NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

Medical Device Attack Scenario

Sarah Jopp, BS, MBA, CISSP
Senior Analyst, Clinical Information Security – Resiliency
Mayo Clinic

Challenges to Securing Medical Devices

zero downtime 24/7

clinical workflow issues

“behind-the-perimeter-firewall” mentality

limitations on adding security software

FDA

(re-)approval takes long time

patient safety requires special handling

lack of Software Development Lifecycle

AV, anti-malware limitations

Common Types of Vulnerabilities

```
text:00AAB614 00 00 00 00                 nop
text:00AAB618 24 46 E0 18                 addiu   $a2, $v0, (aRemotessh - 0x5D0000)  # "remotessh"
text:00AAB61C 8F 99 98 C4                 la      $t9, param_set
text:00AAB620 00 00 00 00                 nop
text:00AAB624 03 20 F8 09                 jalr    $t9 ; param_set
text:00AAB628 00 00 00 00                 nop
text:00AAB62C 8F DC 00 10                 lw      $gp, 0x10($fp)
text:00AAB630 8F C4 00 18                 lw      $a0, 0x18($fp)
text:00AAB634 24 05 00 01                 li      $a1, 1
text:00AAB638 8F 82 80 A4                 la      $v0, aFfffIngress  # "ffff: ingress"
text:00AAB63C 00 00 00 00                 nop
text:00AAB640 24 46 E0 24                 addiu   $a2, $v0, (a5sap9i26 - 0x5D0000)  # "5SaP9I26"
text:00AAB644 8F 99 98 C4                 la      $t9, param_set
text:00AAB648 00 00 00 00                 nop
text:00AAB64C 03 20 F8 09                 jalr    $t9 ; param_set
text:00AAB650 00 00 00 00                 nop
text:00AAB654 8F DC 00 10                 lw      $gp, 0x10($fp)
text:00AAB658 8F C4 00 18                 lw      $a0, 0x18($fp)
text:00AAB65C 24 05 00 02                 li      $a1, 2
```

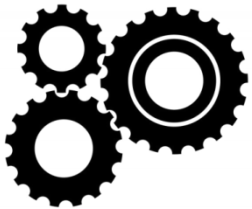
Hardcoded Credentials

no/weak/custom encryption

Default Passwords

Unsupported Operating System

Lack of Patch Management



Insecure configuration

Web app injections

Attack Chain

Series of vulnerabilities an attacker will exploit to gain complete access to a critical asset - starting from zero access (*not to be confused with the cyber kill chain*)

