1 Intruders

2 Intruder Behavior Patterns
What is an Intruder?

A.K.A. - hacker or cracker (as opposed to a virus)

3 Classes

Masquerader - a person who exploits the system via a legitimate user account (an outsider)

Misfeasor - a legitimate user who access unauthorized data or uses the data in an unauthorized manner (an insider)

Clandestine user - an individual who seizes supervisory system control and evades auditing (either insider or outsider)
What is an Intruder?

A.K.A. - hacker or cracker (as opposed to a virus)
What is an Intruder?

A.K.A. - hacker or cracker (as opposed to a virus)

3 Classes

- **Masquerader** - a person who exploits the system via a legitimate user account (an outsider)
- **Misfeasor** - a legitimate user who access unauthorized data or uses the data in an unauthorized manner (an insider)
- **Clandestine user** - an individual who seizes supervisory system control and evades auditing (either insider or outsider)
Intruder Behavior Patterns

- Intruder behavior is constantly changing: different tasks to avoid detection, make use of new attack vectors
- Still, intruders do have certain basic behaviors that can be detected – behavior patterns
- Several Examples Follow:

Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
Intruder Behavior Patterns

- Intruder behavior is constantly changing: different tasks to avoid detection, make use of new attack vectors
- Still, intruders do have certain basic behaviors that can be detected – behavior patterns
- Several Examples Follow:

**Hacker**

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
Intruder Behavior Patterns

- Intruder behavior is constantly changing: different tasks to avoid detection, make use of new attack vectors
- Still, intruders do have certain basic behaviors that can be detected – behavior patterns
- Several Examples Follow:

**Hacker**

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. - pcAnywere)
Intruder Behavior Patterns

- Intruder behavior is constantly changing: different tasks to avoid detection, make use of new attack vectors
- Still, intruders do have certain basic behaviors that can be detected – behavior patterns
- Several Examples Follow:

### Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. pcAnywere)
4. Brute force passwords
Intruder Behavior Patterns

- Intruder behavior is constantly changing: different tasks to avoid detection, make use of new attack vectors
- Still, intruders do have certain basic behaviors that can be detected – behavior patterns
- Several Examples Follow:

<table>
<thead>
<tr>
<th>Hacker</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select the target using IP lookup tools such as NSLookup, Dig, and others</td>
</tr>
<tr>
<td>2</td>
<td>Map network for accessible services using tools such as NMAP</td>
</tr>
<tr>
<td>3</td>
<td>Identify potential vulnerable services (i.e. - pcAnywere)</td>
</tr>
<tr>
<td>4</td>
<td>Brute force passwords</td>
</tr>
<tr>
<td>5</td>
<td>Install remote administration tool (DameWare)</td>
</tr>
</tbody>
</table>
Intruder Behavior Patterns

- Intruder behavior is constantly changing: different tasks to avoid detection, make use of new attack vectors
- Still, intruders do have certain basic behaviors that can be detected – behavior patterns
- Several Examples Follow:

Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. - pcAnywhere)
4. Brute force passwords
5. Install remote administration tool (DameWare)
6. Wait for administrator to log on – capture that password
Intruder Behavior Patterns

- Intruder behavior is constantly changing: different tasks to avoid detection, make use of new attack vectors
- Still, intruders do have certain basic behaviors that can be detected – behavior patterns
- Several Examples Follow:

### Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. - pcAnywere)
4. Brute force passwords
5. Install remote administration tool (DameWare)
6. Wait for administrator to log on – capture that password
7. Use that password to access remainder of network
What motivates hackers? - Recognition
Hackers are often very open about sharing the vulnerabilities they found (bragging)
IDSs are designed to detect such attacks (IPSs designed to prevent, Chapter 9)
Select the target using IP lookup tools such as NSLookup, Dig, and others.
Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. - pcAnywere)
Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. - pcAnywhere)
4. Brute force passwords
Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potential vulnerable services (i.e. pcAnywere).
5. Install remote administration tool (DameWare).
1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. pcAnywere)
4. Brute force passwords
5. Install remote administration tool (DameWare)
6. Wait for administrator to log on – capture that password
Hacker

