto-Malware, and Logic Bombs

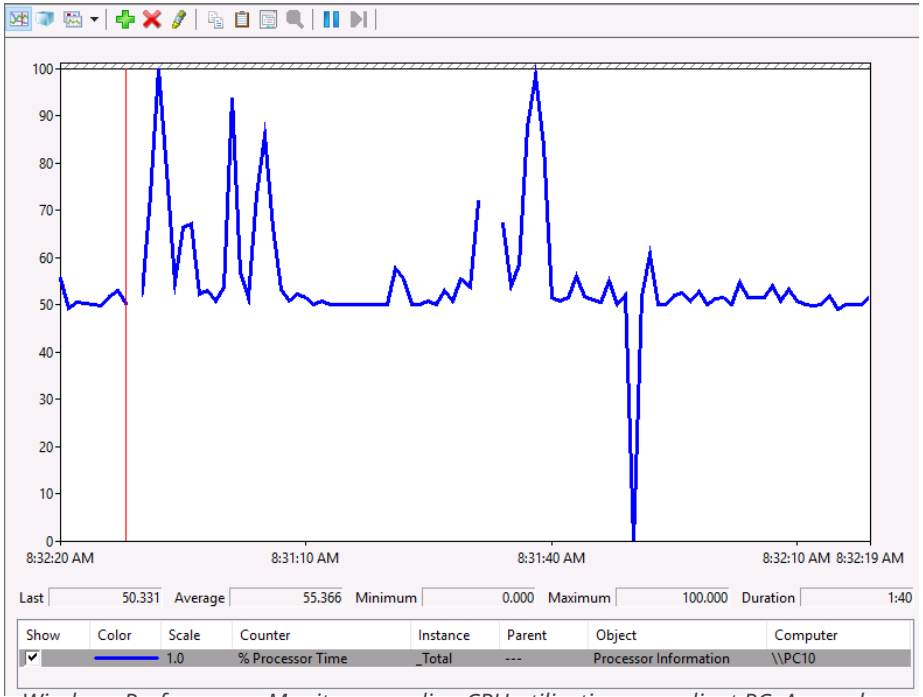
- Ransomware
  - Nuisance (lock out user by replacing shell)
- Crypto-malware
  - High impact ransomware (encrypt data files or drives)
- Cryptomining/crypojacking
  - Hijack resources to mine cryptocurrency
- Logic bombs

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

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

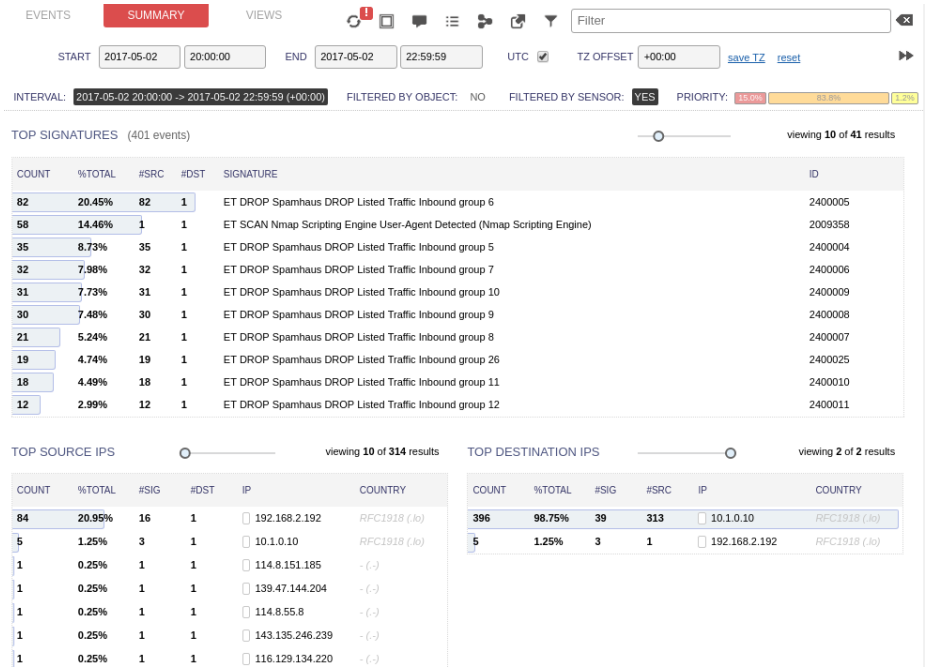
- Reconnaissance and credential harvesting
- Denial of service
- Weaponization/delivery/breach
- Command and control (C2 or C&C), beaconing, and persistence
- Lateral movement, pivoting, and privilege escalation
- Data exfiltration