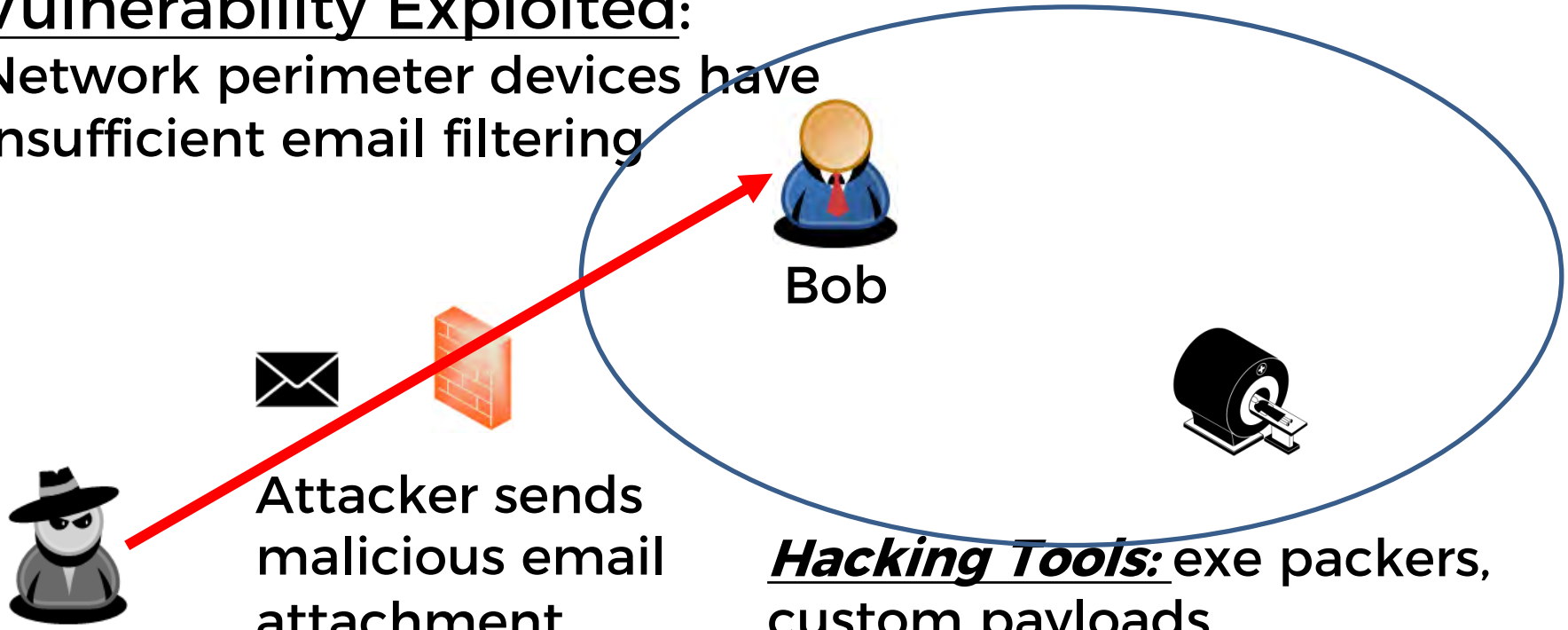
Example Scenario: *Gain Unauthorized Access to MRI scanner*

1. Gain access to intranet by exploiting *user ignorance* (phishing) and weak email filtering
2. Install and maintain backdoor access to victim's system by exploiting *weak perimeter and endpoint security*
3. Pivot to medical device server by exploiting web application *default password*
4. Elevate privileges by exploiting *unpatched server OS*
5. Gain access to medical device by exploiting *trust between server and device*

Step 1: Gain access to intranet

Vulnerability Exploited:

Network perimeter devices have insufficient email filtering

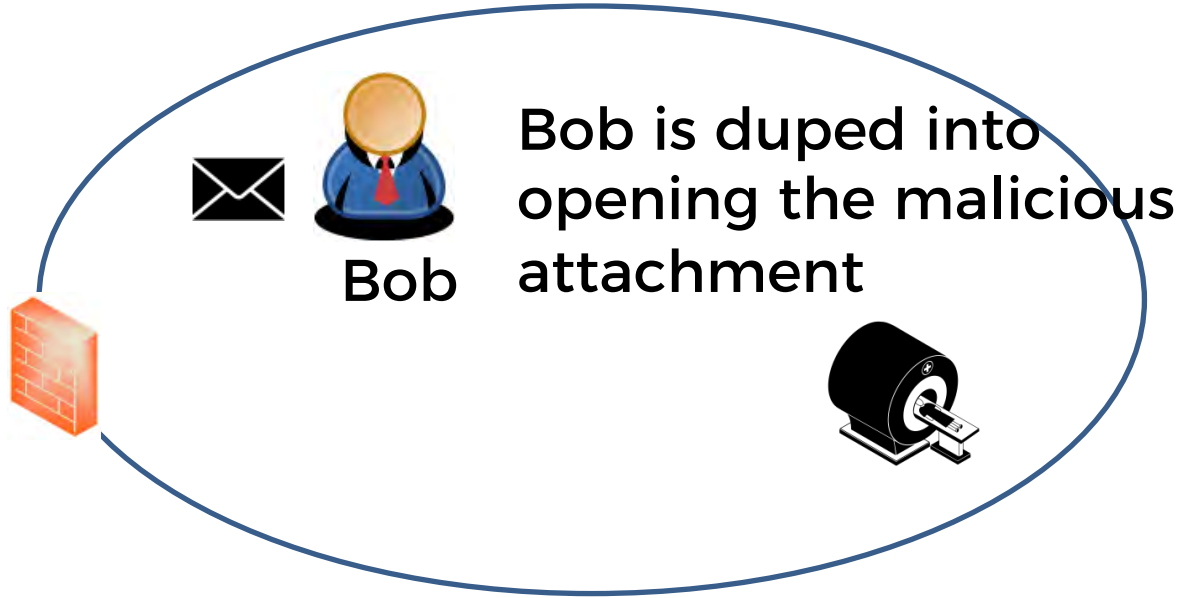


Attacker sends malicious email attachment

Hacking Tools: exe packers, custom payloads

Step 1: Gain access to intranet

Vulnerability Exploited:
User ignorance



Hacking Tools: social engineering, patience

Step 1: Gain access to intranet

Vulnerability Exploited:

Insufficient Endpoint Protection

Weak perimeter firewall / IDS

Bob

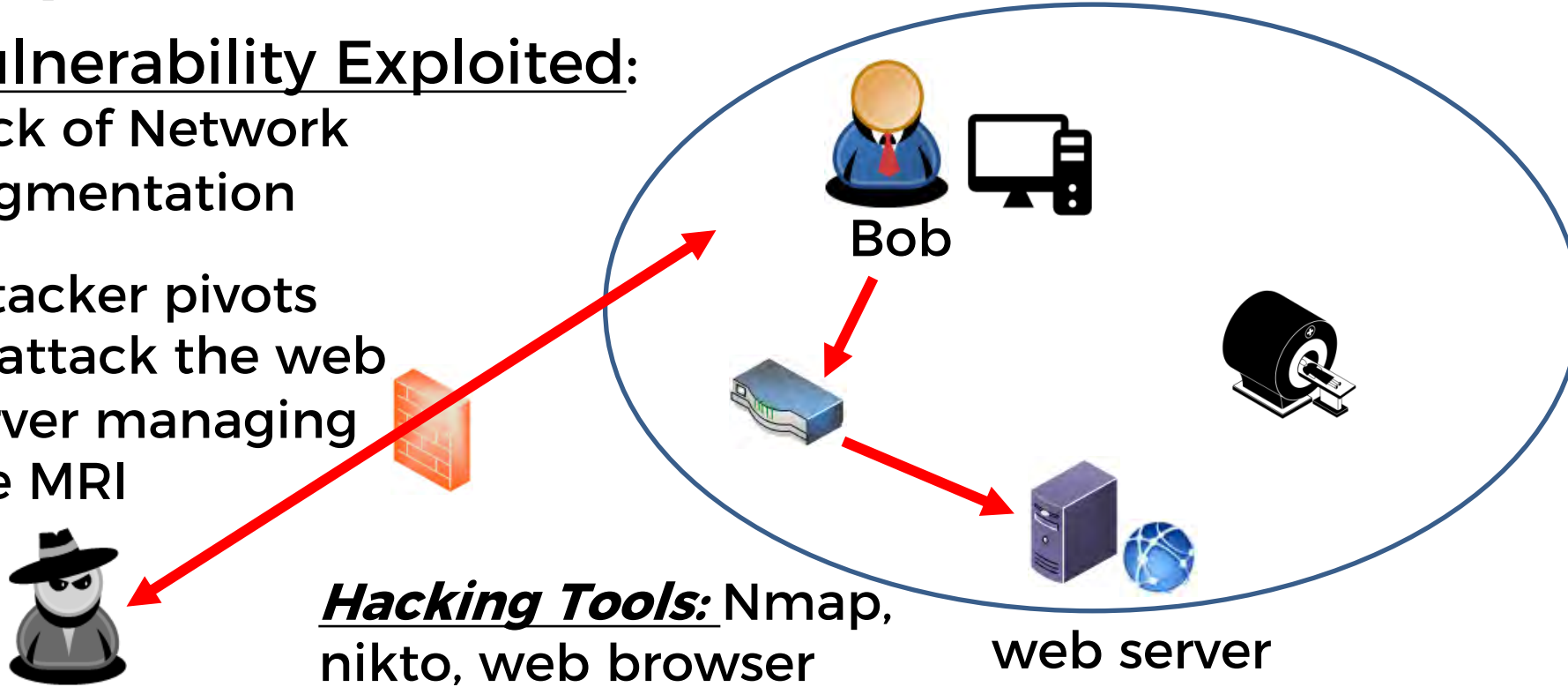
Attacker's malware is installed on Bob's machine and calls back to attacker's machine