1. Select the target using IP lookup tools such as NSLookup, Dig, and others
2. Map network for accessible services using tools such as NMAP
3. Identify potential vulnerable services (i.e. - pcAnywere)
4. Brute force passwords
5. Install remote administration tool (DameWare)
6. Wait for administrator to log on – capture that password
7. Use that password to access remainder of network
Criminal Enterprise

Criminal “gangs” (loosely knit) of hackers who hack for monetary gain. Usually clandestine groups (can be in the employ of governments or corporations). Usually Eastern European, Russian or Southeast Asian. Meet in underground forums (DarkMarket.org or theftservices.com) Commonly target credit card files at e-commerce servers. Use card #s and post them to “carder” sites so others will use as well and obscure usage patterns

Usually have specific targets rather than targets of opportunity

IDSs and IPSs provide protection (but window is more narrow with swift attacks); Encryption should be an additional layer of security
Criminal Enterprise

1. Act quickly and precisely to make their activities hard to detect
Criminal Enterprise

1. Act quickly and precisely to make their activities hard to detect
2. Exploit perimeter through vulnerable ports
Criminal Enterprise

1. Act quickly and precisely to make their activities hard to detect
2. Exploit perimeter through vulnerable ports
3. Use Trojan horses (hidden software) to leave back doors
Criminal Enterprise

1. Act quickly and precisely to make their activities hard to detect
2. Exploit perimeter through vulnerable ports
3. Use Trojan horses (hidden software) to leave back doors
4. Use sniffers to capture passwords
Criminal Enterprise

1. Act quickly and precisely to make their activities hard to detect
2. Exploit perimeter through vulnerable ports
3. Use Trojan horses (hidden software) to leave back doors
4. Use sniffers to capture passwords
5. Leave quickly
Criminal Enterprise

1. Act quickly and precisely to make their activities hard to detect
2. Exploit perimeter through vulnerable ports
3. Use Trojan horses (hidden software) to leave back doors
4. Use sniffers to capture passwords
5. Leave quickly
6. Make few or no mistakes
Among the most difficult kinds of threats to manage (have certain privileges entrusted to them already)
IDSs and IPSs are useful, focus more on:

- Enforce least privilege; Make judicious use of logs
- Use strong authentication (Upon termination delete account immediately)
- Upon termination make a mirror image of employee’s HD before reissuing it.
Insider Threat

1. Create network accounts for themselves and their friends
Insider Threat

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn’t normally use for their jobs
Insider Threat

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn’t normally use for their jobs
3. E-mail employee lists
Insider Threat

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn’t normally use for their jobs
3. E-mail employee lists
4. Conduct furtive IM chats
Insider Threat

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn’t normally use for their jobs
3. E-mail employee lists
4. Conduct furtive IM chats
5. Visit websites that cater to disgruntled employees; f’dcountry.com
Insider Threat

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn’t normally use for their jobs
3. E-mail employee lists
4. Conduct furtive IM chats
5. Visit websites that cater to disgruntled employees; f’dcompany.com
6. Perform large downloads or file copies
Insider Threat

1. Create network accounts for themselves and their friends
2. Access accounts and applications they wouldn’t normally use for their jobs
3. E-mail employee lists
4. Conduct furtive IM chats
5. Visit websites that cater to disgruntles employees; f’dcompany.com
6. Perform large downloads or file copies
7. Access the network during off hours
Intrusion Objective: gain access to or increase privileges on a system
Intrusion Objective: gain access to or increase privileges on a system
Most initial attacks leverage software vulnerabilities to execute code that opens a back door
Intrusion Objective: gain access to or increase privileges on a system

Most initial attacks leverage software vulnerabilities to execute code that opens a back door

Example: buffer overflows on programs that run at a certain privilege level (drivers are key targets)
Intrusion Objective: gain access to or increase privileges on a system.
Most initial attacks leverage software vulnerabilities to execute code that opens a back door.
Example: buffer overflows on programs that run at a certain privilege level (drivers are key targets).
Intruder tries to access private information (password): with this knowledge it now becomes also like an insider threat.