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)

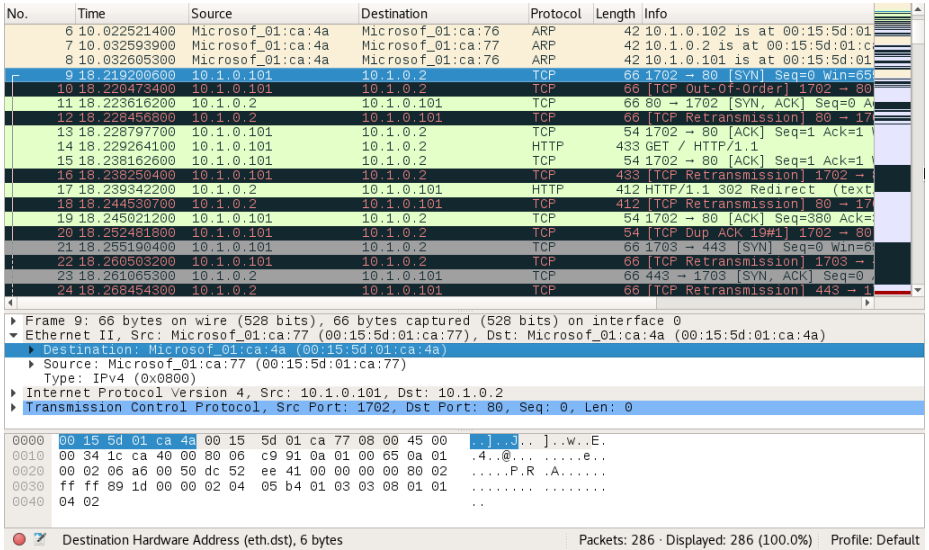
- Reflected attacks
  - Spoof victim's IP address and attempt to open connections with multiple servers
  - Those servers direct their SYN/ACK responses to the victim
- Amplified attacks
  - Bogus DNS/NTP queries
  - Direct responses at victim
  - Queries can be constructed to generate large response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



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

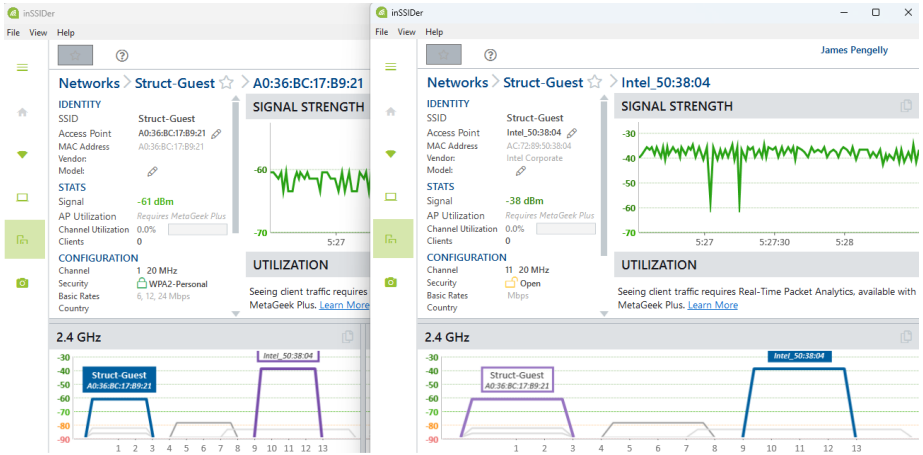


Screenshot used with permission from wireshark.org.

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



Screenshot used with permission from MetaGeek.