Hacking Tools: reverse shell (msfvenom)

Step 2: Gain access to web server

Vulnerability Exploited:
Lack of Network Segmentation

Attacker pivots to attack the web server managing the MRI

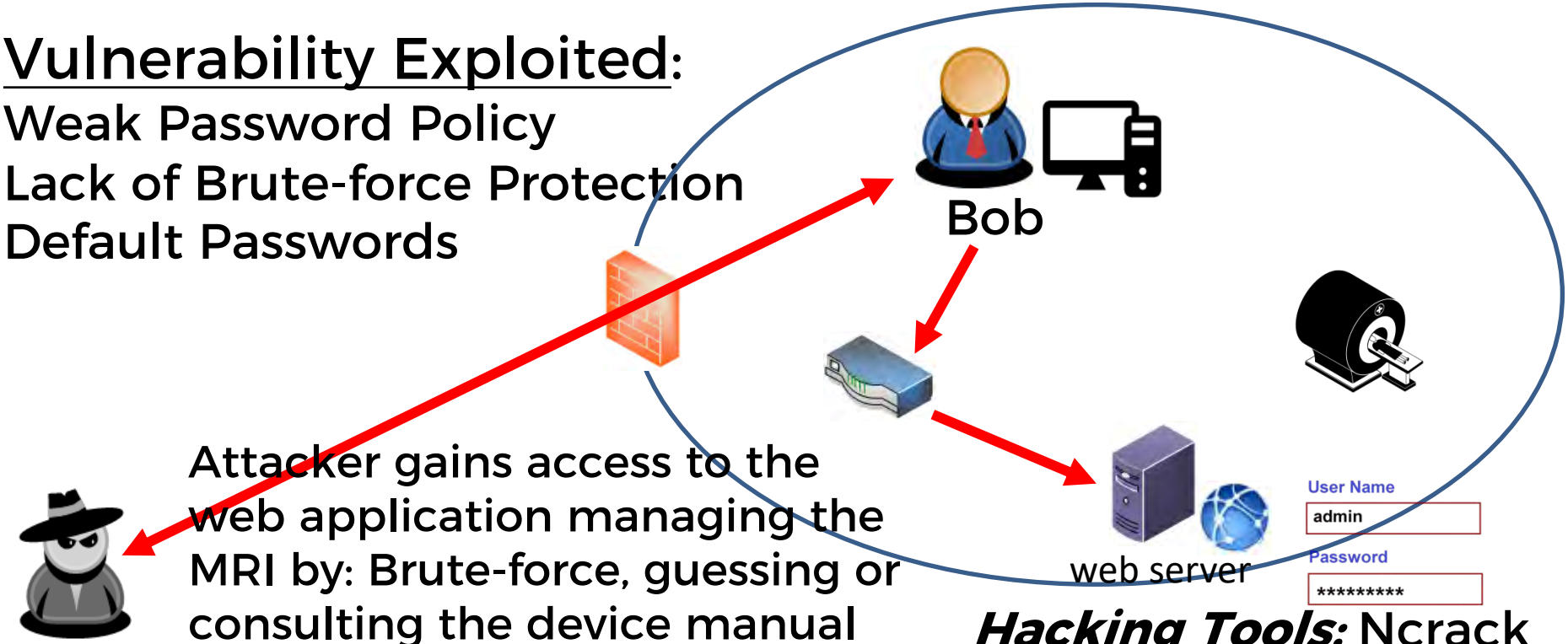


Hacking Tools: Nmap, nikto, web browser

Step 2: Gain access to web server

Vulnerability Exploited:

Weak Password Policy
Lack of Brute-force Protection
Default Passwords

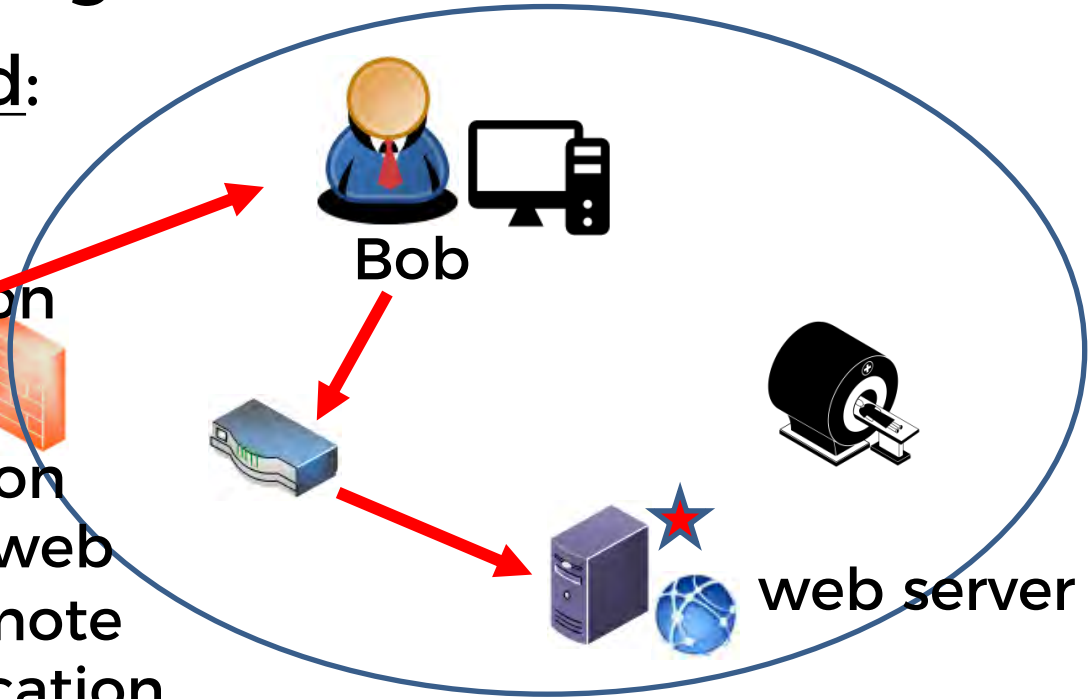


Attacker gains access to the web application managing the MRI by: Brute-force, guessing or consulting the device manual

Hacking Tools: Ncrack

Step 3: Elevate privileges on web server

<u>Vulnerability Exploited</u>:
Web server running with excessive privileges
Unpatched web application



