Lecture Notes – "Think Like an Attacker: Introduction to MITRE ATT&CK"

1. Introduction: Thinking Like an Attacker

Cybersecurity relies on understanding not only defensive measures but also attacker psychology and methodology.
This lecture introduces key attacker behaviours, the MITRE ATT&CK framework, and a real-world case study involving Scattered Spider's 2025 ransomware attack on Marks & Spencer.

2. Information Warfare Landscape

Defenders

- Penetration Testing
- Vulnerability Management
- Cyber Threat Intelligence
- Detection & Monitoring
- Incident Response

Attackers

- Social Engineering
- Server Exploitation
- Web Application Attacks
- Malware Deployment
- Man-in-the-Middle Attacks

Grey Hat Hackers

- Individuals who break into systems without malicious intent but without permission
- Often claim to help by identifying vulnerabilities
- Still illegal and ethically problematic

3. TTPS – Tactics, Techniques, and Procedures

Tactics – The "Why"

The broader goals behind attacker actions.
Examples: gain access, escalate privileges, maintain persistence, exfiltrate data.

Techniques – The "How"

The methods used to achieve those goals.
Examples: phishing, credential dumping, exploiting vulnerabilities.

Procedures – The "What exactly they did"

Specific sequences or implementations of techniques during an attack.

4. The Attack Lifecycle (Based on MITRE Phases)

1. **Reconnaissance** – Researching the target
2. **Initial Access** – Gaining a foothold
3. **Execution** – Running malicious code
4. **Persistence** – Maintaining access over time
5. **Privilege Escalation** – Increasing permissions
6. **Defence Evasion** – Avoiding detection
7. **Credential Access** – Obtaining login credentials
8. **Discovery** – Mapping internal systems
9. **Lateral Movement** – Expanding control to more systems
10. **Command and Control** – Communicating with attacker servers
11. **Exfiltration** – Stealing data
12. **Impact** – Disruption, encryption, deletion

5. MITRE ATT&CK Framework Overview

- A globally used knowledge base cataloguing attacker behaviour
- Helps in threat modelling, detection engineering, and incident response
- Organised around Tactics (goals) and Techniques (methods)
- Widely used by security teams to map incidents to known threat actors

6. Case Study: Marks & Spencer (M&S) Ransomware Attack – 2025

Background

- **Timeline:** Feb – July 2025
- **Threat Actor:** Scattered Spider (UNC3944 / Octo Tempest / 0ktapus)
- **Ransomware:** DragonForce encryptor
- **Initial Vector:** Third-party compromise of Tata Consultancy Services' IT helpdesk
- **Impact:**
    - £300–500 million financial loss
    - 46-day online sales suspension
    - Customer data breach
    - Hiring freeze and severe operational disruption

7. Phase 1 – Initial Access, Reconnaissance & Escalation

Initial Access Tactic

- Phishing, smishing, and callback phishing targeting IT help desk staff
- Attackers impersonated IT specialists to acquire credentials

Reconnaissance

- Researched third-party vendors
- Identified privileged accounts and admin groups

Discovery

- Searched internal systems (SharePoint, network drives, wikis)
- Identified “vSphere Admins” Active Directory group

Privilege Escalation

- Added compromised accounts to VMware admins group
- Exploited ESXi vulnerabilities to gain advanced privileges

8. Phase 2 – Lateral Movement, Persistence & Exfiltration

Persistence

- Gained root access on VMware vCenter
- Enabled SSH through a root shell
- Installed remote access tools to maintain long-term entry

Lateral Movement

- Used remote console and reverse shells to navigate hypervisor infrastructure
- Hypervisor-level access bypassed many endpoint detection tools

Exfiltration

- Stole large volumes of sensitive data
- Exfiltrated data to several external sites, including data centers

9. Phase 3 – Backup Sabotage & Ransomware Deployment

Technique: Inhibit System Recovery

- Deleted backup jobs
- Removed snapshots required for system restoration

Technique: Data Encrypted for Impact

- Used SSH to push ransomware scripts to ESXi servers
- Used vim-cmd to trigger execution of the ransomware payload

- Resulted in mass encryption of critical VMware systems
- Caused extensive downtime and business disruption

10. Impact on Marks & Spencer

- Online store shutdown for 46 days
- Over £300 million in financial losses
- Hiring freeze and business slowdown
- Severe strain on IT staff and operations
- Long-term reputational and trust damage

11. Threat Actor Profile: Scattered Spider (G1015)

Key Details

- Member arrested: 20-year-old from Florida
- Aliases: “King Bob”, “Sosa”
- Sentence: 10 years imprisonment
- Ordered to pay $13.4 million restitution
- Noted for involvement in “The Com” cybercrime group

“The Com” – Underground Criminal Network

Activities include:

- Social engineering
- SIM swapping
- Crypto theft
- Ransomware operations
- Sextortion
- Swatting
- Kidnapping & physical violence
- Torture & murder

The group blends cybercrime with organised physical crime, making them especially dangerous.

12. MITRE ATT&CK Mapping for Scattered Spider

- Maps Scattered Spider’s behaviours to MITRE tactics
- Helps organisations understand typical patterns:
    - Social engineering for Initial Access

- Identity-focused attacks
- Cloud & virtualisation exploitation
- Hypervisor-level operations
- Data theft + extortion + encryption