Week 3: Advanced Security and Final Reporting

1. **Basic Penetration testing**

   Nmap commands used

   nmap -p 3000 localhost

   nmap -O -p 3000 localhost

   nmap -A -sS -p 3000 localhost

   nmap -A -sS -sV -p 3000 localhost

   nmap -p 22,80,443 localhost

   nmap -T4 -F localhost

2. **Set Up Basic Logging**

Logger.js

```
// logger.js
const { createLogger, format, transports } = require('winston');

const logger = createLogger({
  level: 'info',
  format: format.combine(
    format.timestamp(),
    format.printf(({ timestamp, level, message }) => {
      return `[${timestamp}] ${level.toUpperCase()}: ${message}`;
    })
  ),
  transports: [
    new transports.Console(),
    new transports.File({ filename: 'logs/app.log' })
  ],
});

module.exports = logger;
```

App.js

```
// POST /login
router.post('/login', async (req, res) => {
  const { email, password } = req.body;
```

```
  try {
    const user = await findUserByEmail(email); // your auth logic
    if (!user) {
      logger.warn(`User login failed: Email not found - ${email}`);
      return res.status(401).render('login', { error: 'Invalid credentials' });
    }

    const isPasswordValid = await verifyPassword(password, user.password);
    if (!isPasswordValid) {
      logger.warn(`User login failed: Wrong password - ${email}`);
      return res.status(401).render('login', { error: 'Invalid credentials' });
    }

    // Successful login
    req.session.userId = user.id;
    logger.info(`User logged in: ${email}`);
    res.redirect('/dashboard');
  } catch (err) {
    logger.error(`Login error for ${email}: ${err.message}`);
    res.status(500).send('Server error');
  }
});

module.exports = router;
```