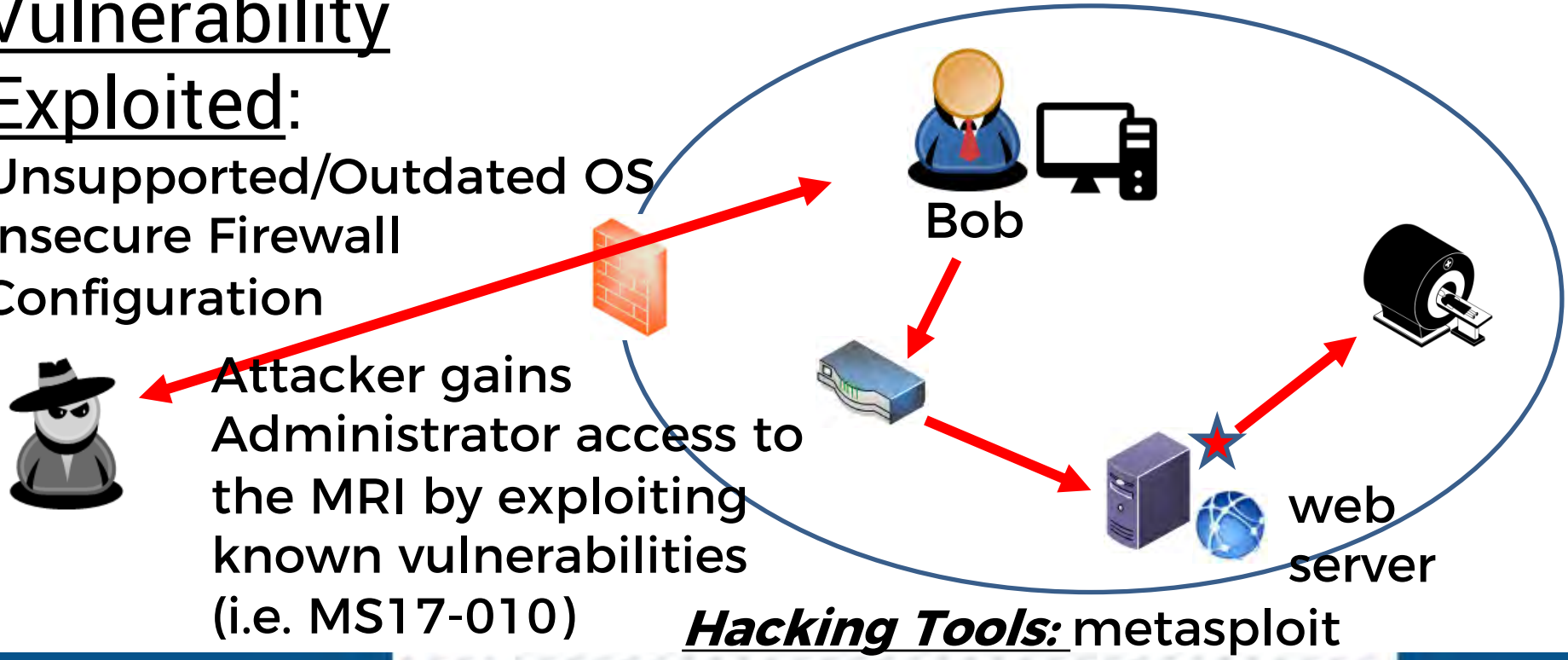
Attacker gains shell on server by exploiting web app and running remote code as a web application user (elevated privileges).

<u>Hacking Tools:</u> web browser, metasploit

Step 4: Gain access to MRI scanner

Vulnerability Exploited:

Unsupported/Outdated OS
Insecure Firewall Configuration



Attacker gains Administrator access to the MRI by exploiting known vulnerabilities (i.e. MS17-010)

Hacking Tools: metasploit

Testing Methods for Common Vulnerabilities

Hardcoded Credentials

Default Passwords

no/weak/ custom encryption

Unsupported OS

Lack of Patch Mgmt.

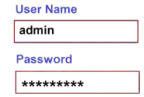
Insecure config.

Web app injections

Reverse engineering of binary executable files	✓		✓			
Assessment of cryptographic aspects of application			✓			
Analysis of custom protocols			✓			✓
Manual web application assessments		✓				

Testing Methods for Common Vulnerabilities

Hardcoded Credentials



Default Passwords

no/weak/ custom encryption

Unsupported OS

Lack of Patch Mgmt.

Insecure config.

Web app injections

Manual host Configuration reviews	✓		✓	✓	✓	
Interview vendor staff	✓		✓	✓		
Remote scan of services for vulnerabilities			✓	✓		

Questions