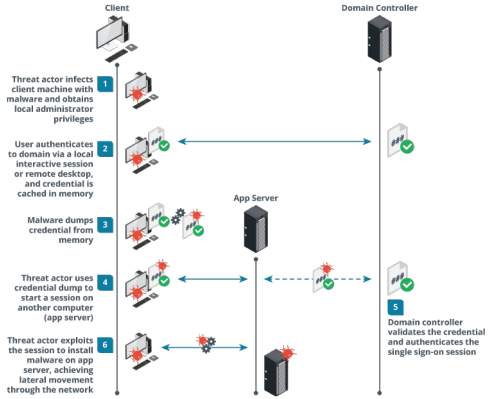
- Rogue access points
  - Non-malicious backdoors
  - Evil twins masquerade as legitimate AP
  - Launch on-path attacks
  - Indicators and detection
- Wireless denial of service
  - Jamming and disassociation
- Wireless replay and key recovery

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

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

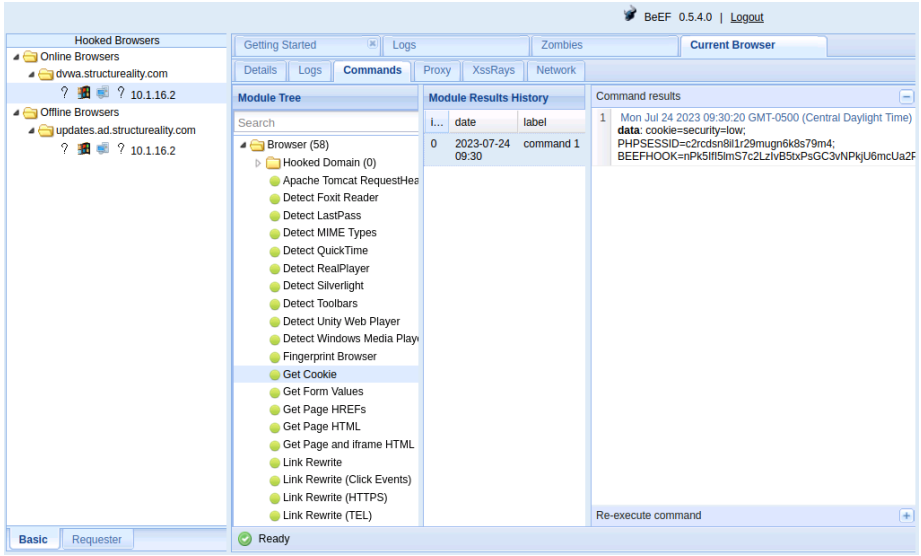
Topic 13C

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

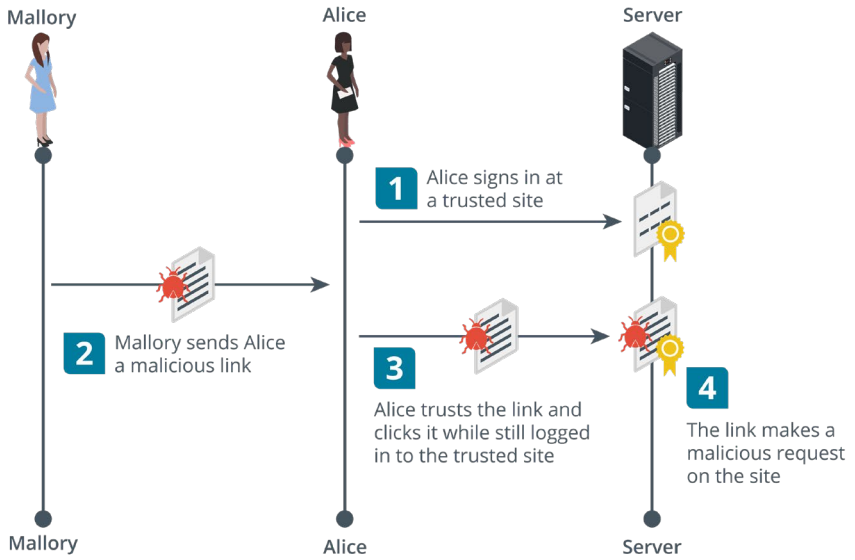


Using The Browser Exploitation Framework (BeEF) to obtain the session cookie from a browser.

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

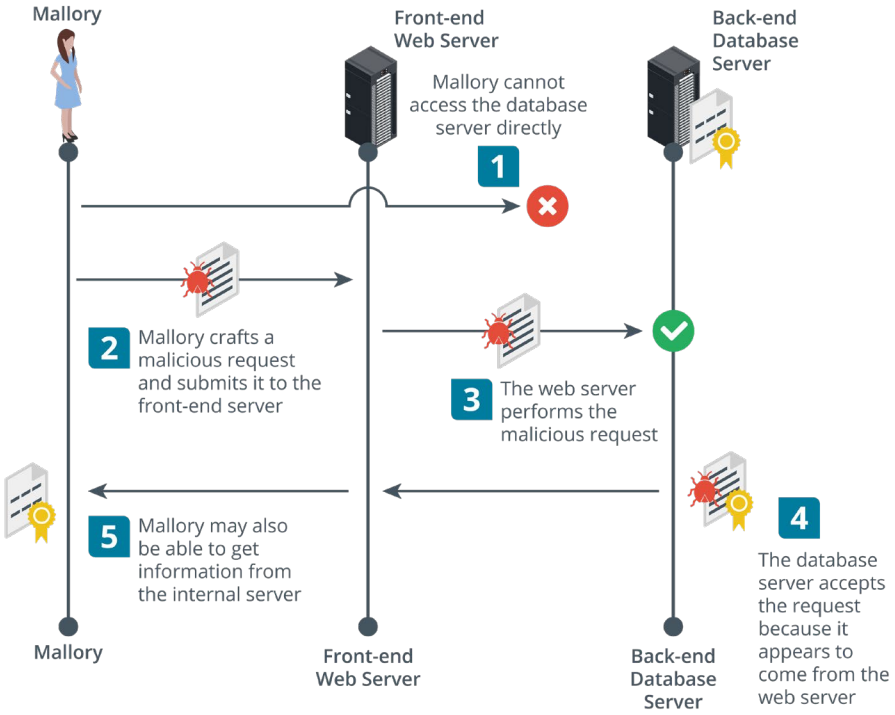
Forgery Attacks (1)

- 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

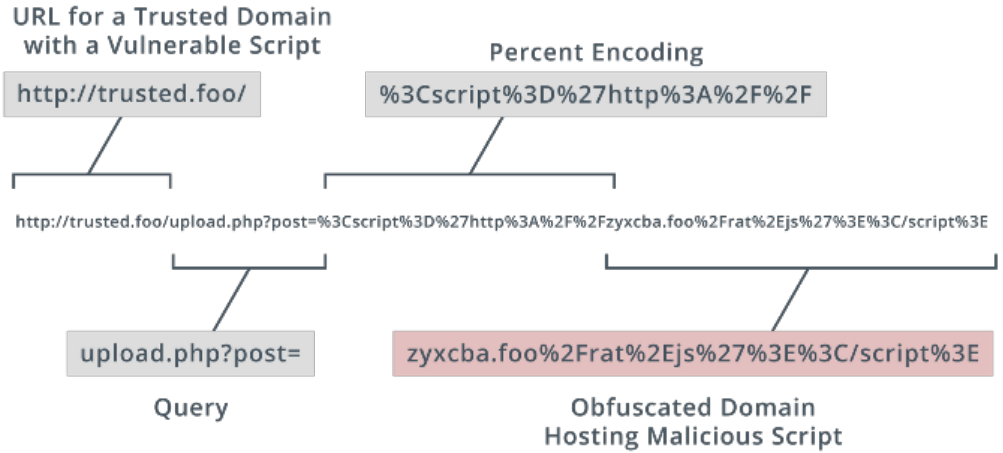
- Directory traversal
  - Obtain access to files outside web site root directory
  - Canonicalization attack and percent encoding
- Command injection
  - Cause server to run OS shell commands

```
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)"
```

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

Lesson 13

Summary